Smart College for Modern Education

Hebron _ Palestine

Information Technology Department

Final Year Project Report 2023

Security Incident Response Plan For Smart College

Prepared by:

Khitam abu awwad 22110016

Saif AL-Hmouz 22110175

Malak AL-sayed 22110027

Project Supervisor: Afnan Al-Madhoun

Based on the smart college system for modern education, the supervision and follow-up of the direct supervisor of the project and the follow-up of the members of the examining committee, this project was submitted to the Information Technology Department, to complete the requirements of the intermediate diploma degree in cybersecurity.

Dedication

By the name of the God the most Merciful, the most Compassionate

we dedicate this graduation project to both my family and friends who stood by me and supported me throughout my studies.

To my parents who raised me on good morals and instilled in my heart a love of science and knowledge, and provided me with moral support that was crucial in the realization of this project.

we dedicate this graduation project to my brother who left me and could not watch me knowing that if he were alive, he would have been proud of me and my achievement.

we also dedicate this graduation project to all the teachers and professors who shaped my personality and helped me build my academic future.

Finally, we dedicate this project to myself and to God who has given me this opportunity and helped me achieve it.

Acknowledgement

We would like to express our thanks and great appreciation to all the individuals who contributed to our graduation project. This project would not have been possible without their sincere efforts and unlimited support.
First, we would like to thank our supervisor who guided and helped us throughout the project. She gave us valuable advice and clear guidance that was crucial in the completion of the project. and We would also like to thank all our team members for their boundless efforts and teamwork. It was a pleasant and positive experience to work with this team. and We would also like to thank all other contributors to the project, including volunteers and consultants who provided technical and knowledge support to us. and Finally, we extend our thanks and appreciation to our families and friends who stood by us and supported us during the project period. Their support and encouragement played a big role in the success of the project.

Abstract

The Incident Response Plan is a plan that outlines the actions and guidelines that must be taken when a security incident occurs such as a security breach, cyberattack, data leak, data outage or loss or any event that affects the security and safety of the electronic systems of any organization The goal of the plan is to address the incident effectively and quickly, reduce the negative effects on the organization and promote the restoration of natural order with the least possible damage.

The Smart College for Modern Education includes a huge amount of important and sensitive data and there are many points through which it is possible to access that data or the loss and interruption of data or the exposure of protection devices in the Smart College to malfunction and stop working, which leads to the lack of continuity of work in the college and this negatively affects the functioning of the college.

To avoid these problems that we mentioned, a response plan can be made to provide data import and backup procedures and avoid the loss of correct data, and these plans work to ensure that the damage of attacks that the college can be exposed to.

Among the expected results of such a plan in the Smart College:

1Reduce the damage of cyberattacks that the college can be exposed to.

2. Preserving data from loss or interruption

3. The ability to make alternative copies of data through high-quality protection devices that can keep data for a long time without interruption

4. Adding alternative structures to protection devices as alternative structures to the structure in the college that work to prevent disruption of sites or services for a longer period so as to ensure the retrieval and work of systems within 6 hours of work with the help of the response team that is appointed,

which consists of two people specialized in cybersecurity in the smart college and they work in the information technology department and also a person from the administrative affairs department because it works on the most important site in terms of data availability and a person from academic affairs.

Table of Contents:

Subject…… page

List of figures

List of tables

List of Abbreviations

Abbreviations	connotation
CIRP	Security Incident Response Plan

CHAPTER ONE

الفصل الأول

Introduction - المقدمة

1.1 Introduction

It is no secret to everyone that the wide spread of Cyber security attacks on many sectors and companies differs in their activity and the nature of their work, and these attacks fundamentally affect these organizations, which may lead to great losses. Therefore, the importance of responding to security incidents came in order to raise the speed of detecting these attacks to prevent

any financial losses or data leakage. or other activities that may affect the conduct of business or affect reputation.

Security incident response plans are a set of procedures that organizations use to respond to security threats. They are designed to ensure that the organization is prepared to respond in a timely and effective manner to any security incident.

The objective of security incident response plans is to ensure that the organization is able to detect, contain, and recover from security incidents in a timely and effective manner.

When an incident or security breach occurs, a structured approach will help mitigate its effects as soon as possible. [1]

The Smart College for Modern Education Cyber Incident Response Plan project aims to develop and implement effective response procedures to the cybersecurity challenges that the college and its systems can face.

The idea of the response plan for security incidents in the smart college is: analysis and evaluation, development of response strategy, establishment of a response team.

The goal of the college's security incident response plans is to ensure that the college is able to detect, contain and recover from security incidents in a timely and effective manner.

1.2 Overview:

In this chapter :

The Security Incident Response Plan is one of the main tools to ensure security protection and safety in the college, and aims to identify the necessary steps to respond effectively to security incidents such as security breaches, computer viruses, electronic fraud and other electronic risks.

In this chapter we will talk about how the college can benefit from the security incident response plan:

1_ Reduce negative impacts: A cyber incident response plan can reduce the negative impacts of potential incidents. For example, in the case of a malware attack or server hack, effective measures can be identified to limit the spread of the attack and restore the system in the shortest possible time. This ensures the continuity of services and avoids interruption of educational and administrative processes.

