Generador de Órdenes de Trabajo Automatizadas sobre el Equipamiento Informático ante Eventos Detectados para la Protección de la Red

Trabajo Final de Grado - Ingeniería en Informática
Instituto Universitario Aeronáutico

Autora: Nabila Melania Nahir Gudiño Ochoa

Asesora: Ing. Mgter. María Elena Ciolli

Agradecimientos

Agradezco a mis padres y mis amigos que de una u otra forma me acompañaron y dieron la fuerza para perseverar a lo largo de mi carrera universitaria lo cual me lleva el día de hoy a estar presentando este trabajo final de grado.

También agradezco a mi asesor de tesis, la Ing. Mgter. María Elena Ciolli, por sus conocimientos, la motivación que me brindó, sus palabras de ánimo y su paciencia para ser mi guía durante el desarrollo de este proyecto.

Dedicatoria

Dedico de manera especial este trabajo a mis padres ya que ellos fueron mi principal cimiento en la construcción de mi vida, tanto personal como profesional. Sentaron las bases de mi sentido de responsabilidad, ética y moralidad, además de los deseos de progreso y superación. Me criaron como una niña llena de imaginación e inventiva lo cual me llevó a ser la mujer que soy ahora, llena de proyectos en mi futuro a corto y largo plazo. No estaría donde estoy si no fuera por su apoyo incondicional, es por eso que dedico este trabajo final de grado a ellos.

Índice de Contenido

Abstracto

Hoy en día es común el uso de dispositivos informáticos en todas las organizaciones a fin de automatizar tareas administrativas y procesos organizacionales. El problema es que no se tiene presente que esa dependencia provoca que cualquier cambio no previsto en esos equipos llegue a afectar por completo el normal funcionamiento de la organización.

La auditoría informática determina si un sistema es capaz de salvaguardar los activos organizacionales, mantiene la integridad de los datos, utiliza eficientemente los recursos y cumple con las regulaciones establecidas. Si un sistema puede cumplir a lo largo del tiempo con todos estos requerimientos, entonces es un sistema seguro.

En el Instituto Universitario Aeronáutico se posee un sistema de auditoría remota para los equipos de la red. Se relevan los equipos conectados a la red y sus componentes hardware y software. El sistema además es capaz de detectar cuándo se cambia un componente, es decir cuando se "desenchufa" un hardware como una memoria RAM o cuando se actualiza la versión de un software específico.

El sistema existente cumple con el objetivo que se planteó para su desarrollo: puede detectar equipos, revelar cambios y notificarlos; pero le faltan dos componentes cruciales por cumplir que lo convertirían en un sistema sumamente útil:

1. **Política de Seguridad:** el sistema no guía al auditor que debe atender un incidente sobre cómo proceder ante ese tipo de situaciones.
2. **Personalización:** el sistema cubre todos los componentes que pueden auditarse y no consideró la posibilidad de que el Jefe Auditor pueda necesitar una configuración diferente.

Esta revelación fue la base del presente Trabajo Final de Grado. Se determinó la necesidad de tener una Política de Seguridad de la Información Informatizada y que el sistema fuera capaz de tener en cuenta esta política a la hora de generar alertas. Además se vio la necesidad de poder personalizar el sistema y decidir qué alertas consideramos importantes y cuáles no, por ejemplo, en las notificaciones por incidentes de componentes hardware, es importante tener alertas si un equipo en una auditoría tiene una memoria RAM menos respecto a la auditoría anterior sin haber notificado ese cambio. Las modificaciones descriptas serán implementadas por el presente Trabajo Final de Grado mediante el diseño y desarrollo de módulos que serán agregados al sistema existente.

Introducción

Antecedentes

Se posee un sistema capaz de relevar todo el hardware y software instalado en cada equipo conectado en la red y que además es capaz de informar sobre la existencia de nuevo equipamiento informático (equipos y dispositivos de red) agregado en la red que aún no ha sido auditado.

Se dispone de un sistema que emite alertas en tiempo real en caso de ocurrir cualquier cambio en cuanto a hardware y software en los equipos presentes en la red. Dichos cambios los divide en alertas programadas (donde el usuario realiza un pedido de cambio y éste es autorizado) y no programadas (cuando el cambio no fue pedido ni autorizado con anterioridad).

Los sistemas mencionados en los párrafos anteriores poseen cada uno una base de datos independiente que conserva los valores históricos.

Se dispone de la serie de Circulares Informáticas utilizadas por la Institución, emitidas por la Fuerza Aérea Argentina entre los años 1997 y 2015, las cuales tratan sobre temas de seguridad de la información en los equipos informáticos de la red interna.

Situación Problemática

Luego del relevamiento realizado a través de entrevistas con integrantes del departamento de sistemas se detectó que aunque el sistema utilizado cumplía con su cometido, dado que el sistema solo informa a los auditores sobre cualquier anomalía en la red y no toma decisiones respecto a esas anomalías, llega un momento en que los auditores tienen demasiadas alertas por atender y, en la cantidad, puede que ignoren una alerta crítica que queda perdida entre numerosas de alertas triviales.

La problemática descrita se ve reflejada en las situaciones que se detallan a continuación:

- Los auditores deben estar pendientes de una lista surtida de alertas triviales y críticas debido a la imposibilidad de poder pre-filtrar las alertas que van a ser generadas por el sistema.
- Como se sobrecarga a los auditores de información, puede que en su necesidad de solucionar las numerosas alertas del sistema, mecanicen sus acciones. Esto es sumamente peligroso porque cuando una acción se vuelve repetitiva y la persona a cargo se acostumbra a tomar cierta acción “por defecto” al detectar ciertos patrones similares, puede descuidar algunas características propias de la alerta actual que la difieren sustancialmente de una anterior y que, de ser pasadas por alto, podría dejar a la red y los datos en una situación vulnerable.
- Las alertas realmente críticas que no son atendidas a la brevedad (tomando algún tipo de acción correctiva) podrían traer consecuencias en la estabilidad e integridad de la red y sus datos.

- No existe una política de acciones a tomar en caso de que ocurra alguna de estas alertas por lo que cualquier solución que se proponga depende de la experiencia de los auditores.

Finalmente se detectó que estos problemas se originan en dos puntos principales que se tratarán en este trabajo final de grado:

- la falta de una política de seguridad que detalle las acciones que se deben tomar ante un evento riesgoso.
- un sistema que implemente dicha política para aquellas situaciones cotidianas y triviales.
- un sistema que pueda ser personalizado por el Área de Auditorías para ayudar a filtrar datos poco relevantes para el proceso de protección de la red y los datos.

Objeto de Estudio

El objeto de estudio del presente Trabajo Final de Grado está compuesto por los siguientes puntos:

- Análisis de la herramienta de auditoría informática automática que forma parte del proyecto MASI haciendo énfasis en los siguientes puntos:
  - Arquitectura de la herramienta de auditoría.
  - Definición de nuevas fuentes de información que ayudarán a filtrar los datos almacenados de manera eficiente.
- Análisis de la herramienta de auditoría informática automática que forma parte del proyecto Acceir haciendo énfasis en los siguientes puntos:
  - Arquitectura de la herramienta de auditoría.
  - Formas de obtención de los datos y manera en que se generan las alertas en el sistema.
  - Definición de nuevos tipos de alertas según lo definido en este Trabajo Final de Grado
- Análisis de la normativa IRAM ISO/IEC 27002 y las Circulares Informáticas emitidas por la Fuerza Aérea Argentina, utilizadas por el Instituto Universitario Aeronáutico.
- Diseño e implementación de una Política de Seguridad basada en la normativa IRAM ISO/IEC 27002 y las Circulares Informáticas emitidas por la Fuerza Aérea Argentina, utilizadas por el Instituto Universitario Aeronáutico.
- Diseño e implementación de nuevos tipos de alertas según las especificaciones definidas en la Política de Seguridad listadas a continuación:
  - Software Requerido
  - Software Prohibido
  - Software Sensible
  - Hardware Sensible
  - Auditorías Requeridas
  - Versión de Sistema Operativo
- Análisis de los beneficios que se obtendrán como resultado de la implementación de la solución.

Campo de Acción

El campo de acción del proyecto se basa en la definición y creación de una Política de Seguridad la cual sienta sus bases en lo expresado en la normativa IRAM ISO/IEC 27002 y la serie de Circulares Informáticas emitidas por la Fuerza Aérea Argentina, utilizadas en el Instituto Universitario Aeronáutico para luego implementarla en la actual herramienta de auditoría informática Open-Audit y Acceir utilizada en el proyecto MASI mediante el diseño y desarrollo de nuevas alertas basadas en la Política de Seguridad ya definida.

El presente Trabajo Final de Grado recorre a lo largo de su desarrollo las siguientes disciplinas:

- Ingeniería de Software, de donde tomamos el concepto de control de cambios que forma parte de la Gestión de la Configuración.
- Auditoría Informática, cuyo estudio nos va a permitir comprender el propósito del proyecto MASI.
- Seguridad Informática, citada varias veces en la serie IRAM ISO/IEC 27000 donde expone la necesidad de control de los equipos de una red para evitar que la misma quede desprotegida y sus datos y equipos queden comprometidos.
- Base de Datos, debido a que la información está almacenada en dos bases de datos que tienen que ser manipuladas para poder obtener la información necesaria.

Objetivo del Proyecto

Objetivo General

El objetivo del presente Trabajo Final de Grado es implementar una Política de Seguridad para la Información Informatizada. Para lograr esto se estudiarán las normativas IRAM - ISO/IEC 27000 que hablan del tema, Políticas de Seguridad emitidas para otras instituciones y las Circulares Informáticas utilizadas por el Instituto Universitario Aeronáutico que le sirve de marco para las decisiones respecto a infraestructura y auditoría informática. Finalmente esta política se utilizará para realizar modificaciones al sistema actual de auditoría remota para que éste sea capaz de aplicar la nueva Política de Seguridad.

Objetivos Específicos

Los objetivos específicos definidos para el presente Trabajo Final de Grado son los siguientes:

- Estudio de sugerencias expuestas por la serie de normas ISO 27000 para solucionar esta problemática.
- Definición de una Política de Seguridad de la información basada en la serie de circulares CI 1997 a CI 2015.
- Análisis de las tablas necesarias para este proyecto de la herramienta OpenAudiT para auditoría remota de hardware y software.

