Research paper on security and privacy policy

Law, Security

ASSIGN BUSTER

Introduction

The purpose of formulating the paper is to provide the readers a comprehensive formal policy for sensitive financial and health care data of LSS. Therefore, in this regard, it is important to understand the whole concept of security, it is essential to understand the various basic concepts that govern it, because otherwise it is not possible to establish a base of study.

Information Resources: computer equipment and telecommunications; systems, programs and applications as well as data and information in an organization. They are also known as " IT assets"

Threat: source or potential unwanted events can result in damage to computer resources of the organization incidents cause.

Risk: the likelihood of an adverse event occurs combined with its impact on the organization.

Basic principles of computer security: computer security is not a product, it is a process (Herath & Rao, 2009, pp. 106-25).

Policy Analysis

Bulgurcu, et. al., (2010, pp. 523-48) highlighted that the primary goal of security policy is to keep risks to a minimum of computing resources, -all resources- and thus ensure the continuity of operations of the organization while managing risk that computer to a certain acceptable cost. We will use techniques organizational structures, administrative, managerial or legal. The secondary objective of security and I stress that it is of our special interest from the point of view of preservation documentary is to ensure that documents, records and computer files of the organization always maintain their overall reliability. This concept varies according to different authors, documentary context and type of organization to which the information is associated. In an archival context and where we try to interoperate security approach with one of digital preservation, we can establish the reliability as the union of six essential characteristics:

permanence

accessibility

Availability

confidentiality (privacy)

authenticity (integrity)

acceptability [non-repudiation] (Siponen & Vance, 2010, pp. 487)

The characteristic of permanence will be associated to the extent that we can ensure that the document exists and is available for a considerable period, if necessary, eternally. It is associated with their presence, their existence, and they obviously depend on its protection, preservation and of course, the duration and continuity of its hardware. It is common to confuse this feature with that of accessibility, which has to do with the document, existing, can be accessed by us and be visible. Are two different concepts. We distinguish well between -the permanent storage safe " stay" - and future access-the " accessibility".

Regarding the first concept, the permanence depends on the permanent safe storage. To ensure the storage of digital objects, in this case file- documents required strategies, procedures and appropriate to create, operate and maintain long-term documentaries technical files. Therefore be designed and meticulously carry out these techniques and procedures for the conservation of both the documentary supports and their digital content: the information in the document itself and the metadata associated with it (Hur & Noh, 2011, pp. 1214-21). The preservation of the support, the bit string, structure and format gives permanence.

Future access to stored digital objects is another question. How to ensure that after been preserved in good condition we will be able to view or play these documents within the files within twenty, fifty or two hundred years? That is: how will ensure our ability to interpret and correctly reproduce the bitstream properly preserved? We must ensure that-having kept in good condition-we will be able to access: to see and / or reproduce these documents within twenty, fifty or two hundred years; i. e. we will be able to play the bitstream properly preserved.

Today and the concept of " permanent record", which consists of a series of strategies and techniques aimed at ensuring maximum interoperability, i. e. the architecture of the file systems of digital information for preservation is independent of handled the technology used to create them precisely to reduce the problem of accessibility. The archival technique known as " persistent object preservation" -persistent object preservation or " POP" -has intended to ensure that digital records remain accessible through the self-made of them, including formats, structural and technological, and so on, made independently of the hardware or software in which they operate (Weber, 2010, pp. 23-30).

Conclusion

As we conclude, one thing is that a document exists, remains in good condition, and another thing is that you can access and can view and analyze its contents. Depending on our ability to have these devices, programs, operating systems, formats, etc., will have access to those documents. There will be or not, " accessibility", regardless of " permanence". This is the meaning to be used usability regarding preservation and security. Do not confuse this term with the concept of " accessibility" and " usability" in the sense of the facilities that are added to certain sites Web so they can be accessed more easily by people with visual, such as special fonts more Large, color contrasts more pronounced, " a magnifying glass" on the virtual screen, and so on. That's another concept of " accessibility" and " usability" that has nothing to do with safety or preservation of information and should not be confused.

References

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

Hur, J., & Noh, D. K. (2011). Attribute-based access control with efficient revocation in data outsourcing systems. Parallel and Distributed Systems, IEEE Transactions on, 22(7), 1214-1221.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 34(3), 487.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer Law & Security Review, 26(1), 23-30.