2_ Enhancing preparedness and readiness: The existence of an electronic incident response plan provides an opportunity to enhance readiness and readiness in the college. Appropriate roles and responsibilities are defined for the teams concerned, and staff and students are trained and sensitized to the plan and procedures. Trainings and simulations can also be performed to ensure that everyone understands the procedures and is able to deal with electronic incidents effectively.[3]

1.3 Objectives

When a cyber security incident occurs, timely and thorough action to manage the impact of the incident is a critical to an effective response process. The response should limit the potential for damage by

ensuring that actions are well known and coordinated. Specifically, the response goals are:

1. Maintaining and protecting the confidentiality of the constituent information and the information of employees and students and ensuring the integrity and availability of the college's smart systems and networks for modern education and related data.
2. Helping the employees of the Smart College for Modern Education to recover their data after a security incident for the computer, network or any other type of data loss or interruption.
3. Provide a consistent response strategy to system and network threats that put Smart College for Modern Education data and systems at risk.
4. Develop and activate a communications plan including initial reporting of the incident as well as ongoing communications, as necessary.
5. Minimizing the reputation risk of Smart College for Modern Education.[4]

1.4 Motivations:

Purpose of the Security Incident Response Plan [CIRP]:

To support a swift and effective response to cyber incidents aligned with the organization's security and business objectives.

Objectives of the CIRP:

1. One of the motives for the response plan is that the college contains many sensitive and important data, whether at the level of students or at the level of employees, and therefore it must be protected from loss or interruption, and to do so, the response plan for security incidents has been resorted to ensure its protection and business continuity in the college..

required to manage responses to cyber incidents.

2. To provide guidance on post incident activities to support continuous improvement .

3. Preserving the safety and security of the institution (Smart College of Modern Education): The plan that we are working on aims to maintain the integrity and security of data and protect it from attacks and security incidents.

4. Maintaining the continuity of data availability in the smart collage for modern education.

The importance of availability in the implementation of the incident response plan in the Smart College for Modern Education:

In general, availability in information security refers to the ability of authorized users to access and use data and systems as intended. Ensuring availability is one of the important aspects that we can rely on in implementing this plan because data availability ensures that employees, students and everyone who has the information have access to the data

and information they need to complete the work and maintain the operations of the college.

Through this plan, we would like to address threats to data availability, including: data outage or loss, network outages, hardware failures, and other threats to availability.

Continuity on availability: The Smart College for Modern Education includes huge amounts of valuable and sensitive data such as staff and student information and information about the agreements that the college concludes with many educational institutions, and there are many access points to that data, some of which can be easily exploited if the recovery and backup measures and avoid the loss of the correct data are not in place.[5]

Table 1.1: Time planning for first semester

Weeks / Tasks	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Choose a project idea																
Collect information about the project																
Writing project proposal																
Requirements analysis																
Test plan																
Documentations																

CHAPTER TWO

الفصل الثاني

Literature Review - الدراسات السابقة

Chapter two.....

2.1Overview:

In this chapter:

Security incedent response studies are about analyzing and assessing the severity of security attacks and developing effective response plans to counter such as . these studies aim to enhance cyber security and reduce the impact of attacks on institutions and individuals .

These studies include several areas, including: risk analysis, identification of potential cyberattacks, and reducing the impact of these attacks.[6]

2.2 Previous Projects and Studies

There are many studies and researches related to security incident response plans, which aim to improve the efficiency and effectiveness of those plans, and the most prominent of these studies are:

2.2.1 A study conducted by MCI experts on best practices for designing security incident response plans, which included reviewing a number of actual cases and analyzing the response methods used in those cases.

2.2.2 A study conducted by researchers from the university of California on the design of a security incident response management system which aims to improve the efficiency of organization response to security attacks.

In addition to studies related to security incident response plans, there are many projects that have been implemented to develop electronic incident response plans, among these projects:

2.2.3 NIST Cyber Security Framework: a project launched by the US National Institute of Standards and Technology (NIST), the project aims to provide a general framework for managing cyber security, including cyber incident response plans. The project was implemented in collaboration with the private and government sectors, and includes an analysis of best practice, identification of cyber security requirements, and guidance for the design and development of cyber incident response plans.

2.2.4 Cyber resilience and information project: it is a project launched by the British cyber security agency (NCSC). The project aims to improve the ability of companies and organization to deal with cyber-attacks and reduce the impact resulting from them. The project includes the development of

security incidents response plans, training of personnel and the necessary security measures to improve cyber security.

