Plan of Contingency For the Unit of Systems and Technology of Information the Autonomous Government Decentralised Antonio Ante in Base to Norm Iso/Iec 27002.

Luis D. Narváez, Karina To. Méndez
ldnarvaez@utn.edu.ec., kary_3040@yahoo.es

Abstract — *The present work analyses a methodology for the development of a Plan of Contingency for the Systems of Information, define general actions to ensure the suitable recovery of information and of the computer services inside the organisation; this methodology comprises the analysis and identification of risks, identification and evaluation of threats and vulnerabilities, estimates of impact, the probability of occurrence, evaluation of stages of contingency, the necessary protections, as well as also the definition solve and strategies that allow to guarantee the continuity of the activities in case to materialise said threats.*

Have present that does not exist a system 100% insurance, since the risks always are presents, in spite of the measures that take to warn it.

***Terms for the indexing*— The Security of the information, Plan of Contingency.**

I. INTRODUCTION

A Plan of Computer Contingency is a group of activities that allow us make actions to minimise the risks in case of some disaster of natural origin or human, keeping the operating capacity of the activities to a minimum level until recovering the whole of the systems and resources; a plan of contingency finds conformed by three fundamental actions that are: prevention, detection and recovery.

Prevention: they are actions that help us to warn any eventuality that affect the activities of the organisations of total or partial way to end to reduce the impacts produced.

Detection: they Are the actions that have to take during or immediately after the materialisation of the threat to end to diminish it.

Recovery: they define the processes or contours that have to follow after having controlled the threat, in this plan makes the restoration of the teams and activities to his initial state before materialising the threat.

II. TERMS AND BASIC DEFINITIONS

A. *Information* — The information can find it of different forms, in paper or of digital way, the information always has to have measures of security to end to avoid losses or modification of data that can put in risk the continuity of the activities of the organisation.

B. *Security of the conjoint* — information of rules, controls and procedures that adopt the organisations for salvaguardar the information of the different threats like frauds, espionages, vandalisms, fires, floods, wanton software, attacks of third, negation of services, etc.

C. *It looms* — unauthorised disclosure of the information without modifying the state of the system.

D. *RiesgOr*— a vulnerability exploded by one or several threats that when materialising cause damages and interruptions of the services and processes of information.

E. *Vulnerability* — Is a weakness in the security of the information that can give place by different causes as for example the fault of maintenance, fault of knowledge in the personnel, desactualizaciones of the critical systems, etc.

III. BASES OF THE SECURITY OF THE INFORMATION

"It does not exist a system 100% insurance, since the risks always are presents, in spite of the measures that take to warn it."

With this sentence can say that it does not exist a system totally sure, but if a reliable system, the same that it bases in 3 fundamental pillars of the security of information as it observes in the fig.1.

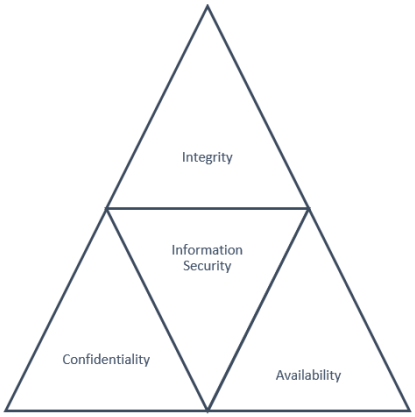


Fig. 1. Security of the information according to the norm ISO/IEC 17799

Confidentiality: Characteristic that guarantees that the information was accessible only for the people authorised to have access to the same.

Integrity: Characteristic that conserves the accuracy and whole of the information, ensuring that the information arrive complete and without modifications.

Availability: it Guarantees that the users authorised have access to the information whenever they require it.

IV. SYSTEMS OF INFORMATION

A system of information finds conformed by three elements as they are: the information, human resources and computational teams that operate in group to make activities of administration, storage, processing, transmission or reception data and information with the only purpose to fulfil with the aims of the organisation.

Entrance: capture of data so much from the interior as of the outside of the system of information.

Processing: convert data and information of a more significant way for the business.

Exit: transfer the already processed information to the users so that they develop his daily activities.

