Sistema de control de cambios informáticos ajustado a la normativa IRAM ISO/IEC 27000

Maria Elena Ciolli, Porchietto Claudio
Departamento de informática
Del Instituto Universitario Aeronáutico
Córdoba, Argentina
Mciolli@gmail.com, Porchietto@gmail.com

Abstract
La reducción de los costos del equipamiento informático provocó que todo tipo y tamaño de organización haga uso de los mismos en un creciente número de áreas. Esto ha llevado a que cuenten con un importante volumen de equipamiento informático para llevar adelante su actividad. Por ende es cada vez menos viable el control manual de los activos informáticos.
En el trabajo "Rediseño e Implementación De Herramientas Informáticas Para La Auditoria De Sistemas En Red" presentado con anterioridad, se abordó a una solución para este problema, donde se propone con la herramienta Open-AudiT mantener una base de datos actualizada de todos los activos informáticos de la red.
La misma posee un problema. No brinda una trazabilidad de los cambios. Es por ello que se decidió trabajar en la creación de una nueva plataforma que explote la información recopilada por Open-AudiT. Para ello se llevó adelante la extrapolación del concepto de "Control de Cambios" de la Ingeniería del Software al control de cambios en el equipamiento informático mediante la construcción de un sistema web y de una serie de procesos que transforman los datos recibidos de Open-AudiT en información para el control de cambios del equipamiento informático. Junto con ello se generó un total de 20 reportes con 4 pantallas adicionales de ingreso de datos, para realizar una búsqueda personalizada, ajustados a lo requerido por la norma IRAM ISO/IEC 27000.

Palabras
Normativas, IRAM ISO/IEC 27000, Open Audit, Acceir, LDAP.

Introducción

El proyecto se originó al detectar un problema común a todas aquellas organizaciones que tienen gran cantidad de equipamiento informático en distintas plataformas.
Muchos de los cambios que ocurren en estos equipos no son gestionados lo que se traduce en ineficiencia y gastos innecesarios para la organización.
Este problema es muy común durante el desarrollo de sistemas informáticos[1], por lo cual la Ingeniería de Software lo trata mediante la gestión de la configuración del software que implica identificar, organizar, y controlar las modificaciones que sufre el software que construye un equipo de desarrollo, siendo la meta maximizar la productividad minimizando los errores.
Por otra parte, existiendo la normativa IRAM ISO/IEC 27000, se decidió ajustar el nuevo sistema a sus requerimientos. Las normas ISO nos permiten asegurar la calidad y nos otorgan una serie de procedimientos que garantizan la buena ejecución de los procedimientos en todos los campos de la organización, esto no sólo mejora la credibilidad y asegura la confianza en la organización, sino que también ayuda a cumplir con las regulaciones y vuelve a la organización más competitiva. Las secciones de la norma que deseamos cubrir en este proyecto son las referidas al Inventario de Activos y sus Propietarios (secciones 7.1.1 y 7.1.2) y Gestión de Incidentes (13.1.1) [2]
El problema planteado se basa en que las personas con acceso al equipamiento informático generan situaciones en donde se hace indispensable la gestión del equipamiento de la manera más eficaz y eficiente posible, ya sea para solicitar un cambio o por realizar un cambio no previsto.
Una parte importante de la solución que fue resuelta y explicada con anterioridad [3] es detectar y almacenar el estado actual del equipamiento informático.

Debe entenderse por cambio del equipo informático a cualquier cambio tanto de un componente de hardware como un componente de software. Ahora bien, qué se debe entender por un cambio de un componente. Cambiar la versión de un programa o el espacio libre en disco no es un cambio. Esto sólo son actualizaciones del estado de los componentes. Por ende se los trata de manera diferente. Pero el cambio en el número de serie de un disco o la aparición de un software nuevo sí constituye un cambio a gestionar.

La normativa [2] nos expresa que la gestión de activos reposa sobre tres grandes pilares:

- Inventario de los activos: se necesita saber con precisión qué activos tiene la organización y por qué son importantes. La normativa recomienda clasificarlos según su nivel de importancia y, además, tener este inventario actualizado.
- Pertenencia de los activos: se necesita saber con exactitud quién está a cargo de los activos de la organización, sus responsabilidades y permisos sobre el mismo.
- Gestión de Incidentes ocurridos en los activos auditados: se necesita conocer lo antes posible cualquier incidente que ocurra en el sistema auditado y que involucre algún activo.