Briefly, the difference between these projects and the plan that we are working on in the smart collage for modern education is the work of responding to security incidents of kinds and recovering from them in an effective manner and trying to use this plan in an attempt not to interrupt or loss data in the collage network and also to maintain the availability of this data in addition to training employees at the smart collage of modern education to face these incidents. [7]

2.3 Summary and review

A security incident response plan is a plan that defines the procedures that must be followed to identify and deal with security incidents related to electronic systems and networks. This plan contains clear and accurate procedures to prevent and address security incidents quickly and effectively to reduce the impact on the institution (Smart College of Modern Education) .The security incident response plan includes several phases, including:

Identify and classify potential security incidents and assess the level of impact they can cause. Develop a strategic plan to deal with security incidents and identify the tools and resources necessary to deal with them Implement the strategic plan, verify its effectiveness and evaluate it Continuously Provide training and education to employees about the plan to respond to security incidents and ensure that they understand and apply her correctly. Having a security incident response plan is vital for Smart College for Modern Education because it relies on technology, as it helps improve its ability to deal with security incidents effectively and reduce the negative

impact on the company's operations. It is worth mentioning that there are many previous projects and studies that dealt with security incident response plans that have proven effective in improving the ability of institutions and organizations to deal with security incidents and mitigate their impact on their operations.[8]

2.4 Pose the problem

The problem is that security incidents can occur in the Smart College of Modern Education at any time and may lead to disruption of services and affect users or employees in addition to their inability to the data they need and this educational institution can be difficult to deal with these incidents due to their unexpected nature and the lack of a plan to deal with them and these incidents can be represented in the loss or interruption of data or the lack of availability of this data, which negatively

Affects The nature of the work of the educational institution (Smart College for Modern Education) [9]

2.5 Solution methodology:

To resolve the problem of data loss or interruption, a security incident response plan should be developed that includes data recovery procedures in the event of loss or disconnection with data. This plan includes the following steps:

2.5.1 Assess the current situation: In the beginning, before starting the response plan, the current situation in the college was evaluated in terms of the type of protection systems and devices used, the existing backup plans and the structure that the college follows to respond to security incidents that

can affect the college, and the extent to which employees and students know the importance of security in the institution.

2.5.2 Find the source of the defect: After evaluating the situation in the college, the sources in the college were searched for that could be a defect and work on data loss or interruption, such as protection devices that have been wrongly configured or there are files containing virus files and other sources of defect.

2.5.3 Identify lost data: In case of data loss, the plan has been activated so that the lost data and the parts that can be recovered and cannot be recovered are identified.

2.5.4 Use recovery tools: During the work of the plan, we developed a set of tools to recover lost data or recover data without losing any parts of it, through the work of backup structures such as the use of cloud storage or storing data on data center devices so that it is far from the college building.

2.5.5 Re-analysis and auditing: After the work of the structures to maintain the non-loss of data and complete the work of the smart college systems and sites without interruption, the data must be audited and analyzed after its recovery to ensure its validity and completeness so that any files that contain attacks or affect the continuation of the work or affect the work of protection systems are addressed.

2.5.6 Take preventive measures: After the implementation of the plan and the ability not to stop the college's sites and systems, a set of preventive measures have been taken that maintain that security incidents do not occur in the future in the college by repeating the copies of important data and storing it in a safe place Using protection devices with backup protection devices for the main devices The settings are made on both devices manually

so that when a malfunction occurs in one of the main protection devices, the backup devices are made within 6 Working hours by the response team in addition to increasing the expertise of employees and training them on the importance of security and protection from cyberattacks.

In addition, the training and preparation of the Security Incident response team must be provided, and plans should be updated periodically to ensure a rapid and effective response in the event of an incident

CHAPTER THREE

الفصل الثالث

الخلفية النظرية -Theoretical Background

3.1 Overview:

In this chapter :

The response plan for security incidents revolves around the idea of dealing with security attacks and incidents and ensuring the continuity of electronic systems and important data in the institution (Smart College for Modern Education). This plan focuses on managing and organizing the response to security incidents effectively, which helps in maintaining safety and security in addition to the availability of data in the institution.

Security incident response plans are based on several core theories, including information security theory and crisis management theory.

1-Information security theory states that cybersecurity is a process that maintains confidentiality, transition, and availability of important and vital information, and this process is the application of appropriate policies, procedures and technologies to protect data from hacking, damage, loss and theft.

2- Crisis management theory states that crisis management requires predicting potential events and developing plans to respond to and deal with them effectively using available resources. In the case of cyberattacks, response plans are prepared that include removing the attack, verifying the integrity of systems, restoring critical data, analyzing the attack to identify sources and take action to prevent it from happening again.[10]

3.2 The business idea of the project

The idea of working on the project that we are working on requires achieving many goals and following some steps, which are:

3.2.1 Identify the team responsible for preparing the plan: Identifying a specialized team in the field of cybersecurity from the Smart College in Teaching Hadith and other departments in the college to implement the project.

3.2.2 Objectives and Risk Analysis: Identify the main risks that may face the Smart College of Modern Education and analyze the objectives required to protect it from cyberattacks.

3.2.3 Develop the necessary plans: Develop security incident response plans that contain the steps required to verify the integrity of systems and data and restore them in the event of an attack, outage and loss of data.

3.2.4 Team Training: Training team members based on the implementation of plans and procedures required to manage security incidents.