In the fig.2 it observes of graphic way the process that makes in a system of information

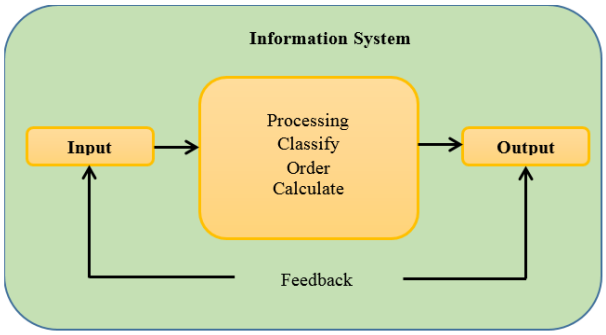


Fig. 2. Process of a System of Information

V. CHARACTERISTICS OF THE PLAN OF COMPUTER CONTINGENCY.

A plan of effective contingency, minimises the damages ocasionados to the organisation product of the materialisation of the threats of natural origin or by human errors, therefore it has to fulfil with the following characteristic:

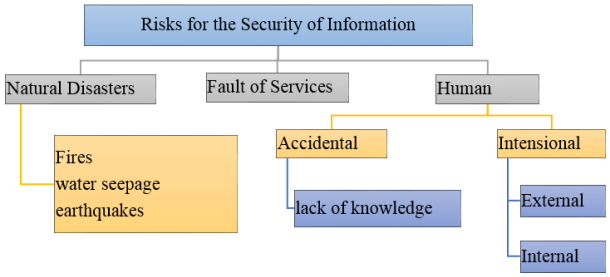
- *Approval*: it Has to be approved by the direction and the users.
- *Flexibility*: it Has to can adapt to any contingency, does not have to be specific for an alone disaster.
- *Maintenance*: Be precise, avoid unnecessary details so that it can be updated.
- *Cost-effectiveness*: The measures applied in each one of the eventualities will have to be evaluated in regard to the advantages that offer us, have to be reasonable.
- *Answer organised:* Have a list of the actions and services that have to receive priority.
- *Responsibility:* it will contain the name of the managers that have to assume the different functions in case of an emergency.
- *Proofs:* they will make proofs with inventories of time and procedures of backrest, has to have a methodology.

VI. PHASES OF A PLAN OF COMPUTER CONTINGENCY

A. Planning— contemplates activities like the initial diagnostic of the current situation of the institution, design of proposals for a determinate problem, diagnostic of the structure organizacional, services that offer to the citizenship, services consumed, material used and the inventory of the computer resources, doing use of tools automated or of manual form by means of the compilation of information, as well as also the delimitation of the scope of the plan of contingency.

B. Identification of stages of contingency and threat — obtains of the information purchased of the critical risks, identify them, know the causes and the impact that would generate for the organisation if they materialize. In the diagram 1 observes the possible stages of contingency that put in risk the security of the information.

Diagram 1. Risks for the Security of the información



Natural disasters: earthquakes, fires, floods or leaks of water.

Disasters by fault of services: you fail in the system of energy, ventilation and in the system of security, in the network of data, the teams of networking and servers.

You fail by third: human errors, denial of services, wanton software computer viruses, vandalisms, espionages, suspension in the processing of information.

C. Evaluation of Risks — for the evaluation of the risks has to identify , quantify and prioritise the risks givet ro of the organisation, the results obtained have to provide the necessary information to make a suitable management of risk by means of the implementation of controls of protection against the risks identified; it considers the following process:

1. Identification of the risks.
2. Evaluate of the risks in terms of impact and probability of occurrence.
3. Establish a suitable order of priority in the treatment of the risks.
4. Identify the maximum time of interruption allowed in the services and critical processes.
5. Define the designation of roles of work and obligations to the personnel in case of emergency.
6. Make a monitory continuous of the risks.

D. Identification of Technological Vulnerabilities does use of the list of the active and the existent controls inside the organisation, the vulnerabilities can find in the following areas:

- Organisation.
- Processes and procedures.
- Routines of management.
- Personnel.
- Physical environment.
- Configuration of the system of information.
- Hardware, software or teams of communications.

For the evaluation of the technological vulnerabilities does use of different technical or methods for example the utilisation of tools of software of automatic exploration, glimpsed, questionnaires, physical inspections among others; everything will depend on the importance of the system of technology of information and the available resources.