- Análisis de las tablas necesarias para este proyecto de la herramienta ACCEIR de control de cambios de hardware y software instalado.
- Desarrollo de un módulo para procesamiento de información obtenida del Proyecto MASI, OpenAudit, Acceir y syslog.
- Definición de órdenes de trabajo del sistema las cuales se dividirán en: acciones automáticas realizadas por el propio sistema de forma remota y acciones asignadas a auditores humanos.
- Desarrollo de un módulo para la realización de las órdenes de trabajo mencionadas en el punto anterior.

Beneficios Esperados

Se sabe que los datos del equipamiento informático de la red son datos sensibles y es necesario que se proteja de cualquier posible intrusión. Si bien el sistema actual posee un sistema de alertas no previstas que informa a los auditores humanos si se produce algún cambio en algún dispositivo en la red, el mismo carece de una política de seguridad establecida que diga a los auditores qué deben hacer ante estas situaciones.

Se espera que la redacción de la Política de Seguridad de la Información oriente a los auditores sobre qué acciones deben tomar ante la aparición de alertas no previstas.

Además, la Política de Seguridad de la Información será la base para crear los nuevos módulos facilitadores para creación de filtros personalizados los cuales se espera que ayuden a disminuir la cantidad de alertas al evitar que se generen alertas triviales.

Finalmente se espera que con la disminución de la cantidad de alertas generales, se logre aumentar el tiempo que los auditores pueden dedicarle a cada alerta individual y, de esa manera, lograr un tratamiento más personalizado.

Delimitación del Proyecto

El proyecto implicó el estudio del actual sistema de auditoría presente en el Instituto Universitario Aeronáutico el cual estaba formado por la herramienta Open Audit y Acceir.

No se describe el funcionamiento detallado, características específicas, ventajas y desventajas, ni aplicación de ninguna de las herramientas previas al presente Trabajo Final de Grado, solo se explicará brevemente lo necesario para exponer el funcionamiento de las mejoras brindadas por este Trabajo Final de Grado.

No se describe la implementación o desarrollo de la herramienta de auditoría sobre las diferentes plataformas, ni se modifica la funcionalidad existente en la misma a excepción de aquellas en relación a la obtención de datos. Solo se describen los cambios necesarios para la configuración de las funciones aportadas por este trabajo de tesis.

No se describen aquellos pasos de configuración necesarios para la implementación de la solución (instalación de sistema operativo, servidores de

base de datos, servidor web, configuración de firewalls, etc.).Tampoco se analizan casos específicos de errores cometidos por dicha problemática, solamente se mencionan como parte del problema inicial.

Lo que sí se describe, son los procesos de ejecución que la solución requiere, ventajas obtenidas luego de la implementación de la solución actual, modificaciones sobre el sistema anterior en vistas de mejoras en su funcionamiento y utilidad para el equipo de auditoría.

Aporte Práctico

En la actualidad los equipos informáticos son una herramienta presente en la mayoría de las organizaciones. En aquellas con un número considerable de equipos y de personal se genera una necesidad de control estricto en cuanto al uso de los equipos institucionales para evitar intrusiones en la red que causen pérdida de información, deterioro del rendimiento de la red, deterioro físico de los equipos institucionales, por nombrar algunos problemas.

La relevancia social de este proyecto viene dada en la ayuda que se aporta al equipo de auditores que deben atender numerosos casos por día de discordancias entre lo que sucede en las redes que auditan y lo permitido por las políticas institucionales.

Los resultados obtenidos van a estar disponibles en el corto y mediano plazo y se verán reflejados en la facilidad que tendrá el equipo auditor en mantener a los equipos de las redes auditadas dentro de los márgenes fijados por la política de seguridad utilizada por la institución, esto es debido a que el mismo sistema pondrá en aviso al equipo auditor cuando algún equipo esté infringiendo alguna política y le recomendará acciones a seguir para proteger al resto de los equipos de la red.

Aporte Teórico

Se estudiaron las normativas vigentes para la auditoría de equipos en una red informática y el manual de buenas prácticas contenidos en la serie de normativas IRAM – ISO/IEC 27000.

También se estudiaron las tecnologías, arquitecturas y paradigmas utilizadas por la solución desplegada en la institución (WEB, HTML5, Web Services, REST, etc.) con el fin de no complejizar la mantenibilidad del proyecto. De esta manera el proyecto estará compuesto por varios módulos de programación y arquitectura similar a la inicial, lo cual lo convierte en un sistema de fácil mantenimiento y permitirá la adición de módulos nuevos o modificación de los existentes sin agregar mayor complejidad.

La gran cantidad de equipos informáticos existentes en las organizaciones actualmente hace que la problemática detectada sea común a muchas de ellas, por lo que las conclusiones y soluciones alcanzadas pueden ser fácilmente replicadas.

Método de Investigación

Para la realización de este proyecto se consideró que la opción que mejor se adapta era el método Hipotético-Deductivo ya que permite plantear una hipótesis que puede analizarse de manera deductiva o inductiva para luego ser comprobada de manera experimental. Con esta elección se busca que el desarrollo teórico esté siempre relacionado con la realidad y no pierda sentido.

La deducción parte de premisas generales para llegar a lo particular. La ventaja de su uso se basa en que luego de seguir una secuencia de pasos simples y lógicos se pueden descubrir detalles que, de otra forma, podrían ser pasados por alto y luego generar fallas al utilizar la solución.

La inducción, por el contrario, parte del estudio de lo particular para llegar a conclusiones generales. Este método es útil para lograr pensar y generar soluciones que puedan ser personalizables ya que no fueron diseñadas para resolver un solo problema en particular, sino que fueron pensadas para solucionar una serie de problemas más generales con características comunes.

Por último, la experimentación científica va a permitir corroborar las conclusiones alcanzadas con los métodos anteriores lo que aumenta la seguridad de los resultados de la investigación. Este método permite la modificación de variables lo que ayuda a una mejor detección de errores y una mayor calidad de la investigación.

En este proyecto se utilizaron los conceptos del método Hipotético-Deductivo en las siguientes etapas:

- Se aplicó la observación para entender la problemática en el Marco contextual y Marco teórico. Como resultado de esta observación se generó una hipótesis.
- Luego, en el Marco teórico, se generó un modelo para validar la hipótesis.
- Al concretarse el modelo, se pudo verificar la hipótesis.

Enfoque Metodológico

Para la realización de este proyecto se consideró que la opción que mejor se adapta era la metodología ágil SCRUM ya que permite crear una lista de entregables que ayudará a organizar no sólo el proyecto en general, sino para facilitar la creación de módulos que sean totalmente independientes entre ellos.

En la etapa inicial se analizó la problemática planteada para obtener una mejor visión del problema.

Como segunda instancia se analizó de manera exhaustiva la normativa IRAM - ISO/IEC 27000 con el fin de entender cuáles son los puntos esenciales para poder definir y desarrollar una política de seguridad que se adapte a las circulares informativas que regían las auditorías de la institución. Esta sería la base de los requerimientos de las mejoras para el sistema de auditoría.

En tercera instancia, se analizó el sistema de auditoría que había sido desplegado. Se estudió desde cómo había sido diseñado y desarrollado (tecnologías y arquitecturas), hasta la solución que brinda y las ventajas que

aporta al equipo de auditores. Se prestó especial atención en cuáles necesidades había cubierto de manera exitosa y cuáles dejaba descubiertas.

La cuarta etapa consistió en el desarrollo de una solución utilizando las tecnologías y arquitecturas analizadas en la etapa anterior, teniendo en cuenta las necesidades no cubiertas por el sistema de auditoría actual y haciendo énfasis en los requerimientos definidos en la segunda etapa luego del estudio de la normativa.

En la etapa final se implementó la solución final desarrollada sobre un servidor virtual. Cada una de estas etapas se subdividió en otras más pequeñas para ir generando entregables.

Desarrollo

Auditoría Informática

Introducción a la Auditoría

Se define auditoría como un examen sistemático a personas, organizaciones, sistemas, procesos, proyectos o productos. Es importante que sea realizado por una persona, o grupo de personas, que sea independiente del sistema auditado ya que su objetivo es emitir una opinión independiente y competente, es decir, que evite parcialidades y sea lo más objetiva y certera posible.

Auditoría Informática

Una Auditoría Informática, por su parte, es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informático, es decir, computadoras personales, servidores, el entorno en el que se encuentran, las personas que los utilizan, etc., es capaz de cuidar los activos empresariales, mantener la integridad de sus datos y utilizar eficientemente los recursos que tiene disponibles.

Tipos de Auditoría Informática

La Auditoría Informática permite la posibilidad de realizarse de forma tanto interna como externa, siempre buscando mantener el mayor nivel de objetividad posible:

- **Auditoría Interna:** es aquella que se realiza por el personal de la empresa o institución.
- **Auditoría Externa:** es aquella realizada por empresas dedicadas a este tipo de actividad que son contratadas por la empresa o institución que necesita la auditoría. Normalmente este tipo de auditoría realizan una serie de pruebas que buscan determinar si la empresa o institución cumple con determinados objetivos o estrategias y luego se proponen los cambios necesarios para lograr certificar cierto nivel de seguridad.

La Auditoría Informática puede realizarse en el nivel que se necesita, por ejemplo a nivel organización, un área específica o un departamento específico. En cualquier nivel que se realice, se pueden aplicar los siguientes tipos de auditoría informática:

- Auditoría al ciclo de vida del desarrollo de un sistema.
- Auditoría a un sistema en operación.
- Auditoría a controles generales (gestión).
- Auditoría a la administración de la función de informática.
- Auditoría a los equipos informáticos.
- Auditoría de redes.

Auditoría Informática Remota

El concepto de auditoría informática remota se basa en el uso de herramientas para el control remoto del hardware y software de una red informática, con la finalidad de obtener un informe que permita detectar los cambios, actualizaciones de hardware y software experimentados por cada una de las estaciones de trabajo que forman parte de esta red.

Proyectos Previos sobre el que se basa este Trabajo Final de Grado

Proyecto M.A.S.I. - Open Audit

M.A.S.I. es un proyecto desarrollado para el Ministerio de Defensa de la Nación destinado al monitoreo y control remoto del hardware y software de cada una de las estaciones de trabajo que integran una red dentro de una organización, obteniendo automáticamente información sobre los cambios en la configuración de cada uno de ellos.