3.2.5 Verify the effectiveness of plans: determine the effectiveness of plans and update them periodically to meet the needs of the organization and technological changes.[11]

3.3 Tools used

There are several tools that we will work on in the security incident response plan, including:

3.3.1 Security Programs: These programs can be used in this plan to protect systems and data from cyberattacks, and include antivirus, firewalls, and anti-malware and intrusion programs.

3.3.2 Security monitoring tools: These tools help monitor the college's smart systems for modern education and analyze unusual activities, and include monitoring, analysis and reporting tools.

Data recovery tools: Tools that help recover data lost or damaged by cyberattacks, including backup, data recovery, review and analysis tools.

3.4 Materials used

There are many materials that we will use in the response plan for security incidents according to the objectives of the plan that we are working on in the Smart College for Modern Education, and these materials are divided into several categories as follows:

3.4.1 Evidence and Documentation: This category includes the documents and materials needed to establish a security incident response plan, such as security policies, procedures, and guidelines. It can include employee guidance documents, internal work instructions, and management guidelines.

3.4.2 Software and Tools: This category includes software and tools that will be used to implement security incident response plans. These tools can include protection software, security monitoring tools, data recovery and analysis software, error analysis tools, and tools for threat assessment.

3.4.3 Equipment: This category includes equipment needed to implement Security Incident Response Plans.

3.4.4 Communications: This category includes communications, software, and applications that help in communication and coordination between members of the cyber incident response team and external parties, such as service providers, government authorities, and cybersecurity professionals.

3.4.5 Educational programs: These programs are used to educate employees about cybersecurity risks and teach them how to deal with them. These training programs include suspicious email warnings and how to detect malware example: Interactive Online Training Provide interactive online training programs aimed at familiarizing employees with cybersecurity concepts and improving their awareness of common cyber threats such as spam, phone fraud, phishing, and others .[12]

CHAPTER FOUR

الفصل الرابع

Practical implementation-التنفيذ العملي

4.1Overview:

In this chapter :

The practical implementation of the security incident response plan included several important steps, as follows:

Incident detection: Determine whether a security incident has occurred, determine the type of incident and the extent of its impact on systems and

data, Assessment: Assess the situation comprehensively and determine whether action is required to deal with the incident, and what steps are required to address it, Actual response: Take concrete action to address the incident, such as isolating damaged systems, identifying and removing the cause of the incident, recovering lost data, and working to improve cybersecurity, The basic steps to implement the security incident response plan also include training and qualification of the response team, testing and updating the plan periodically to ensure its effectiveness and updating it to face changing and new threats in the field of information security.[13]

4.2 Project implementation steps with detailed explanation of each step:

The first step in working on the plan is to form a response team and a response team in the college:

4.2.1 Preparation:

Preparing for the security incident response plan at the Smart College for Modern Education required several steps:

1. Goal setting: Identify key objectives of the response plan, such as securing data and maintaining service continuity.
2. Risk Analysis: Analyze and evaluate potential risks that the college can face, such as attacks, viruses, and intrusions.
3. Establishing a response team: Forming an incident response team in the college so that it consists of members specialized in information technology and management, such as: two people from the information technology department in the college and a person from

the management department. So that the team has the knowledge and skills to deal with security incidents.

4. Identify Contact & Communication: Identify appropriate communication and reporting methods when an incident occurs. So that there are effective ways to communicate with team members and relevant external parties.

4.2.2 Team reasponse:

Security Incident Response Plan Response Team at Smart College for Modern Education: This team consists of a group of experts and specialists in the field of cybersecurity, such as: two people from the IT department at the Smart College, a person from administrative affairs and a professor from academic affairs. The incident response team aims to protect the data and electronic systems in the college and to counter any security attacks that may be exposed to it. Among the tasks of the team are:

1. Immediate verification and response: Team members were assigned to continuously monitor the college's electronic systems
2. and verify potential security incidents. If an incident is discovered, members of this team take swift action to deal with and contain it.
3. Threat Assessment and Investigation: The response team assesses security threats and analyzes potential risks that the smart college may face. The necessary investigations are carried out to identify the sources of the attacks and identify security gaps.
4. Enhancement and improvement: Based on investigations and threat assessments carried out by the response team, recommendations and improvements are provided to enhance security in a smart college environment. Maintenance procedures and updates are implemented to enhance electronic protection.

5. Data and Systems Protection: The response team works to protect sensitive data in the smart college. Through the use of advanced tools and technologies, the team counters cyberattacks and secures systems and applications.
6. Prevention and Training: The response team helps educate faculty members on best practices in cybersecurity and teach them how to properly identify and deal with threats. Training sessions and workshops are organized to emphasize the importance of security awareness and preventive measures.