The criteria for the evaluation of the technological vulnerabilities of establish of the following way:

TABLE I
CRITERIOS OF EVALUATION OF TECHNOLOGICAL VULNERABILITIES

Characteristics / Denomination	Ease of Exploitation	Capacity of Detection	Cost of Recovery
Alta	Likely	Difficult	High
Average	Likely	Possible	High
Drop	Likely	Possible	Minimum
Minimum	Little Likely	Likely	Minimum

E. Assessment of the active — Once identificado the active of greater importance inside the organisation proceeds to the definition of a scale of assessment for each one of the active critics identified inside the organisation; the assessment can be of quantitative form like qualitative

In the table 2 observes the different characteristic for the allocation of a value to each one of the active of the organisation.

TABLE II
ASSESSMENT OF THE ACTIVE

ASSESSMENT OF THE ACTIVE				
Value	**Denomination**	**Availability**	**Integrity**	**Confidentiality**
4	I criticise	The information, installations and resources always has to be available His loss is considered like catastrophic for the Institution.	All information, installation or resource where the integrity is important and has to guarantee His catastrophic serious loss.	It covers all information, installation or resource described as of confidential use. Only it can be used with explicit permission
3	High	All information, installation or resource whose availability can be arrested person by some hours.	It covers all information, installation or resource in which the integrity is very important and has to guarantee.	All information, installation or resource described as of use restricted. Only it can be used by personnel authorised.
2	Half	All information, installation or resource whose availability can be arrested person by 24 maximum hours.	All resource, information or installation in which the integrity is of half importance and has to guarantee.	Information, installation or resource described as of use semi-restricted. Only it can be used by internal personnel.
1	Low	This level covers all information, installation or resource whose availability can be arrested person by 48 maximum hours.	This level covers all information, installation or resource in which the integrity is not very important but has to guarantee.	This level covers all information, installation or resource described as of internal use. Only it can be used by internal personnel or users/customers.

The criteria that considers for the allocation of the values:

- The original cost of the active.
- The original value by loss of confidentiality, availability and integrity.
- The impact generated for the organisation by the years or suspension of the services.

F. Analysis of risk – inside an organisation the analysis of the risks allows us identify active, controls of security, criteria of design and evaluation of plans of contingency. The analysis of risks finds comprised by three elements that allow to give a value the risks inside the organisation: probability of occurrence of the risk, the impact of the risk and the determination of the risk.

1. *Probability of occurrence* of a threat – establishes under which circumstances the active will have value or needed protection, determined in base to statistics collected along the administration and considered the following:

- The importance of the active for the organisation.
- The ease of exploitation of a vulnerability in the active.
- The technical susceptibility of the vulnerability to the exploitation.

1.1. *Andvaluación of probability of risk* – makes by means of the identification of the threats, the active affected and the vulnerabilities, also took in account the frequency with which the threats occur.

In the table 3 defines the quantifications for the designation of the frequency of each one of the vulnerabilities found.

TABLE III
PROBABILITY OF OCCURRENCE

Level	Denomination	Description
76-100 %	Very Frequent	Repetitive events
51-75%	Frequent	Isolated events
26 -50 %	Occasional	Sucede Some time
0 -25%	Remote	Impossible that suceda

2. *Impact of the Risk* – defines like an eventuality inside the security of the information that can affect to more than an active inside the organisation, these impacts can be immediate or futures that would cause financial losses. The immediate impact can be direct when it needs the replacement of the active stray, configuration, installation or copy of support, the cost of the operations suspended because of the incident; or indirect when the affectation is the loss of opportunities by the damages produced in this team, cuando used resources that pugave to use in another part and the costs by interruption of the activities.

The criteria for the determination of the impact in the active are the following:

- The degree of affectation or the cost that would involve for the organisation if it produces some damage or the interruption of a critical process.
- Of agreement to the importance of the active of the institution.
- The brechas of security that exist so much to level of logical like physicist.

- The operations that make so much to the interior as to the outside.
- The financial value for the organisation if it suffers some emergency.

In the table 4 defines the values to determine the priorities of evaluation of the impact.