Elementos del Trabajo y metodología

El deficiente control de los equipos informáticos produce los siguientes eventos:

- Los componentes de un equipo pueden ser sacados del interior del mismo por personas no autorizadas. Estos casos mayormente son robos de componentes que afectan al patrimonio de la organización.
- Los empleados instalan software ilegal en sus estaciones de trabajo sin pedir autorización, lo que puede derivar en consecuencias legales para la organización al no poseer licencias de estos programas.
- El software no autorizado con lleva la pérdida de información sensible para la empresa.
- En ocasiones el usuario reemplaza componentes de equipamiento informático (memorias, discos, etc.) sin previa verificación por el personal técnico correspondiente generando gastos innecesarios por compra de componentes inadecuados.

¿Qué es ACCEIR?

Acceir es una solución que permite gestionar los cambios ocurridos en el equipamiento informático dentro de una red. Es el acrónimo de **A**utomatización del **C**ontrol de **C**ambios para el **E**quipamiento **I**nformático en **R**ed.

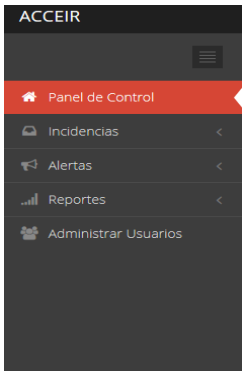

Figura 1 Menú principal.

El sistema provee los siguientes grupos de funcionalidades:

- **Panel de Control:** muestra un resumen de las principales métricas del sistema. Es visible para todos los perfiles.
- **Incidencias:** agrupa las funcionalidades relacionadas con las incidencias ya sea creación, edición y listado de las mismas.
- **Alertas:** contiene las opciones para acceder a los listados de alertas previstas y no previstas. Estas opciones son solo visibles para los perfiles de Auditor y Jefe Auditor.
- **Reportes:** permite acceder a los diferentes reportes del sistema. Solo disponible para Auditor y Jefe Auditor.
- **Administra Usuarios:** permite acceder a la gestión de usuarios dentro del sistema. Solo disponible para el Jefe Auditor.

- **Barra superior:** el icono de un sobre de correo se muestra el notificador de novedades el cuál lista las siguientes novedades ocurridas en el sistema. También se listan las incidencias creadas por cambios no previstos que siguen sin cerrar. Esto es de gran ayuda a la hora de dar una rápida respuesta.

Existen tres perfiles de usuario.

- Jefe de Auditores: Tiene acceso a todas las funciones del sistema como gestionar cambios de componentes en los equipos, designar auditores, visualizar incidencias, generar reportes y administrar usuarios.
- Auditor: Tiene acceso a un número limitado de funciones del sistema como realizar una auditoria previamente designado por el Jefe de Auditores, visualizar alertas y reportes. No puede crear usuarios.
- Usuario: Solo puede realizar una gestión de cambio o consulta sobre algún componente.

Para gestionar los cambios el sistema utiliza la siguiente estructura:

1) Gestión de consultas de usuario que puedan derivar en cambios en equipos.
   a) Usuario: genera un ítem Consulta de Configuración (CC) para obtener información sobre la configuración de equipo informático.
   b) Auditor: recibe la CC y responde las inquietudes planteadas.
2) Gestión de cambios
   a) Usuario: solicita cambio/actualización de componente, cargando n° Ideti y n° de Solicitud de Gastos a través del campo mensaje de una Solicitud de Cambio de Equipo Informático (SCEI).
   b) Auditor: autoriza el cambio solicitado por el usuario, informándolo al Departamento Técnico para que proceda con el mismo.
   c) Auditor: carga en el campo mensaje n° de Orden de Compra y n° de Nota de Provisión o n° de Nota de Entrega informado por el Departamento Técnico luego de actualizar componente en la OC.
   d) Auditor: marca cambio/actualización como realizado en la OC.
3) Gestión de cambios detectados automáticamente
   a) Herramienta de Auditoría: detecta cambio en equipo informático y propaga la novedad.
   b) Herramienta de control de cambios: detecta novedad sobre el cambio y:
      i) Si el cambio está asociado a una OC: actualiza información de la misma y la cierra.
      ii) Si el cambio no está asociado a una OC: se genera una Alerta de Cambio No Previsto (ACNP).
4) Gestión de ACNP
   a) Auditor: validación de los cambios descriptos en la ACNP mediante un examen físico del equipo involucrado. Se debe determinar si:
      i) Se revierten los cambios, por lo que se genera una OC.
      ii) Se mantienen los cambios en el equipo y se cierra la ACNP.