Esta herramienta buscar recolectar de manera remota y automática la siguiente información disponible en los equipos informáticos de una organización:

- **Datos de componentes de hardware:** procesador, placa base, memoria, placa de video, adaptadores de red, periféricos, módems, dispositivos multimedia, etc.
- **Datos de componentes de software instalado:** sistema operativo, aplicaciones instaladas, motores de base de datos, programas autoejecutables, seguridad del equipo, etc.

Este proyecto utiliza Open Audit como herramienta base para obtener la información de la configuración de los equipos de manera automática. Esta aplicación es open source y está desarrollada bajo PHP, y permite auditar los componentes de una red. Sus principales características son:

- Auditoría de Hardware y de Software
- Auditoría de dominios Windows.
- Brinda soporte para Linux
- Audita dispositivos IP y otros componentes de red, no necesariamente tienen que ser computadoras.

Proyecto Acceir

Acceir es un proyecto nacido como un Trabajo Final de Grado. Tiene como finalidad brindar una solución que permite gestionar los datos generados por una herramienta de auditoría informática remota de manera que se pueda llevar a cabo un control de cambios en equipamiento informático de manera eficiente.

Particularmente en la Institución, la herramienta Acceir utiliza los datos recogidos por la herramienta Open Audit para lograr los siguientes:

- **Detección de cambios:** es un proceso que se encarga de revisar los datos de auditoría actual a fin de detectar modificaciones en los componentes de los equipos.
- **Gestión de cambios:** analiza los cambios detectados en los componentes y determina si los mismos son cambios previstos o no.
- **Generador de alertas:** están asociadas a un cambio ocurrido o por ocurrir en un equipo por lo que pueden ser alertas previstas o alertas no previstas.
- **Generador de incidencias:** son entidades asociadas a la gestión de los cambios en los componentes. Pueden ser generadas por un usuario o por el proceso de gestión de cambios de manera automática al detectar un cambio no previsto. Los diferentes perfiles de usuario interactúan con la gestión de cambios a través de las incidencias.

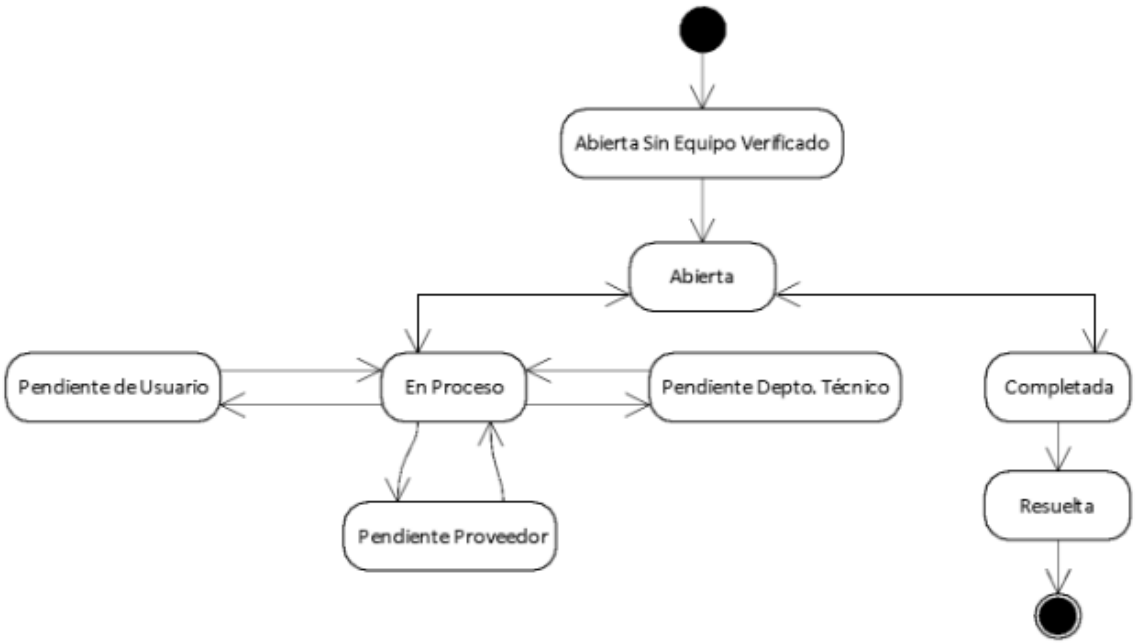
Diagrama de Estados de un Incidente en Acceir

El sistema Acceir gestiona los diferentes cambios en el hardware a través de incidencias sin importar si los cambios son previstos o no. Cada una de estas incidencias tiene un estado actual que determina los posibles estados futuros.

Los estados en las incidencias representan la siguiente información:

- **Abierta Sin Equipo Verificado:** es el estado inicial de la incidencia al momento de crearse.
- **Abierta:** indica que un auditor ha determinado que el equipo seleccionado por el usuario creador en la incidencia es correcto.
- **En Proceso:** indica que se está trabajando sobre la incidencia.
- **Pendiente de Usuario:** cuando el avance de la resolución de la incidencia queda supeditado a una acción que debe realizar el usuario que creo la incidencia.
- **Pendiente Proveedor:** cuando no se puede avanzar con la resolución de la incidencia hasta obtener una respuesta de un proveedor.
- **Pendiente Depto. Técnico:** el estado indica que se debe esperar una acción del departamento técnico, comúnmente se refiere a realizar un cambio en el hardware del equipo asociado a la incidencia.

La sucesión posible de las incidencias son las detalladas a continuación:



El perfil de usuario puede limitar en algunos casos los estados disponibles para la incidencia:

- **Perfil Usuario**: no puede cambiar ningún estado de la incidencia
- **Perfil Auditor**: puede cambiar una incidencia a cualquier estado a excepción de “Resuelta”.
- **Perfil Jefe Auditor**: puede cambiar a todos los estados disponibles para la incidencia incluido el estado “Resuelta”.

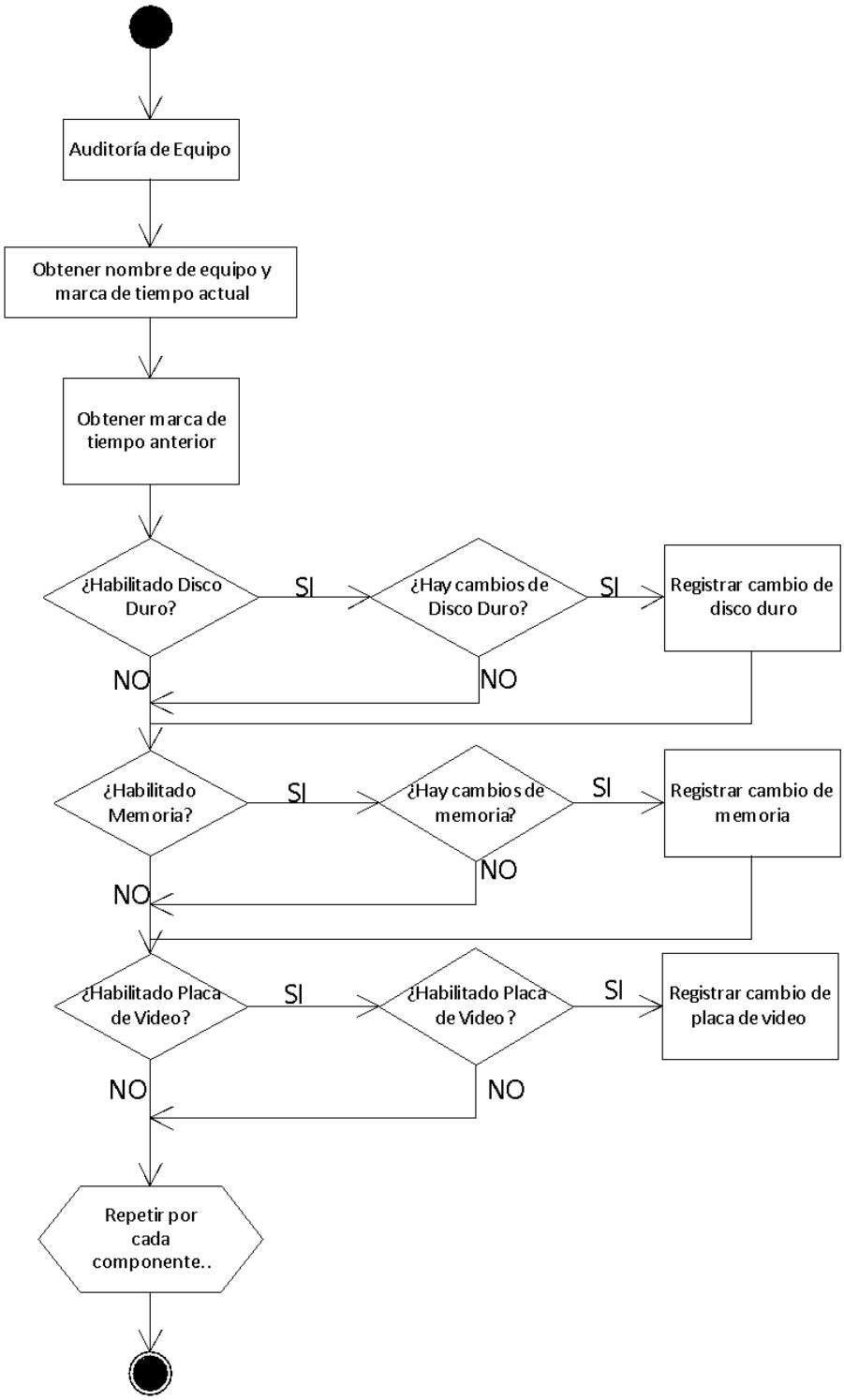
Para todos los cambios de estados el sistema solicita que se ingrese el motivo del mismo. En caso de pasar al estado “Resuelto” se exige adicionalmente el ingreso del motivo de finalización pudiendo elegir entre la opción “Incidencia correctamente resuelta” o “Incidencia Rechazada”.

Diagrama de Detección de Cambios

Dentro de la herramienta de auditoría informática (Proyecto MASI) solo se auditan los equipos para saber que componentes tienen pero no se determina si hay cambios en los mismos. La detección de las modificaciones (componentes agregados o quitados) corre por cuenta del Proyecto ACCEIR mediante una serie de procesos que se llevan a cabo cada vez que MASI audita un equipo.

Estos procesos fueron agrupados en dos diagramas de actividades diferentes. Uno para la detección de cambios en los componentes propiamente dicha y otro que describe las reglas que se aplican para procesar los cambios detectados.