4.2.3 Smart College Structure:

In the structure of the Smart College of Modern Education, the structure is divided into two parts:

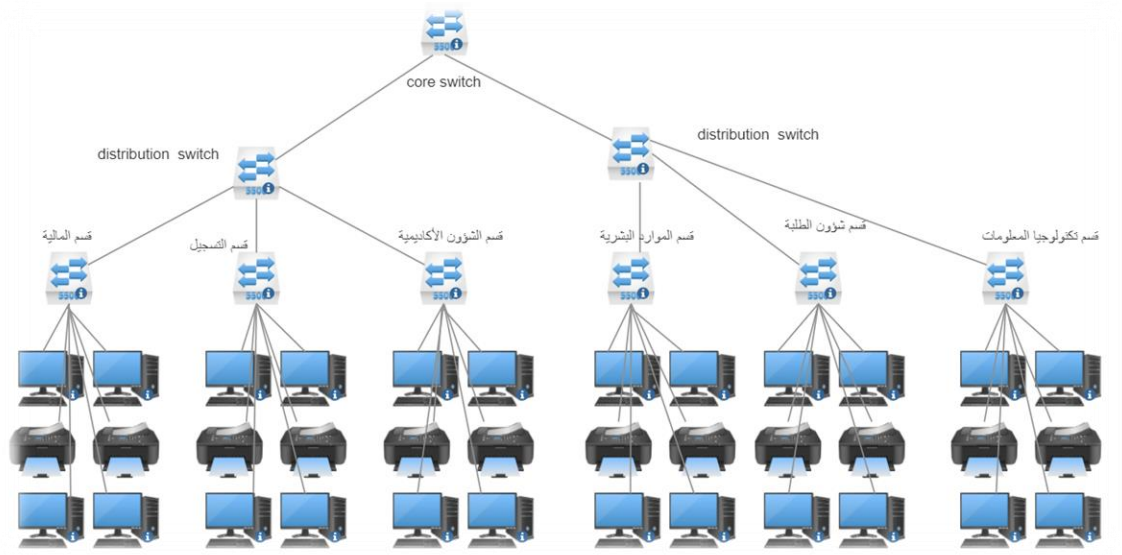

Figure 4.1 Distribution of switches in the departments of the Smart College

The first part, which is the network:

First, the cloud is connected with 3 firewalls, each Firewall is connected to the core switch through two ports, the first core switch port and the

second core switch port, in addition to that 2 core switches are connected to each other so that one of the core switch works when a malfunction in one of the core switches, and also on each floor there are a number of devices and switches, the ground floor contains 2 switches, the first 3 switch, the second 4 switches and the third 3 switch and fourth 3 switch, the fifth 2 switch and the sixth 1 switch so that the fifth floor contains the server room The firewall distribution in the college is as follows: firewall internet_ FG firewall DC_ FG and firewall stand by, so that the latter type works as a backup copy that works in the event of a defect or malfunction in one of the firewalls. In addition to many other devices such as computers, printer…

4.2.4 College Alternative Incident Response Plan:

The alternative plan in the Smart College for Modern Education for incident response is the Firewall standby mode, meaning that when there is a cut or loss of data in one of the firewalls, all data manual moves to the firewall standby so that it is turned on within two hours of work.

4.2.5 Smart College Websites:

As for the sites available in the college according to priorities, they are available as follows: Portal site, College website, Model site, registration site, Graduates site, and Student Lending Site.

Based on the structure mentioned above, if one of the firewalls malfunctions, this malfunction will affect the continuity of these sites, and therefore through the response plan that we are working on in the Smart College, we have developed a plan that maintains the continuity of the work of these sites so that the work of the highest priority sites continues without interruption, and one of these highest-priority sites in

the college is the portal site because this site provides a variety of academic and administrative services and information for students enrolled in the Smart College for Modern Education Among these services : College announcements Subject management and semester results The registration site is usually used to register in classes and choose courses.

Based on these priorities of the sites, response plans have been made to maintain the continuity of the work of these sites, which are as follows:

1- The response team that was appointed in the plan should work on retrieving the sites that happened down in the college within 6 working hours.

2- Work on holiday response plan team in case they are required to work for an emergency at the college.

3- Make backup copies on sites and devices outside the college building.

4- Based on the response plan, work must be done to recover the highest priority sites that happened down within a working day.

These structures include:

1- The high availability structure ((active _ passive) can be implemented so that there are 2 firewalls, the first is of the FG type and the second is also of the FG type so that both firewalls are of the 600F _ FG type The reason for choosing this type is that it is able to handle the expected data traffic volume and handle it efficiently in college in addition to the security features available in this type, one firewall

works normally and the second has a configuration, but it does not but it does not work except in the event of a malfunction in the first server.