Los puntos 1 a y 2 a nos obliga a tener todos los usuarios registrados por lo que se decidido no implantar la gestión de usuarios dentro del sistema sino derivarla a LDAP. Cada usuario tiene asociado un perfil asociado, el cual determina el nivel de acceso al sistema.

Por fiabilidad se decidió que el sistema tenga los dos métodos de gestión de usuarios. Usuarios locales, y usuarios de dominios.

El proceso con que logra ingresar un usuario es:

1. Se ingresa un nombre de usuario y una clave.
2. El sistema verifica en la base de datos si el usuario existe y si el hash de la clave ingresada coincide con el almacenado.

3. Si los datos son correctos, se accede al sistema y se determina el perfil.
4. Si el usuario no está en la base de datos a través de las funciones LDAP [3] se realiza una búsqueda en el dominio para determinar si el usuario existe y si la clave coincide con la almacenada. Cabe destacar que sólo se ingresa el fragmento antes del "**@**" ya que el dominio se define en la configuración del sistema.
5. Si la búsqueda fue exitosa, devuelve el nombre del usuario y un perfil del grupo al que pertenece, el cual determina se mapea a lo perfil de usuario del sistema el tipo de acceso al sistema.

Resultados

Teniendo como fuente de información la base de datos de Open-AudiT y el proceso de gestión de incidentes de ACCEIR se generaron reportes que facilitan atacar a los tres pilares de la normativa.

Sobre el primer pilar, Inventario de los activos, se generaron 7 reportes y 3 pantallas de ingreso de datos:

- Máquinas Auditadas.
- Máquinas Auditadas por Red.
- Información Básica de Máquina.
- Hardware de la Máquina.
- Software de la Máquina.
- Pantalla para Ingresar Datos Manuales.
- Ingresar datos para Buscar Máquina por UUID.
- Buscar Software Instalado.
- Software Instalado Gráfico.
- Software Instalado en Detalle.

Sobre el segundo pilar, pertenencia de los activos, se generaron 6 reportes y 1 pantalla para el ingreso de datos:

- Historial de Asignaciones.
- Personas Asentadas en el Sistema.
- Personas Asentadas en Detalle.
- Máquinas sin Datos Manuales Cargados.
- Personas Asentadas por Departamento.
- Ingresar Datos para Buscar Persona.
- Persona Buscada.

Sobre el tercer pilar, Gestión de Incidentes ocurridos, se generaron 6 reportes:

- Incidentes de una Máquina.
- Incidentes en Máquinas Auditadas.
- Todos los Incidentes.
- Incidentes en Máquinas Auditadas por Tipo.
- Todos los Incidentes del Tipo.
- Todos los Incidentes por Tipo y Red.

Discusión

Si bien esta implementación está inspirada en las normativas IRAM/ISO 27000 la herramienta no es suficiente para certificar la organización. Existen apartados dentro de la misma que hablan de la seguridad física de los elementos de la red que no son contemplados dentro de la herramienta ya que no es su fin.

Conclusión

La norma IRAM ISO 27000 y afines fueron de gran ayuda a la hora de fijar los requerimientos del sistema. Así también lo fue el paradigma de gestión de cambios de ingeniería de software para desarrollar los procedimientos para gestionar un cambio.

Con el sistema Acceir acoplado al sistema Open-AudiT se tiene un control eficaz y de rápida respuesta a los cambios de los todos los componentes de la red.

Los cambios que sean requeridos tienen un curso formal y quedan asentados dentro del sistema dando una clara comunicación entre usuarios y administradores.

Los cambios no previstos son alertados inmediatamente los auditores dando una rápida respuesta y minimizando fallos de seguridad.

Los informes que proporciona abarcan desde resúmenes globales de la red a los más detallados donde se puede examinar el hardware y software específico de cada estación en particular.

Referencias

[1] Roger S. Pressman. Ingeniería del Software; un enfoque práctico. Quinta Edición. Madrid: McGraw-Hill 2002.

[2] ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems – Requirements

[3] "Rediseño e Implementación De Herramientas Informáticas Para La Auditoria De Sistemas En Red", Porchietto Claudio, Ciolli Maria elena. CoNaIISI 2014.

[4] https://es.wikipedia.org/wiki/Protocolo_Ligero_de_Acceso_a_Directorios.

[5] **https://es.wikipedia.org/wiki/Auditoria_informatica**

Datos de Contacto:
Claudio Porchietto. Instituto Universitario Aeronáutico. Avenida Fuerza Aérea 6500 Código Postal 5022. Porchietto@gmail.com