Con cada auditoría se realiza el siguiente proceso de detección de cambios (solo se muestran algunos componentes para facilitar la legibilidad)



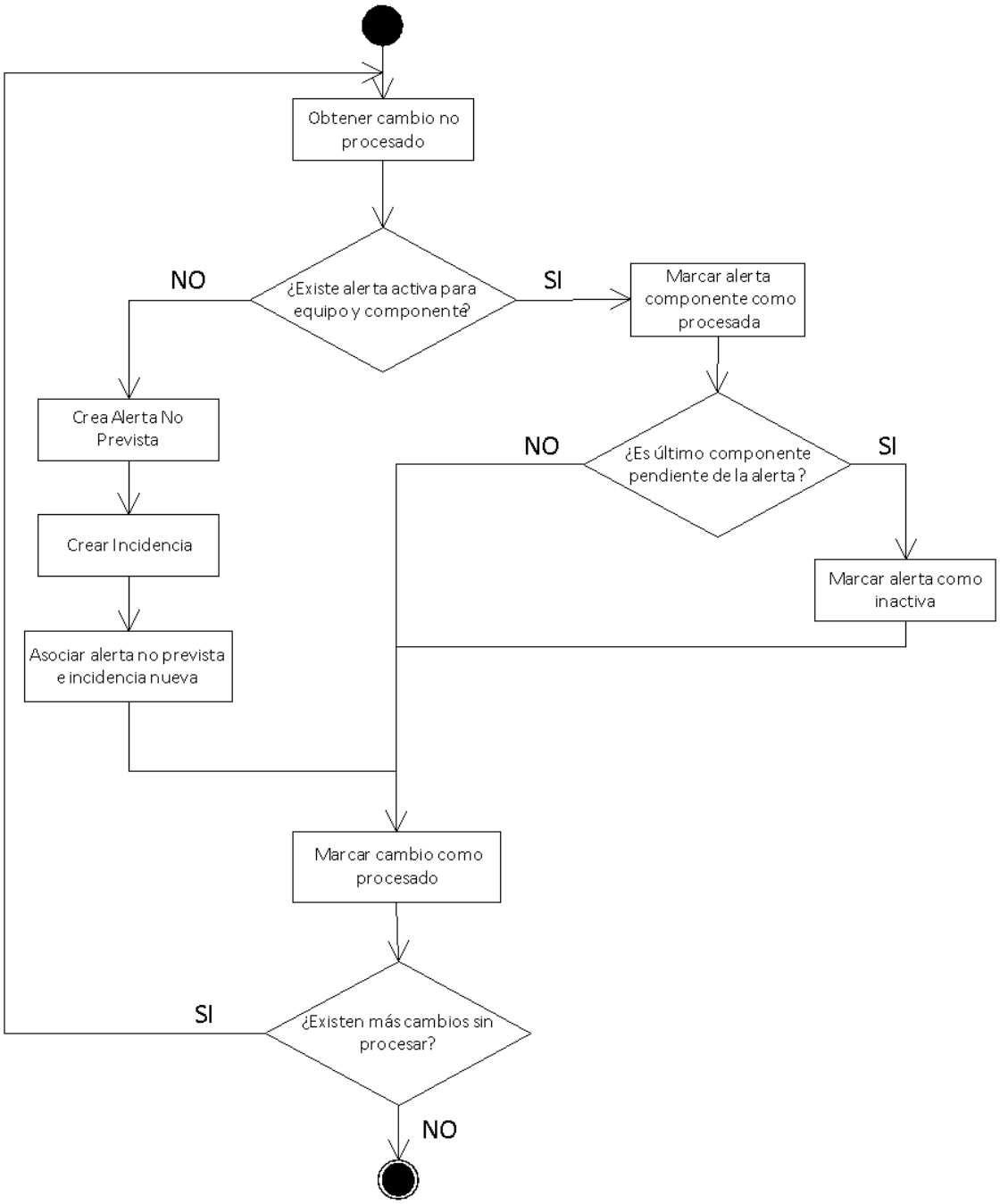
La lógica del diagrama de la Figura se encuentra implementada dentro del sistema de la siguiente manera:

1. Luego de que la herramienta Open Audit realiza una auditoría sobre un equipo hace una llamada al procedimiento almacenado **acceir_detectar_cambios** pasando como parámetros el

nombre del equipo y la marca de tiempo correspondiente a la auditoría realizada.

2. Dentro del procedimiento **acceir_detectar_cambios** se detectan los cambios que pudiesen existir en los componentes de hardware y software a partir de la ejecución de los siguientes procedimientos almacenados:
    a. **acceir_detectar_cambios_battery**
    b. **acceir_detectar_cambios_floppy**
    c. **acceir_detectar_cambios_hd**
    d. **acceir_detectar_cambios_keyboard**
    e. **acceir_detectar_cambios_memory**
    f. **acceir_detectar_cambios_modem**
    g. **acceir_detectar_cambios_monitor**
    h. **acceir_detectar_cambios_motherboard**
    i. **acceir_detectar_cambios_mouse**
    j. **acceir_detectar_cambios_network_card**
    k. **acceir_detectar_cambios_onboard_device**
    l. **acceir_detectar_cambios_optical_drive**
    m. **acceir_detectar_cambios_other**
    n. **acceir_detectar_cambios_processor**
    o. **acceir_detectar_cambios_software**
    p. **acceir_detectar_cambios_sound**
    q. **acceir_detectar_cambios_tape_drive**
    r. **acceir_detectar_cambios_usb**
    s. **acceir_detectar_cambios_video**
3. Si en el paso anterior se detecta un cambio en alguno de los componentes se llama al procedimiento **acceir_procesar_cambio** que almacena estos datos en la tabla **acceir_cambios_componentes**.

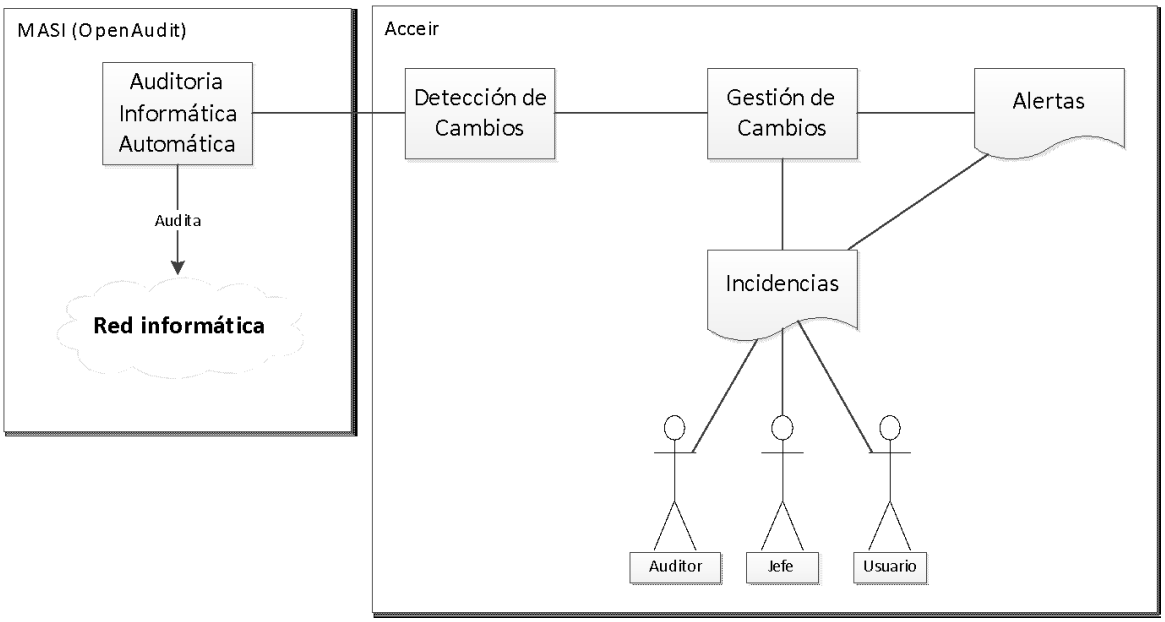
Si se detectan cambios en los componentes del equipo se procede a procesarlos como indica el siguiente diagrama.



Toda la lógica presentada en la Figura se encuentra implementada en el procedimiento almacenado **acceir_generar_alerta**. Este procedimiento se llama luego de completar la detección de cambios y se encarga de generar las alertas previstas o no previstas y las incidencias asociadas a estas últimas si así correspondiera.

Los datos que alimentan este procedimiento provienen de la tabla **acceir_cambios_componentes**.

Diagrama General del Sistema de Auditoría Informática Remota Actual



Aspectos No Cubiertos por los Proyectos Anteriores

Los siguientes son aspectos son consideraciones útiles para un Sistema de Auditoría Informática Remota y que no están cubiertos por los proyectos que están activos actualmente:

- Personalización de Alertas
- Distinción de Software según el Sistema Operativo del equipo
- Control de Periodicidad de Auditorías
- Control de Versión de Sistema Operativo
  - Windows
  - Linux
- Control de Información de Log de Switchs de la Red

Normativas IRAM – ISO/IEC 27000

Origen de la Serie ISO/IEC 27000

La información es un activo vital tanto para el éxito como para la continuidad en el mercado de cualquier organización. Asegurar dicha información y los sistemas que la procesan es, por lo tanto, un objetivo primordial en cualquier organización.

Es necesario implantar un sistema que aborde una adecuada gestión de la seguridad de la información de manera metódica, documentada y basada en objetivos de seguridad claros y una evaluación de riesgos a los que está sometida la información de la organización.

En este contexto, en 1901 nació la primera entidad de normalización a nivel mundial, la BSI (Institución Británica de Estandarización) publicó importantes normas como:

- BS 5750 en el año 1979, actual ISO 9001, norma internacional de sistemas de gestión de calidad.
- BS 7750 en el año 1992, actual ISO 14001, norma internacional de sistemas de gestión ambiental.
- BS 7799 en el año 1995, actual ISO 27001, de la cual hablaremos a continuación.

La norma BS 7799 aparece por primera vez en 1995 con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de seguridad de su información. La primera parte (BS 7799-1) es una guía de buenas prácticas y no establece un sistema de certificación. Años más tarde, la segunda parte (BS 7799-2) establece los requisitos para que un sistema de seguridad de la información sea certificable por una entidad independiente.