2- Firewall Stand By provides both Internet _ FG and Data Center FG
3- The presence of vendor If any vulnerability occurs on any first vendor, the second vendor contains this vulnerability

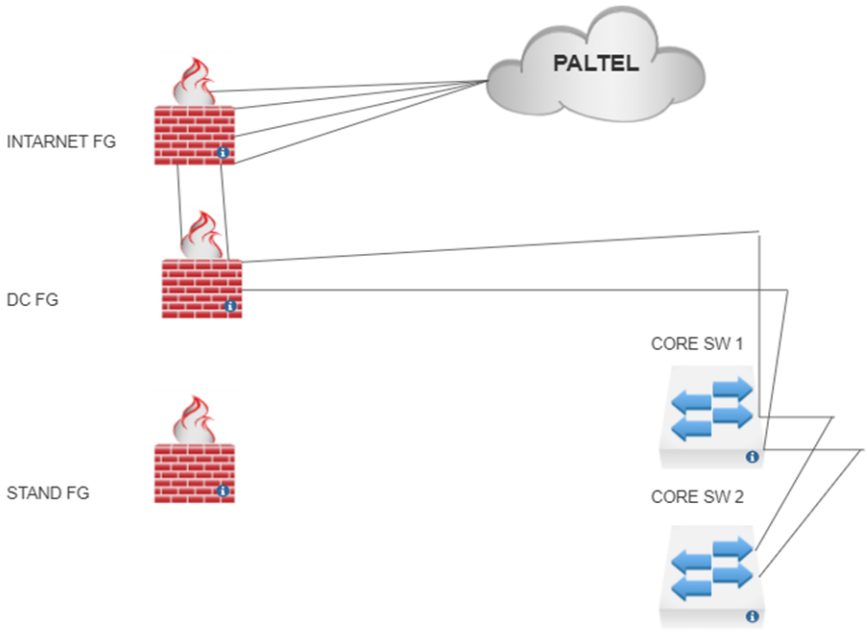

Figure 4.2 Structuring firewalls in collage

In the case of responding to incidents that occur on firewalls, a plan has been developed, which is:

1_ In the case of hacking attacks: a plan has been developed that the assigned response team must identify the cause of the breach and correct existing security vulnerabilities.

2_ Firewall failure leads to internet and network interruption and in this scenario the following actions can be taken:

3- Identify the cause of the failure in the firewall and take the necessary actions to fix it and strengthen protection.

The second part is for the Data Center:

In the structure of the Smart College for Modern Education, the Data Center is located on the fifth floor of the college so that it consists of 3 servers and the supervisor to inspire the Prox Mox system, these servers are also linked to the cloud backup, in addition to the presence of a 4 server located in the same place for backup, and these servers are linked to each other through the cluster The function of this cluster is that if a down occurs to one server, the other server works automatically in addition to using a process the replication in the backup process, As for the VM between servers, it distributes the load to other servers in the event of a down of one of the servers.

As for maintaining the continuity of information in the college's servers and preserving it from loss, several structures have been developed through the plan that we are working on, which are as follows:

1_ Implement a regular backup strategy and store backup copies of servers in the college in servers located in secure locations outside the college to maintain the integrity of data and the ability to recover it in case of loss.

2_ The Distributed Server strategy can be used so that many servers are distributed over a wide area network in the college.

3_ Virtualized server Create multiple virtual servers on a single server or group of servers.

In the case of responding to incidents that occur on the server, a plan has been developed, which are:

1_ The use of special antivirus for servers with follow-up and periodic review to detect attacks.

2_ Power outage or hardware failure: Report the problem to the relevant service team or service provider.

3_ Activate the fault response plan and prioritize the restoration of services, Test faulty devices and repair or replace them if necessary.