TABLE IV
PRIORITIES OF EVALUATION OF THE IMPACT

Impact	Value	Description
Low	1	When they do not affect the activities and the main systems work of normal form.
Half	2	When the damages are partial and give in the systems, does not affect to the operations.
High	3	When they see affected of direct way the operations and functions, the users and the computer systems.
Criticise	4	Loss of critical information, severe damages in the teams, Suspension of functions

3. *Determination of the Risk* – establishes by means of the the determination of the impact of the threats on the active critics by the probability of occurrence of each one of the threats. In the figure 3 observes of graphic way the determination of the levels of risk.

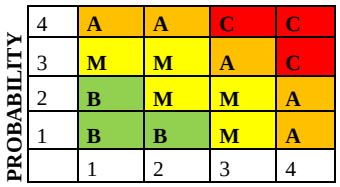


Fig. 3. Levels of Risk

- The red indicates us the critical risks (C)
- The orange does not indicate that they are high risks (A)
- The yellow are half risks (M)
- The green does not indicate the low risks (B)

G. Types of analysis of Risks - The estimate of the risk defines of agreement to different levels of detail depending on the criticidad of the active and vulnerabilities known. The estimate of risks can make of two forms: quantitative and qualitative.

Qualitative: When we use adjectives calificativos like high, low average, by means of these can describe the consequences or probabilities of occurrence of a risk

Quantitative: The quantitative estimate allows to give numerical values so much for the consequences as for the probability of occurrence, uses like source data of previous incidents.

H. Identificación of preventive controls – allow to offer efficient alternatives that minimise the apparition of vulnerabilities, these procedures have to be documented together with the causes that caused it and the actions taken.

It considers the following:

- The training of teams that offer support in case of a contingency.
- The association of solutions with each risk identified.
- Determine critical processes and the impact for the organisation if these fail.
- Identify a stray acceptable of information and services
- Keep updated the document where find the solutions and rules of implementation.

I. Strategies of Technological Protection - has to define a strategy of recovery that contain a guide of procedures for the recovery in front of the disaster, the election of the same will determine of agreement to the criticidad of the processes or applications, time of recovery and the security required. Dand agreement to the type of organisation exist different types of centres of recovery, to continuation details some types of centres hardware of backrest in remote headquarters.

In the table 5 determines the type of centres of recovery of information of agreement to the needs of each institution.

TABLE V
PROBABILITY OF OCCURRENCE

Centres ofR ecuperación	Compatibilidad	Cost of I nstalación
Hot Sites:	Total in software and hardware use immediate	Half high
Warm Sites:	Partial configuration of the primary centre, there is q expect for his use	Moderate
Cold Sites:	Basic infrastructure, electricity, rooms to install teams	Low
Duplicate centre:	Redundancia Of alone teams of the critical processes designed to go in in operation to the instant to having declared an emergency.	Andlevied

VII. DOCUMENTATION OF THE PROCESS

After having made the analysis of the risks and elaborate a series of recommendations in case of some eventuality or disasters proceeds to the documentation of the described previously in the stages. This document has to be drafted in a simple and intelligible language for all.

It has to contain the following information:

- Know the previous situation to the disaster.
- Have information of the risks.
- Identify processes and resources of Infrastructure of telecommunications that has to recover.
- Designation of responsibilities and solutions to make in case of contingencies.

Has to make a continuous review of the plan of contingency established, as so much the technology like the business grow, evolve and what in this moment is useful more forward will be obsolete.

For a suitable maintenance of the plan of contingency is important to consider the following:

- The needs of the business.
- The acquisition again hardware or development of new applications of software.
- The critical processes change of agreement to the needs of the business.

VIII. REALISATION OF PROOFS AND VALIDATION OF THE PLANS OF CONTINGENCY

The proofs in a plan of contingency allows us ensure that so much the team of recovery like the rest of the personnel have to know his responsibilities for the restablecimiento of the operating capacity of the network and the security of the information; the proofs have to contemplate the following information.

a) Verify that the information of the plan this correct and complete.
b) Evaluation of the personnel involved.
c) Evaluation of the coordination between the team of emergency and external components.
d) Evaluation of the capacity of recovery.
e) Evaluation of the general performance of the organisation after the recovery.

IX. NORMS AND STANDARDS OF SECURITY

IUNDER/IEC 27000 is a group of standards that provide a march of management of the security of the usable information by any type of organisation.

The ranks of numbering reserved by ISO goesn of 27000 to 27019 and of 27030 to 27044.