Las dos partes de la BS 7799 se revisaron en 1999 y la primera parte se adoptó casi sin cambios en la ISO 17799 en el año 2000. En el año 2002 se revisó la segunda parte para adecuarse a la filosofía de normas ISO de sistemas de gestión. Finalmente, en 2005 y con más de 1700 empresas certificadas en la BS 7799-2, este esquema se publicó por ISO como ISO 27001, al tiempo se revisó y actualizó la ISO 17799 y finalmente en Julio de 2007 se la renombrada como ISO 27002 manteniendo el contenido.

En Marzo de 2006 se publicó la tercera parte del estándar de BSI, la BS 7799-3 centrada en la gestión del riesgo de los sistemas de información.

La serie 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los sistemas de gestión de seguridad de la información (SGSI).

A semejanza de otras normas ISO, la 27000 está compuesta de una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 270444.

- **ISO 27000:** Contiene los términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Es una introducción y base para el resto de la serie. La tercera versión salió en Enero de 2014.
- **ISO 27001:** Publicada el 15 de Octubre de 2005 y revisada en Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Dicho en otras palabras, es la certificación que deben obtener las organizaciones. Adopta un enfoque de

gestión de riesgos y promueve la mejora continua de los procesos.

- **ISO 27002:** Es el código de buenas prácticas para la gestión de seguridad de la información. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799:2005. Fue publicada bajo el nombre actual en Julio de 2007 y se revisó en Septiembre de 2013.

Ciclo PDCA

El Ciclo PDCA, sigla en inglés de Planificar, Hacer, Verificar y Actuar (Plan, Do, Check, Act), también conocido como Ciclo de Mejora Continua o Círculo de Deming (en honor a su creador)). Esta metodología describe los cuatro pasos escénica les que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales, etc.).

El Círculo de Deming está compuesto por cuatro etapas cíclicas. Una vez se acaba la etapa final, se debe volver a la primera para repetir el ciclo nuevamente de forma tal que las actividades se re evalúan periódicamente para incorporar mejoras.

¿Cómo implantar el Ciclo PDCA en una organización?

1. **Planificar:** Se buscan actividades susceptibles de mejora y se establecen objetivos a alcanzar.
2. **Hacer:** Se realizan los cambios para implantar la mejora propuesta, generalmente se prueba la mejora en pequeña escala para luego hacerlo a gran escala
3. Verificar: Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento y si cumple con las expectativas iniciales.
4. **Actuar:** Una vez finalizado el tiempo de prueba se estudian los resultados y se comparan con el funcionamiento previo a la implantación de la mejora. Si es satisfactorio, se implanta la mejora de manera definitiva, sino, deberán proponerse cambios para ajustar los resultados obtenidos a los esperados o desechar la mejora definitivamente. Finalmente, se vuelve a comenzar el ciclo buscando nuevas mejoras a implantar.

Relación entre el Ciclo PDCA y las Normas ISO

Varias normas ISO hacen referencia al Ciclo PDCA enfocando dicho ciclo en el aspecto concerniente a la norma, por ejemplo, la ISO 9001 habla de la mejora continua en el sistema de gestión de calidad, y la ISO 27001 habla de la mejora continua en el sistema de gestión en la Seguridad de la Información.

¿Cómo está compuesta la IRAM ISO/IEC 27001?

LA IRAM/ ISO-IEC 27001 se divide en 9 secciones más los anexos. Las secciones 0 a 3 son introductorias (no son obligatorias para la implementación), mientras que las secciones 4 a 8 son obligatorias, lo que implica que una organización debe implementar todos los requerimientos de estas secciones si quiere cumplir con la norma.

Introducción

- Sección 0 – Introducción: explica el objetivo de ISO 27001, su compatibilidad con otras normas de gestión y hace una introducción al método PDCA
- Sección 1 – Alcance: Especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- Sección 2 – Referencias normativas: Hace referencia a otras normas que sirven de referencia ya que proporcionan términos y definiciones.
- Sección 3 – Términos y definiciones: Breve descripción de los términos más utilizados en la norma.

Ciclo PDCA

- Sección 4 – Contexto de la organización: Define los requerimientos para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI, los requisitos de documentación y control de la misma. También define las partes interesadas, sus requisitos y el alcance del SGSI.
- Sección 5 – Liderazgo: Define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades (como la gestión y provisión de recursos y concienciación, formación y capacitación del personal) y el contenido de la política de alto nivel sobre seguridad de la información.
- Sección 6 – Planificación: Define cómo realizar las auditorías internas de control y cumplimiento.
- Sección 7 – Define cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.
- Sección 8 – Mejora: Define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Anexos

- Anexo A - Objetivos de control y controles: anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.
- Anexo B - Relación con los principios de la OCDE: anexo informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE
- Anexo C - Correspondencia con otras normas: anexo informativo con una tabla de correspondencia de cláusulas con ISO 9001 y ISO 14001.
- Anexo D – Bibliografía de ISO/IEC 27001: normas y publicaciones de referencia.
- Anexo E – Bibliografía de IRAM
- Anexo F – Integrantes de los organismos de estudio de IRAM

¿Cómo está compuesta la IRAM ISO/IEC 27002?

La IRAM/ ISO-IEC 27002 se divide en 15 secciones más los anexos. Las secciones 0 a 3 son introductorias, mientras que las secciones 4 a 15 es la guía de buenas prácticas.

Introducción

- Sección 0 – Introducción: Conceptos generales de seguridad de la información y SGSI.
- Sección 1 – Campo de aplicación: Especifica el objetivo de la norma.
- Sección 2 – Términos y definiciones: Breve descripción de los términos más usados en la norma.
- Sección 3 – Estructura del estándar: Descripción de la estructura de la norma.

Guía de Buenas Prácticas

- Sección 4 – Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- Sección 5 – Política de seguridad: documento de política de seguridad y su gestión.
- Sección 6 – Aspectos organizativos de la seguridad de la información: organización de la seguridad interna y seguridad con terceros.
- Sección 7 – Gestión de activos: responsabilidad sobre los activos y clasificación de la información.
- Sección 8 – Seguridad ligada a los recursos humanos: antes de la incorporación, durante el empleo y en la desvinculación del empleo o cambio de puesto de trabajo.
- Sección 9 – Seguridad física y ambiental: definición de áreas seguras y protección contra amenazas externas y/o del ambiente y seguridad de los equipos.
- Sección 10 – Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación, gestión de la provisión de servicios por terceros, planificación y aceptación del sistema, protección contra código malicioso y descargable, copias de seguridad, gestión de la seguridad de las redes, manipulación de los soportes, intercambio de información, servicios de comercio electrónico y supervisión.
- Sección 11 – Control de acceso: requisitos de negocio para el control de acceso, gestión de acceso de usuario, responsabilidades de usuario, control de acceso a la red, control de acceso al sistema operativo, control de acceso a las aplicaciones y a la información y control de computadoras portátiles y teletrabajo.
- Sección 12 – Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información, tratamiento correcto de las aplicaciones, controles criptográficos, seguridad de los archivos de sistema, seguridad en los procesos de desarrollo y soporte y la gestión de la vulnerabilidad técnica.

- Sección 13 – Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información y la gestión de incidentes de seguridad de la información y mejoras.
- Sección 14 – Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- Sección 15 – Cumplimiento: cumplimiento de los requisitos legales, cumplimiento de las políticas y normas de seguridad y cumplimiento técnico y las consideraciones sobre las auditorías de los sistemas de información.

Anexos

- Anexo A – Bibliografía: normas y publicaciones de referencia.
- Anexo B – Bibliografía IRAM
- Anexo C – Integrantes de los organismos de estudio IRAM

Selección de Secciones de IRAM-ISO/IEC 27002 para el Trabajo Final de Grado

Luego del estudio exhaustivo de la serie ISO 27000 y de los objetivos de cada integrante de la serie, definimos que este Trabajo Final de Grado debería enfocarse en las normas 27001 y 27002, pero, dado que la Institución no poseía ningún documento que agrupará todas políticas, se decidió diseñar dicho documento basándonos en las buenas prácticas expuestas en la IRAM – ISO/IEC 27002. La intención es dejar el camino definido para que en un futuro el sistema de auditoría pueda certificar IRAM – ISO/IEC 27001.

Las secciones elegidas de la IRAM - ISO/IEC 27002 para desarrollar el presente Trabajo Final de Grado fueron:

- Sección 4 – Evaluación y tratamiento del riesgo.
- Sección 5 – Política de seguridad.
- Sección 6 – Aspectos organizativos de la seguridad de la información.
- Sección 7 – Gestión de activos.
- Sección 8 – Seguridad ligada a los recursos humanos.
- Sección 10 – Gestión de comunicaciones y operaciones.
- Sección 11 – Control de acceso.
- Sección 13 – Gestión de incidentes de seguridad de la información.
- Sección 15 – Cumplimiento.

Se eligieron los temas mencionados anteriormente debido a que:

- Poseen algún componente que puede ser programable: Todos aquellos puntos que implican la definición lugares físicos (por ejemplo control de acceso físico a la zona de servidores) es algo que no podría ser controlado por el sistema informático de auditoría remota sino por los auditores humanos.
- Se pueden implementar dentro del tiempo acotado que se propuso para la realización del presente Trabajo Final de Grado: el tiempo es finito y

se decidió que el proceso de desarrollo no demandará más de seis meses debido a que el foco es analizar la normativa y poder aplicarla, no desarrollar un sistema nuevo.

- No conlleva a la creación de grandes módulos de código sino a la mejora en el funcionamiento del código ya existente: la idea es mejorar el funcionamiento del sistema de auditoría ya existente, no se busca cambiarlo por uno nuevo.
- Los puntos elegidos son los que consideramos los más críticos: los puntos elegidos no son todos los que podrían ni deberían agregarse en una política de seguridad definitiva para la Institución, es por eso que luego de exponer los puntos que se hicieron en este Trabajo Final de Grado se expondrán los puntos restantes que consideramos deberían tenerse en cuenta para continuar con la labor que se inició en este Trabajo.

Circulares Informáticas de la Fuerza Aérea Argentina utilizadas en el Instituto Universitario Aeronáutico

La Institución es un organismo dependiente de la Fuerza Aérea Argentina y, como tal, su accionar y desarrollo está dirigido por esta.

En la Institución, en los temas concernientes a la Seguridad en la Información, se regían por una serie de Circulares Informáticas emitidas por la Fuerza Aérea Argentina.