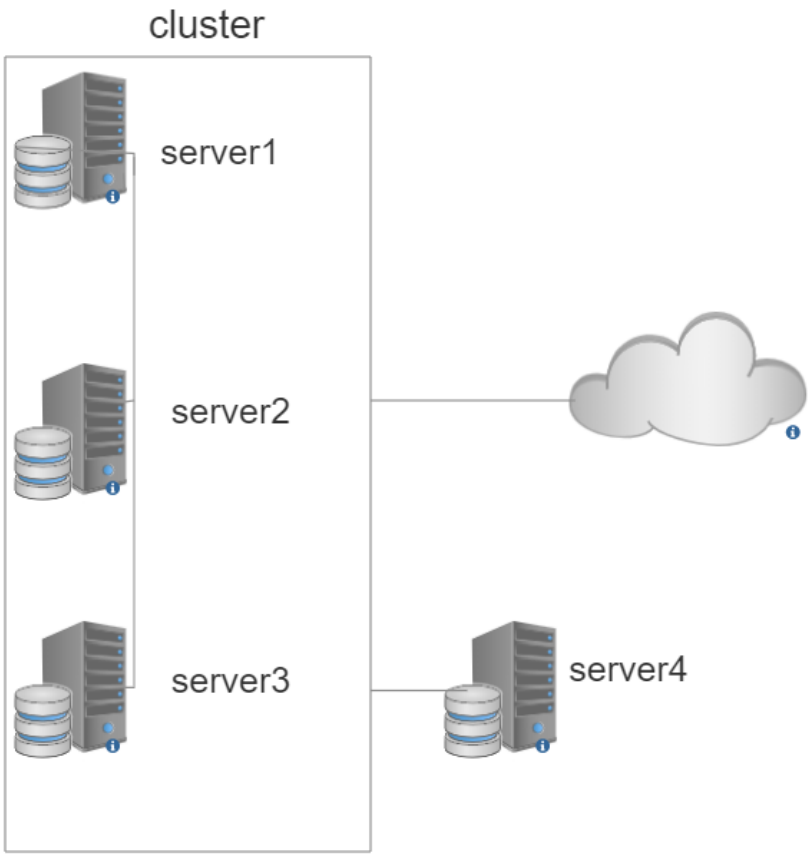

Figure 4.3 Structuring datacenter in collage

4.3 Results and comparisons:

The implementation of the plan in the Smart College for Modern Education contributed to enhancing cybersecurity and maintaining the uninterrupted work of the educational institution for a long time, and the plan that has been worked on aims to achieve a quick and effective response in the event of a security incident in the college and also the important thing in this plan is to plan in advance and prepare for security incidents by appointing a response team from within the smart college and working to train employees and students on how to deal with cybersecurity threats.

Among the results reached during the work on the plan Is to do a check on the plan:

4.3.1 Plan testing: Conduct regular testing and training of the response plan to ensure its effectiveness and ensure that the team is able to deal with incidents effectively. Update the plan based on lessons learned from the exercises.

After working on the plan in the smart college, we conducted an examination of it to ensure the effectiveness of the plan, and this examination is related to the effectiveness and ability of the backup to work, the amount of time it takes to recover data, and specify how much time each VM needs to back up and how long each VM exits.

Through the examination that was performed, an example was obtained, which is the time to retrieve data in lighting systems and the time it takes to recover the data is half an hour, which means that if the data is cut, it will take half an hour to retrieve it.

Through the examination, this illustrative image was obtained, which shows the time of data retrieval:

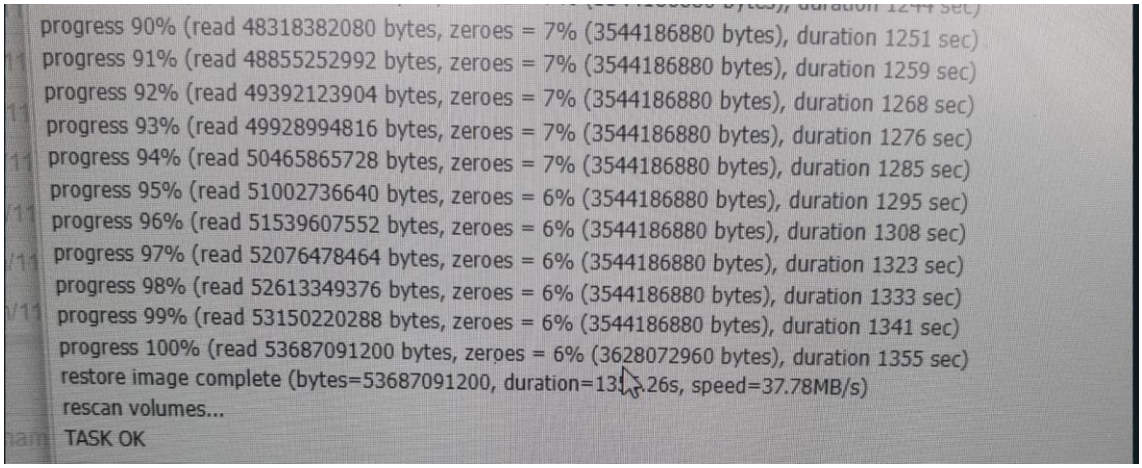

Figure 4.4 Backup process

The image attached above shows that when the data was restored.

Proxmox stores the full data, but each time it stores the changing data

In case of disconnection, you can work on defining a second server in a second place linked to the cloud or local that makes a restore.

Based on the results of the plan and the priority of sites in the college, the data is recovered as follows:

1. In the VM1 that contains data (portal website:portal.scme.edu.ps), the data is recovered in at least 15 minutes.

2. In the VM2 that contains data (college website scme.edu.ps), a data recovery is performed in 30 minutes.

3. In other sites such as Model (registration site) (Graduates website) (student lending site), data is retrieved during working hours.

So that the Model site is restored within 20 minutes

Registration site is restored within 6 hours of operation

4. (Graduates website and student lending site) their data is restored after restoring the data of the rest of the sites, because they are less priority than the rest of the sites.

5. This restore is done from the local backup And this restoration process is a police check.

4.4 **Recommendations:**

Among the recommendations reached through the project that has been worked on, which is entitled Security Incident Response Plan:

4.4.1 Identify a security incident response team: Identify a response team that is specialized in dealing with cyber incidents and must be from within the scope of the college so that the team is among the departments that work in the college.

4.4.2 Work on risk assessment: Evaluate risks in the college continuously to identify potential threats and dangers such as data loss, interruption or exposure of protection devices to malfunction so that this helps to assess the impact of accidents and the likelihood of their occurrence and this helps in determining the priorities of the plan.

4.4.3 Continuous Training and Outreach: Provide continuous training to team members and other staff in the college on the response plan and best practices in cybersecurity. Awareness helps to raise awareness and enhance capabilities to deal with cyber incidents.[14]

4.4.4 Development of response procedures: the ability not to maintain the plan that has been worked on to respond to incidents in the college so that a clear and specific plan is developed and developed for cybersecurity incidents and these plans include dealing with security breaches, data loss and other cyberattacks.