A. ISO 27000: it Contains terms and definitions that employ in all the series 27000. It is free, unlike thes other of the series, that have a cost.

B. ISO 27001: Published on 15 October 2005. It is lto main norm of the series and contains the requirements of the SGSI. It allows to establish conditions of transition for those companies certified.

C. ISO 27002: Published on 1 July 2007. It is a guide of best practices that describes the aims of control and recommended controls regarding security of the information. It is not certificable.

D. ISO 27005: Published on 4 June 2008. It establishes the guidelines for the management of the risk in the security of the information. It supports the general concepts specified in the norm ISO/IEC 27001 and is designed to help to the satisfactory application of the security of the information based in an approach of management of risks.

E. IUNDER 27011: Published to finals of 2008. It consists in a guide of management of security of the specific information for telecommunications, elaborated jointly with the ITU.

F. ISO 27031: Published in May of 2010. It consists in a guide of continuity of business regarding technologies of the information and communications.

G. ISO 27032: Published in February of 2009. It consists in a relative guide to the ciberseguridad.

X. CONCLUSIONS

The development of the design of a plan of computer contingency allows to know the latent vulnerabilities in infrastructure of network and services inside the institution, and puts to consideration of the authorities the respective correctivos to end to minimise the risks.

The identification, evaluation of the risks and stages of contingency in the active considered critics for the institution made in base to profiles of threats, considering the impact ocasionado if they materialise said risks.

They define recommendations for the control and administration of the network of the institution that allow to ensure the operating capacity of the network to the minimum of his capacity with the purpose to minimise economic losses and of reputation.

The training of groups of emergency in the computer department will allow greater organisation to the moment to give an answer in front of an incorrupción of services.

With the strategies proposed for the mejoramiento of the security of the information and the reduction of threats in the active critics will improve the efficiency and administration of the network and the proportionate services by the department of systems of the GAD of Antonio Ante.

Finally it concludes that, an institution provista of a plan of computer contingency goes to be prepared for unexpected events, take timely measures and efficient solutions.

XI. REFERENCES

[1] Agreement No. 166. (09 Of 2013). *Governmental diagram Of Security Of The Information (Egsi). I remove, Ecuador.*

[2] Areitio, J. (2008). *Security Of The Information (Computer Networks And Systems Of Information). Madrid: Learminig Paraninfo Sa.*

[3] Contraloría General Of The Republic. (2009). *Norms Tecnicas In Technologies Of Information And Communications. Obtained Of Http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/normas%20t%C3%To9c%20in%20you%20and%20comunics.Pdf*

[4] Hernández, I. J. (December Of 2005). *Methods And Political Of Backrest In Plans Of Contingency. Obtained Of Http://benjamin.davy.free.fr/auditoria/contingenciaybackupensi.pdf*

[5] Smith, R. (2010). Plans Of Contingency And His Audit.

[6] Institute Of the Sea Of Peru. (2012). *Plan Of Computer Contingency.*

[7] Katz, M. (2013). *Networks And Security. Alfaomega.*

[8] National Institute Of Standars And Technology. *(May Of 2010). Contingency Planning Guide For Federal Information Systems.*

[9] Ntc-Iso 27005. (S.F.). *Http://es.scribd.com/doc/124454177/iso-27005-espanol. Obtained Of Http://es.scribd.com/doc/124454177/iso-27005-espanol*

[10] Nte Inen-Iso/Iec 27002. (2009). *Technology Of The Information-Technical Of The Security-Code Of Practices For The Management Of The Security Of The Information. I remove, Ecuador.*

XII. BIOGRAPHYS

Narváez David. It was born in Ibarra-Ecuador on 26 October 1985. It obtained the title of Bachiller in Sciences in the 2003. Afterwards it obtained the degree of Engineer in Electronics and Networks of Communication in the 2012. At present Graduate of the Mastery in Technologies. It exerts from 3 years ago like Educational of Empowers it of Engineering in Sciences Applied Tecnica del Norte University.
Email: ldnarvaez@utn.edu.ec.

Méndez Karina. It was born in Ibarra-Ecuador on 20 October 1989. It obtained the title of Bachiller Technical with specialisation in Computing in the 2007, Colegio National "Ibarra". Toctualmente Egresado of the carrea of Engineering in Electronics and Networks of Communication in the Tecnica del Norte University**.**