El problema principal de basar una Política de Seguridad en varias Circulares Informáticas se da al momento de querer buscar información sobre un tema en específico debido a que, si bien cada Circular posee un objetivo al inicio de su redacción, el número de circulares existente hace casi imposible encontrar cuáles circulares se refieren a un tema específico y, una vez encontrada, no existe manera de saber si es la última resolución sobre el tema o si existe alguna resolución posterior a esa que altera o desecha lo expuesto.

Las Circulares Informáticas que se me facilitaron en el Instituto Universitario Aeronáutico fueron las siguientes:

- CI 02/97: brindar un conjunto unificado de conceptos, terminología y principios ingenieriles que sirvan de guía y den coherencia a los procesos de desarrollo y explotación de aplicaciones informáticas y encaminen los esfuerzos dentro de un proceso de mejora continua de calidad.
- CI 03/97: definir políticas en materia de seguridad informática que sirvan como guía para la definición de estándares y procedimientos tendientes a minimizar el riesgo de pérdida o alteración (intencional o por ignorancia), indisponibilidad o acceso no autorizado (interno o externo) a información en cualquiera de sus formas (impresa, almacenada, en medio magnético, etc.) y bajo cualquier circunstancia (desastres naturales, operaciones no autorizadas, virus, fallas de software, etc.).
- CI 04/97: definir los aspectos básicos para la implementación de medidas de seguridad física en las áreas informáticas.

- CI 05/97: regular la percepción del suplemento por cómputo de datos que recibe el personal civil de la Fuerza, en función de los avances tecnológicos y de las necesidades actuales y futuras de la Institución.
- CI 06/97: definir las características mínimas que debe tener una computadora para ser utilizada como servidor departamental.
- CI 07/97: definir las características necesarias para poder compartir recursos informáticos en grupo de trabajo menores (hasta 6 usuarios) que trabajan, preferentemente, en un ambiente común.
- CI 08/97: brindar un conjunto unificado de conceptos, terminología y procedimientos que sirvan de guía para la utilización de Internet.
- CI 11/97: Establecer procedimientos a seguir en materia de seguridad informática que sirvan para minimizar el riesgo de pérdida, alteración, indisponibilidad o acceso no autorizado a los sistemas informáticos. Contribuyente a los propósitos señalados en las Circulares número 3 y 4.
- CI 12/97: Normalizar el empleo de los Utilitarios más utilizados en equipos de computadoras personales (PC), como así también orientar la capacitación del personal al respecto y establecer procedimientos para la adquisición de software con la finalidad de optimizar el empleo eficiente de los recursos informáticos.
- CI 13/97: Definir el lugar más apropiado para la ubicación física de servidores departamentales en los Organismos que tienen o requieren un servidor de red.
- CI 14/97: Lograr un desarrollo informático armónico en la Fuerza Aérea y establecer disposiciones que regulen el accionar específico.
- CI 16/97: Establecer procedimientos a seguir en materia de seguridad informática que sirvan para minimizar el riesgo de pérdida, alteración, etc., de los sistemas informáticos por ataques de virus. Contribuye al propósito señalado en la Circular número 3.
- CI 03/98: Establecer el propósito y el alcance de la utilización de Internet y servicios afines en el ámbito institucional.
- CI 04/98: Establecer normas y procedimientos para preservar la integridad, la operatividad y la confidencialidad de la información que se almacena y/o procesa por intermedio de equipos informáticos.
- CI 07/98: Definir el protocolo de Conectividad a nivel de enlace (su nivel de acceso a medios) en redes de área local, a ser utilizado como estándar dentro del ámbito de la FAA. Esta definición debe procurar las necesidades inmediatas de conectividad en las redes departamentales, al mismo tiempo que facilitar la posibilidad de integración de redes departamentales dentro del esquema de desarrollo de la red global informática prevista en el Plan Director Informático de la FAA.
- CI 01/99: Establecer los lineamientos generales para elaborar planes de contingencia en base a los resultados de la evaluación de riesgos efectuados sobre funciones o actividades consideradas críticas.
- CI 01/2000: Establecer los lineamientos generales para evitar la utilización de productos de software de ofimática sin su correspondiente licencia de explotación y ofrecer alternativas de solución aceptables.

- CI 02/2000: Establecer los lineamientos generales para la explotación de los servicios de Internet en el ámbito institucional sin comprometer información relacionada con actividades del servicio.
- CI 04/2000: Definir las características del ciclo de vida de productos de software y establecer los estándares aplicables en el ámbito de la FAA para optimizar su desarrollo, explotación y mantenimiento, en base a una estricta racionalización de recursos.
- CI 01/2001: Prohibir la divulgación de información en internet que no esté expresamente autorizada por la Secretaría General y que puede comprometer la seguridad o los intereses de carácter institucional.
- CI 01/2002: Establecer criterios generales para el acceso y la explotación de información procedente de sistemas informáticos en estado de producción en el ámbito institucional.
- CI 02/2002: Establecer criterios generales para la correcta explotación de los servicios de Internet en el ámbito institucional y restringir su uso estrictamente para cuestiones del servicio.
- CI 01/2003: Establecer los lineamientos a seguir en materia de seguridad informática respecto del uso de las cuentas de correo electrónico institucional a efectos de evitar la divulgación de información sensible para la institución y reducir el número de incidentes de seguridad.
- CI 02/2003: Establecer los criterios rectores para el uso correcto del servicio de correo electrónico institucional por parte de los usuarios del mismo.
- CI 01/2004: Establecer los criterios rectores para el uso seguro de las computadoras portátiles que deban ser utilizadas dentro del ámbito de la FAA.
- CI 01/2005: Establecer y mantener la integridad de los productos generados durante un proyecto de desarrollo de software y a lo largo de todo el ciclo de vida del producto.
- CI 01/2006: Establecer los criterios rectorales para el uso seguro de la tecnología inalámbrica (wireless).
- CI 02/2006: Establecer los lineamientos generales para emprender el desarrollo de sistemas de información en el ámbito institucional con recursos de la Fuerza o contratar los servicios de desarrollo para su obtención a terceros.
- CI 03/2006: Ampliar las pautas generales establecidas para canalizar la información de carácter institucional a través de Internet.
- CI 01/2007: Establecer el rol de la Dirección General de Asuntos Institucionales respecto de la información institucional publicada en Internet.
- CI 03/2008: Definir las políticas a seguir para la protección de los recursos informático de la FAA frente a posibles ataques de programas maliciosos (malware).
- CI 01/2011: Actualizar la normativa que rige en el ámbito institucional para agilizar la tramitación técnica en el proceso de adquisición y contratación de bienes, insumos y/o servicios de carácter informático, a propósito de la puesta en funcionamiento del sistema de “Estándares Tecnológicos para la Administración Pública en Línea”.

- CI 01/2012: Establecer las tareas y funciones que tiene el personal que se desempeña como Responsable de Informática en los Organismos y Unidades de la Fuerza.
- CI 01/2015: Establecer la normativa correspondiente a las licencias y uso de software en el ámbito de la FAA.
- CI 02/2015: Establecer procedimientos de seguridad informática a. Cumplimentar al conectar equipamiento informático a la red de datos de la FAA.
- CI 03/2015: Determinar el sistema operativo que utilizarán las computadoras de escritorio de los Organismos y Unidades de la FAA conforme a las necesidades actuales, a los recursos informáticos disponibles y a la compatibilidad de servicios y/o aplicaciones.

Como se puede apreciar, muchas de ellas tratan de temas como definiciones de términos técnicos, definiciones de lineamientos en cuanto al uso de dispositivos, servicios, etc., y definiciones ubicaciones físicas; todas esas Circulares Informáticas, si bien son importantes, no podrían ser contempladas en el código del Sistema de Auditoría Remota.

Aunque se tuvo en cuenta el contenido de todas las circulares al diseñar la Política de Seguridad, las siguientes fueron las que tuvieron más importancia a la hora de definir los ejes principales de la misma:

- CI 04/98
- CI 02/02
- CI 01/2015
- CI 02/2015
- CI 03/2015

Política de Seguridad

La Política de Seguridad es un documento que contiene un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir los recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma. En otras palabras, las políticas de seguridad definen qué está permitido y qué está prohibido dentro de una organización, define los procedimientos y herramientas necesarias para el trabajo diario en la misma, expresan el consenso de los usuarios de los activos organizacionales y permiten adoptar una buena actitud dentro de la organización.

Diseño y Armado de Política de Seguridad para la Institución

Para diseñar el formato y el contenido de la Política nos basamos en otras Políticas de Seguridad utilizadas en establecimientos educativos (como la UNC y UTN) y en las Circulares Informáticas que ya se utilizaba de esa manera en la Institución.

La idea fue utilizar las circulares que tenían una base programable y pasarlas a una Política de Seguridad formal. Por supuesto, esta Política no está completa ni es definitiva, podría incorporar todas las Circulares Informáticas vigentes y las futuras, podría incorporar nuevos puntos además de los descritos por éstas, etc. Esta actividad no se realizó porque se contaba con un tiempo

limitado lo que llevaba a acotar las tareas a lo mínimo necesario para cumplir con las entregas propuestas.

Política de Seguridad para la Institución

La Política de Seguridad que se propuso para la Institución está detallada en el Anexo A del presente Trabajo Final de Grado. A continuación se listan sus títulos con un breve resumen de cada sección:

1. **Introducción:** presentación del documento de Política de Seguridad para la Información Informatizada para el Instituto Universitario Aeronáutico.
2. **Términos y Definiciones:** diccionario de palabras técnicas que serán utilizadas en el documento de Política de Seguridad para la Información Informatizada para el Instituto Universitario Aeronáutico.
3. **Objetivos de la Política de Seguridad de la Información Informatizada:** objetivos y sanciones previstas por incumplimiento del presente documento.
4. **Sanciones:** se detalla el tipo de sanciones dependiendo la falta a la Política de Seguridad que se haya cometido.
5. **Clasificación y Control de Activos:** se especifica cómo se deben inventariar los activos institucionales y se detalla información sobre la asignación de los activos a cada individuo de la Institución y la respuesta ante incidentes y/o anomalías con los equipos.
6. **Respuesta a Incidentes y Anomalías en los Equipos:** se determina cómo debe procederse en caso de un incidente y quién debe reportar cualquier irregularidad en los equipos.
7. **Seguridad de la Red y los Equipos:** se informa lo concerniente a la protección contra el software malicioso, restricciones en la instalación y uso de software específico, protección de la integridad de los equipos, actualización del sistema operativo de los mismos y especificaciones sobre la periodicidad de las auditorías obligatorias. Además detalla cuándo un equipo no puede permanecer en la red y define de quién es la responsabilidad ante este tipo de incidentes.
8. **Actualización del Sistema Operativo de los Equipos:** se determina que debe existir una versión mínima necesaria de Sistema Operativo en los equipos.
9. **Auditorías Obligatorias:** se determina que las auditorías serán requeridas cada cierto periodo de tiempo
10. **Responsabilidades ante Incidentes:** se informa quién será responsable ante los incidentes ocurridos en un equipo.
11. **Anexo 1 - Lista de Software Prohibido:** se enumeran los elementos software prohibidos, divididos por categoría.
12. **Anexo 2 - Lista de Software Requerido:** se enumeran los elementos software requeridos, divididos por categoría.