4.5 **Conclusion:**

The college's security incident response plan is an important framework that helps ensure business continuity and protect sensitive information and systems in the university environment. The summary

of the college's electronic incident response plan includes a set of systematic and preventive measures taken by the college to deal with and contain cybersecurity incidents as soon as possible.

The summary of this plan includes:

1. Define teams and roles: Appoint a security incident response team composed of members specialized in the field of cybersecurity and information technology. Define the roles and responsibilities of each member of the team and clarify the procedures required for rapid response to incidents.

2. Threat Recognition and Security Analysis: Potential security threats that the college may face are evaluated and potential vulnerabilities in systems and networks are analyzed. This helps to take appropriate preventive measures and prepare to deal with accidents.

3. Develop a response and recovery plan: A detailed and comprehensive response plan has been developed that outlines procedures for dealing with security incidents and restoring damaged systems and data. Procedures are documented and updated regularly to ensure they are adapted to emerging threats and changes.[15]

Resources:

[1] "Creating a Cybersecurity Incident Response Plan: A Template for Success" by CSO Online:

How to build an incident response plan, with examples, template | TechTarget

[2] "Computer Security Incident Handling Guide" by NIST Special Publication 800-61: This comprehensive guide provides an overview of incident handling and response, including developing a response capability, implementing an incident response plan, and effectively handling security incidents. It can be found on the NIST website.

[3] Computer Security Incident Handling Guide" from the National Standards and Technology Institute (NIST): https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[4] "SANS Incident Response Whitepapers": This website contains a collection of white papers and resources on security incident response plans by the SANS Institute. You can find the documentation here: https://www.sans.org/white-papers/incident/

[5] "Computer Security Incident Response Team Management: Leadership Skills for Managing the Incident Response Function" by security scientist Leighton Johnson: This book is about managing security incident response teams and developing effective response plans.

What is Incident Response? Plan and Steps | Microsoft Security

[6] "Disaster Recovery Planning: Insuring Business Content" by IPM: HTTPS://O.EPM.COM/TOPIX/Disaster-recovery-planing

[7] "A Guide to Cyber Assist Response" BT National Institute of Standards and Technology (NIST):

http://w.nest.gov/publication/guide-cyber-assisted-response

[8] "Creating a Cybersecurity Incident Response Plan: A Template for Success" by CSO Online:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjdoezCvPj-AhVvRkEAHTb6BMAQFnoECAsQAw&url=https%3A%2F%2Fwww.grcilaw.com%2Fblog%2Fthe-6-phases-of-a-cyber-incident-response-plan&usg=AOvVaw0QPfkCaRrWd8_aoRXZtHUx

[9] "Cybersecurity Incident Response Plan: A Comprehensive Guide" - What is an Incident Response Plan and How to Create One (varonis.com)

[10] "Cybersecurity Assist Response Plan Development: A Comprehensive Guide" - https://resource.infoskinset.com/CyberSecurity-Assisted-Response-Plan-Development-A-Comprehnsif-Guide/

[11] "A Systematic Review of Cybersecurity Incident Response Plans" - https://www.bing.com/ck/a?!&&p=7c423b6ca85a85d4JmltdHM9MTY4NDEwODgwMCZpZ3VpZD0wY2Q4ZTk5Ni1hYTQ0LTYyNjEtMjQ4YS1mODdjYWJkNDYzN2EmaW5zaWQ9NTEzNw&ptn=3&hsh=3&fclid=0cd8e996-aa44-6261-248a-f87cabd4637a&psq=%e2%80%9cIncident+response+%26+computer+forensics%e2%80%9d+(3rd+edition)+by+Matthew+Pepe%2c+Jason+T.+Luttgens+and+Kevin+Mandia&u=a1aHR0cHM6Ly93d3cub3JlaWxseS5jb20vbGlcmFyeS92aWV3L2luY2lkZW50LXJlc3BvbnNlLzk3ODAwNzE3OTg2ODYv&ntb=1

[12] "A Framework for Cyber Incident Response Planning" - https://ieeexplore.ieee.org/abstract/document/7572217

[13] "Developing an Effective Cybersecurity Incident Response Plan" - https://www.sans.org/reading-room/whitepapers/incident/developing-effective-cybersecurity-incident-response-plan-38005

[14] "Cybersecurity Incident Response Plan: An Overview" - https://www.researchgate.net/publication/341523598_Cybersecurity_Incident_Response_Plan_An_Overview

[15] "A Systematic Review of Cybersecurity Incident Response Plans" - https://www.sciencedirect.com/science/article/pii/S0167404821000426

[16] "Assist Response & Computer Forensics by Jason T. Luttgens, Matthew Baby, & Kevin Mandia"

[17] Computer Security Assist Handling Guidi by National Institute of Standard & Technology (NEST).

[18] "Resident Response: Investigating Computer Cream" by Chris Process & Kevin Mandia.