Resumen

En este trabajo se muestra la contribución realizada al Cert Académico ESPE con el objetivo que se presente como servicio una solución para la prevención de perdida de datos (DLP). El trabajo desarrollado muestra la implementación de una herramienta para la aplicación de políticas de seguridad y la gestión de la fuga de información. La herramienta contiene 2 entornos de despliegue en los cuales se encuentran en ambientes de nube y local. El entorno de administración en donde se encuentra la consola de administración mediante el cual se realizan la gestión y manejo general de la herramienta. En la consola de administración se encuentran los apartados de configuración las políticas de seguridad que van a ser desplegadas, manejo de usuarios y de dispositivos finales además de los reportes de uso, mediante el agente en el entorno de usuario final, en lo cual es necesario la instalación del agente de comunicación mediante el cual se realiza la comunicación con la consola de administración que se encuentra en la nube con la maquina final que se encuentra de manera local. El agente es el encargado de recopilar el comportamiento del usuario en el dispositivo y envía la información a la consola, también ejecuta las acciones que se generan con las políticas de seguridad con el control del sistema operativo que lo hospeda. Para el desarrollo se utilizó la metodología Design Science, Scrum, y la herramienta Teramind DLP como software de implementación.

Palabras clave: prevención de perdida de datos, políticas, prevención, seguridad de la información

Abstract

This work shows the contribution made to the Cert Academic ESPE with the aim of presenting as a service a solution for the prevention of data loss (DLP). The work developed shows the implementation of a tool for the application of security policies and the management of information leakage. The tool contains 2 deployment environments in which they are in cloud and on-premises environments. The administration environment where the administration console is located, through which the management and general handling of the tool is carried out. In the administration console are the sections of configuration security policies to be deployed, user management and end devices in addition to the reports of use, through the agent in the end user environment, which requires the installation of the communication agent through which communication with the management console that is in the cloud with the final machine that is locally. The agent is responsible for collecting the user's behavior on the device and sends the information to the console, and executes the actions generated with the security policies with the control of the operating system that hosts it. For the development we used the Design Science methodology, Scrum, and the Teramind DLP tool as implementation software.

Keywords: data loss prevention, policies, prevention, information security