13. **Anexo 3 - Lista de Software Sensible:** se enumeran los elementos software que en caso de ser alterados sin autorización previa, generarán una alerta.
14. **Anexo 4 - Lista de Hardware Sensible:** se enumeran los elementos hardware que en caso de ser alterados sin autorización previa, generarán una alerta.

SCRUM como Metodología Ágil Elegida para este Proyecto Final de Grado

Es un metodología de desarrollo ágil caracterizada por adoptar una estrategia de desarrollo incremental basando la calidad del resultado principalmente en el conocimiento tácito de las personas en equipos auto organizados que son capaces de solapar las diferentes fases del desarrollo a fin de reducir los tiempos de desarrollo.

SCRUM en este Trabajo Final de Grado

Se eligió la metodología ágil SCRUM frente a cualquier metodología clásica porque permite entregas periódicas sin un exceso de documentación para cada entrega. Esto es importante debido a que todo el trabajo (desarrollo y documentación) debería ser cumplido por solo una persona y eso extendería el proyecto en el tiempo y no cumpliría con el límite preestablecido para la realización del mismo. Además, la metodología SCRUM permite que el desarrollo se mantenga centrado en la productividad y la eficiencia del tiempo invertido en el desarrollo, factores sumamente importantes dada la limitación de recursos.

Análisis de Riesgos

Para la realización de este Trabajo Final de Grado se asumen ciertos puntos para evitar que el trabajo se prolongue indefinidamente en el tiempo y para evitar agregar más requerimientos a los que ya se definieron. Los puntos que se asumieron fueron los siguientes:

- Se asume que las fuentes de información mencionadas en el presente Anteproyecto van a ser suficientes para lograr el objetivo del Trabajo Final de Grado.
- Se asume que los sistemas Open Audit y Acceir funcionan correctamente y detectan de forma efectiva los cambios ocurridos en la red y en los dispositivos auditados en tiempo real, quedando fuera del alcance de este proyecto cualquier deficiencia en los sistemas mencionados que pudieran afectar el desempeño del sistema desarrollado en este Trabajo Final de Grado.

Además se definió que el trabajo de investigación y codificación del presente Trabajo Final de Grado culmine en un plazo no mayor a seis meses desde su fecha de comienzo.

Agenda del Proyecto

Es el documento que provee una visión global del enfoque de desarrollo propuesto, así como un cronograma para el desarrollo del producto y un acta de reunión.

N° de Sprint	Descripción de Sprint	Duración (Hs.)	Comienzo	Fin
0	Definición de Componentes Externos a utilizar y del Product Backlog	30	15/Feb/2016	29/Feb/2016
1	Sobre la Investigación, Diseño y Definición de las Políticas de Seguridad Institucional	160	01/Mar/2016	22/Abr/2016
2	Sobre el Software Prohibido	60	25/Abr/2016	13/May/2016
3	Sobre el Software Necesario	60	16/May/2016	03/Jun/2016
4	Sobre el Software Sensible	60	06/Jun/2016	24/Jun/2016
5	Sobre el Tipo de Software y Configuración de Alertas	60	27/Jun/2016	15/Jul/2016
6	Sobre las Auditorías Necesarias	40	18/Jul/2016	29/Jul/2016
7	Sobre el Build Requerido para Windows y Linux	40	01/Ago/2016	12/Ago/2016
8	Sobre las Visualizaciones de Alertas, Incidentes y Sugerencias	60	15/Ago/2016	02/Sep/2016
9	Sobre la Puesta en Marcha y las Pruebas Finales	40	05/Sep/2016	30/Sep/2016

Iteraciones (Sprints)

El cronograma de actividades está determinado por el siguiente Diagrama de Gantt:

	Predecesores	Nombre de la tarea	Fecha de Inicio	Fecha final	Duración
1		**Trabajo Final de Grado**	**09/11/15**	**31/10/16**	**256d**
2		**Aprobación del Anteproyecto**	**09/11/15**	**12/02/16**	70d
3		Aprobación del Anteproyecto	09/11/15	12/02/16	70d
4	2	**Desarrollo Escrito del TFG**	**15/02/16**	**24/11/16**	204d
5		Desarrollo Escrito del TFG	**15/02/16**	**24/11/16**	**204d**
6	2	**Sprint 0 - Definición de Componentes Externos a utilizar y del Product Backlog**	**15/02/16**	**29/02/16**	11d
7		Definición de Componentes Externos (del lado del servidor y del cliente)	15/02/16	15/02/16	1d
8	7	Estudio de Tablas Necesarias en OpenAudit y Acceir	16/02/16	19/02/16	4d
9	8	Definición de Historias de Usuario (Product Backlog)	22/02/16	29/02/16	6d
10	6	**Sprint 1 - Sobre la Investigación, Diseño y Definición de las Políticas de Seguridad Institucional**	**01/03/16**	**23/05/16**	**60d**
11		Estudio de la Serie ISO 27000	01/03/16	03/03/16	3d
12	11	Estudio de Circulares Informáticas	04/03/16	08/03/16	3d
13	12	Estudio de otras Políticas de Seguridad de Universidades (UNC y UTN)	09/03/16	29/03/16	15d
14	13	Diseño y Definición de Política de Seguridad para IUA	30/03/16	23/05/16	39d
15	10	**Sprint 2 - Sobre el Software Prohibido**	**24/05/16**	**13/06/16**	15d
16		Definición de Lista de Software Prohibido	24/05/16	30/05/16	5d
17	16	Desarrollo de Módulo para el Sistema de Auditoría	31/05/16	13/06/16	10d
18	15	**Sprint 3 - Sobre el Software Necesari**	**14/06/16**	**04/07/16**	15d
19		Definición de Lista de Software Necesario	14/06/16	20/06/16	5d
20	19	Desarrollo de Módulo para el Sistema de Auditoría	21/06/16	04/07/16	10d
21	20	**Sprint 4 - Sobre el Software Sensible**	**05/07/16**	**25/07/16**	15d
22		Definición de Lista de Software Sensible	05/07/16	11/07/16	5d
23	22	Desarrollo de Módulo para el Sistema de Auditoría	12/07/16	25/07/16	10d
24	21	**Sprint 5 - Sobre el Tipo de Software y Configuración de Alertas**	**26/07/16**	**15/08/16**	15d
25		Definición de Lista de Tipo de Software	26/07/16	01/08/16	5d
26	25	Desarrollo de Módulo para el Sistema de Auditoría	02/08/16	08/08/16	5d
27	26	Desarrollo de Sección para Configuración de Alertas	09/08/16	15/08/16	5d
28	24	**Sprint 6 - Sobre las Auditorías Necesarias**	**16/08/16**	**29/08/16**	10d
29		Definición de Auditorías Necesarias	16/08/16	18/08/16	3d
30	29	Desarrollo de Módulo para el Sistema de Auditoría	19/08/16	29/08/16	7d
31	28	**Sprint 7 - Sobre el Build Requerido para Windows y Linux**	**30/08/16**	**12/09/16**	10d
32		Definición de Build Requerido para Windows y Linux	30/08/16	01/09/16	3d
33	32	Desarrollo de Módulo para el Sistema de Auditoría	02/09/16	12/09/16	7d
34	31	**Sprint 8 - Sobre las Visualizaciones de Alertas, Incidentes y Sugerencias**	**13/09/16**	**03/10/16**	15d
35		Estudio del Procedimiento del Sistema Acceir para generar Alertas e Incidentes	13/09/16	19/09/16	5d
36	35	Desarrollo de Procedimientos Almacenados para la Generación de las Nuevas Alertas e Incidentes	20/09/16	03/10/16	10d
37	34	**Sprint 9 - Sobre la Puesta en Marcha y las Pruebas Finales**	**04/10/16**	**31/10/16**	20d
38		Puesta en Marcha y Pruebas Finales	04/10/16	31/10/16	20d


2016
2017
Nov Dic Ene Feb Mar Abr May Jun Jul Ago Sep Oct Nov Dic Ene Feb Mar Abr May Jun Jul Ago Sep
Trabajo Final de Grado
Aprobación del Anteproyecto
Aprobación del Anteproyecto
Desarrollo Escrito del TFG
Desarrollo Escrito del TFG
Sprint 0 - Definición de Componentes Externos a utilizar y del Product Backlog
Definición de Componentes Externos (del lado del servidor y del cliente)
Estudio de Tablas Necesarias en OpenAudit y Acceir
Definición de Historias de Usuario (Product Backlog)
Sprint 1 - Sobre la Investigación, Diseño y Definición de las Políticas de Seguridad Institu
Estudio de la Serie ISO 27000
Estudio de Circulares Informáticas
Estudio de otras Políticas de Seguridad de Universidades (UNC y UTN)
Diseño y Definición de Política de Seguridad para IUA
Sprint 2 - Sobre el Software Prohibido
Definición de Lista de Software Prohibido
Desarrollo de Módulo para el Sistema de Auditoría
Sprint 3 - Sobre el Software Necesario
Definición de Lista de Software Necesario
Desarrollo de Módulo para el Sistema de Auditoría
Sprint 4 - Sobre el Software Sensible
Definición de Lista de Software Sensible
Desarrollo de Módulo para el Sistema de Auditoría
Sprint 5 - Sobre el Tipo de Software y Configuración de Alertas
Definición de Lista de Tipo de Software
Desarrollo de Módulo para el Sistema de Auditoría
Desarrollo de Sección para Configuración de Alertas
Sprint 6 - Sobre las Auditorías Necesarias
Definición de Auditorías Necesarias
Desarrollo de Módulo para el Sistema de Auditoría
Sprint 7 - Sobre el Build Requerido para Windows y Linux
Definición de Build Requerido para Windows y Linux
Desarrollo de Módulo para el Sistema de Auditoría
Sprint 8 - Sobre las Visualizaciones de Alertas, Incidentes y Sugerencias
Estudio del Procedimiento del Sistema Acceir para generar Alertas e Incidente
Desarrollo de Procedimientos Almacenados para la Generación de las Nue
Sprint 9 - Sobre la Puesta en Marcha y las Pruebas Finales
Puesta en Marcha y Pruebas Finales

Sprint 0 - Definición de Componentes Externos y del Product Backlog

Componentes Externos Utilizados para la Implementación de las Modificaciones

Para la implementación de las modificaciones planeadas se debe utilizar algunos componentes (librerías y frameworks) fabricados por terceros a fin de mantener el diseño original del Sistema de Auditoría.

Componentes del lado del servidor

Son aquellos componentes que se van a ejecutar dentro del servidor web Apache donde va a correr la aplicación.

- **ADOdb:** librería utilizada para crear una capa de abstracción de la base de datos en PHP, de manera que se puede cambiar la base de datos sin afectar el código de la aplicación.
- **Slim Framework:** se trata de un micro-framework para PHP que, entre otras características, permite crear rutas personalizadas. Esta característica es utilizada en el proyecto para construir rutas amigables y la api REST utilizada.

Componentes del lado del cliente

Los componentes del lado del cliente son aquellos que se ejecutan dentro del navegador del usuario del sistema, básicamente se trata de hojas de estilo (CSS), Javascript y HTML dinámico (DHTML).

- **Bootstrap**: se trata de un framework CSS creado por la empresa Twitter que brinda posibilidades de crear un sitio que se adapta automáticamente a diferentes tamaños de pantalla (diseño responsive). Se utilizó de base para crear el diseño del portal de la aplicación.
- **Jquery**: framework que simplifica el uso de código Javascript.
- **Knockout.js**: framework de Javascript que permite aplicar el patrón MVVM (Modelo-Vista-Vista-Modelo) de manera transparente. Se utiliza este patrón para organizar y simplificar el código Javascript.

Product Backlog

Es un documento que contiene las descripciones generales de las funcionalidad es deseables priorizadas según su retorno sobre la inversión y las estimaciones realizadas a grandes rasgos (valor para el negocio y esfuerzo de desarrollo requerido).

Historia de Usuario	
Número: 1	**Usuario:** Jefe Auditor
Nombre de Historia: Cargar Software Prohibido	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 2
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder cargar en el sistema un software prohibido.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Prohibido debo poder agregar un nuevo Software Prohibido.	

Historia de Usuario	
Número: 2	**Usuario:** Jefe Auditor
Nombre de Historia: Eliminar Software Prohibido	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 2
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder eliminar del sistema un software prohibido cargado previamente.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Prohibido debo poder eliminar el Software Prohibido seleccionado.	

Historia de Usuario	
Número: 3	**Usuario:** Jefe Auditor
Nombre de Historia: Editar Software Prohibido	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 2
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder modificar en el sistema un software prohibido ya cargado en el sistema.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Prohibido debo poder modificar el Software Prohibido seleccionado.	

Historia de Usuario	
Número: 4	**Usuario:** Jefe Auditor
Nombre de Historia: Visualizar Software Prohibido ya cargado	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada:** 2
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar en el sistema los software prohibidos ya cargados en el sistema.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Prohibido debo poder visualizar la lista de Software Prohibido.	

Historia de Usuario	
Número: 5	**Usuario:** Jefe Auditor
Nombre de Historia: Filtrar Software Prohibido ya cargado	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada:** 2
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder filtrar en el sistema la lista de los software prohibidos ya cargados en el sistema.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Prohibido debo poder filtrar la lista de Software Prohibido.	

Historia de Usuario	
Número: 6	**Usuario:** Jefe Auditor
Nombre de Historia: Cargar Software Necesario	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder cargar en el sistema un software necesario.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Necesario debo poder agregar un nuevo Software Necesario.	

Historia de Usuario	
Número: 7	**Usuario:** Jefe Auditor
Nombre de Historia: Eliminar Software Necesario.	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder eliminar del sistema un software necesario cargado previamente.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Necesario debo poder eliminar el Software Necesario seleccionado.	

Historia de Usuario	
Número: 8	**Usuario:** Jefe Auditor
Nombre de Historia: Editar Software Necesario	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder modificar en el sistema un software necesario ya cargado en el sistema.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Necesario debo poder modificar el Software Necesario seleccionado.	

Historia de Usuario	
Número: 9	**Usuario:** Jefe Auditor
Nombre de Historia: Visualizar Software Necesario	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar en el sistema un software necesario ya cargado en el sistema.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Necesario debo poder visualizar la lista de Software Necesario.	

Historia de Usuario	
Número: 10	**Usuario:** Jefe Auditor
Nombre de Historia: Filtrar Software Necesario ya cargado	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder filtrar en el sistema la lista de software necesario ya cargado en el sistema.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Necesario debo poder filtrar la lista de Software Necesario.	

Historia de Usuario	
Número: 11	**Usuario:** Jefe Auditor
Nombre de Historia: Cargar Software Sensible	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder cargar en el sistema un software sensible.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Sensible debo poder agregar un nuevo Software Sensible.	

Historia de Usuario	
Número: 12	**Usuario:** Jefe Auditor
Nombre de Historia: Eliminar Software Sensible	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder eliminar del sistema un software sensible cargado previamente.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Sensible debo poder eliminar el Software Sensible seleccionado.	

Historia de Usuario	
Número: 13	**Usuario:** Jefe Auditor
Nombre de Historia: Editar Software Sensible	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder modificar en el sistema un software sensible ya cargado en el sistema.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Sensible debo poder modificar el Software Sensible seleccionado.	

Historia de Usuario	
Número: 14	**Usuario:** Jefe Auditor
Nombre de Historia: Visualizar Software Sensible	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar en el sistema la lista de software sensible ya cargados.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Sensible debo visualizar la lista de Software Sensibles ya cargados.	

Historia de Usuario	
Número: 15	**Usuario:** Jefe Auditor
Nombre de Historia: Filtrar la lista de Software Sensible	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder filtrar en el sistema la lista de software sensible ya cargados.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Software Sensible debo filtrar la lista de Software Sensibles ya cargados.	

Historia de Usuario	
Número: 16	**Usuario:** Jefe Auditor
Nombre de Historia: Editar Alertas Disponibles	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada:** 4
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder modificar en el sistema la lista de qué alertas estarán habilitadas a la hora de realizar las auditorías automáticas.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Configuración de Alertas debo poder visualizar la lista de Alertas Habilitadas respecto Hardware y Software.	

Historia de Usuario	
Número: 17	**Usuario:** Jefe Auditor
Nombre de Historia: Visualizar Alertas Disponibles	
Prioridad en Negocio: Media	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada:** 4
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar en el sistema la lista de qué alertas estarán habilitadas a la hora de realizar las auditorías automáticas.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Configuración de Alertas debo poder visualizar la lista de Alertas Habilitadas respecto Hardware y Software.	

Historia de Usuario	
Número: 18	**Usuario:** Jefe Auditor
Nombre de Historia: Cargar Tipo de Software	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 4**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder cargar en el sistema un tipo de software.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Tipo de Software debo poder agregar un nuevo Tipo de Software.	

Historia de Usuario	
Número: 19	**Usuario:** Jefe Auditor
Nombre de Historia: Eliminar Tipo de Software	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 4
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder eliminar del sistema un tipo de software cargado previamente.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Tipo de Software debo poder eliminar el Tipo de Software seleccionado.	

Historia de Usuario	
Número: 20	**Usuario:** Jefe Auditor
Nombre de Historia: Editar Tipo de Software	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 4
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder modificar en el sistema un tipo de software ya cargado en el sistema.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Tipo de Software debo poder modificar el Tipo de Software seleccionado.	

Historia de Usuario	
Número: 21	**Usuario:** Jefe Auditor
Nombre de Historia: Visualizar Lista de Tipo de Software	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada: 4**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar en el sistema la lista de tipo de software.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Tipo de Software debo poder visualizar la lista de Tipos de Software previamente cargados.	

Historia de Usuario	
Número: 22	**Usuario:** Jefe Auditor
Nombre de Historia: Filtrar Lista de Tipo de Software	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada: 4**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder filtrar en el sistema la lista de tipo de software.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Tipo de Software debo poder filtrar la lista de Tipos de Software previamente cargados.	

Historia de Usuario	
Número: 23	**Usuario:** Jefe Auditor
Nombre de Historia: Definir Periodicidad de Auditorías Necesarias	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada:** 5
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder definir la periodicidad necesaria para realizar las auditorías	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Auditorías Necesarias debo poder definir el periodo en el cual debe realizarse al menos una auditoría.	

Historia de Usuario	
Número: 24	**Usuario:** Jefe Auditor
Nombre de Historia: Modificar la Periodicidad de Auditorías Necesarias	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada:** 5
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder modificar la periodicidad necesaria para realizar las auditorías	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Auditorías Necesarias debo poder modificar el periodo en el cual debe realizarse al menos una auditoría.	

Historia de Usuario	
Número: 25	**Usuario:** Jefe Auditor
Nombre de Historia: Visualizar Periodicidad de Auditorías Necesarias	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada:** 5
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar la periodicidad necesaria para realizar las auditorías	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Auditorías Necesarias debo poder visualizar el periodo en el cual debe realizarse al menos una auditoría.	

Historia de Usuario	
Número: 26	**Usuario:** Jefe Auditor
Nombre de Historia: Cargar Build Requerido para Equipos con Windows	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 6**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder cargar en el sistema el número de build mínimo requerido para equipos con sistema operativo Windows.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Build Requerido Windows debo poder agregar un nuevo número de build mínimo requerido para los equipos con sistema operativo Windows.	

Historia de Usuario	
Número: 27	**Usuario:** Jefe Auditor
Nombre de Historia: Modificar Build Requerido para Equipos con Windows	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 6**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar en el sistema el número de build mínimo requerido para equipos con sistema operativo Windows.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Build Requerido Windows debo poder visualizar el número de build mínimo requerido para los equipos con sistema operativo Windows.	

Historia de Usuario	
Número: 28	**Usuario:** Jefe Auditor
Nombre de Historia: Visualizar Build Requerido para Equipos con Windows	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada: 6**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar en el sistema el número de build mínimo requerido para equipos con sistema operativo Windows.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Build Requerido Windows debo poder visualizar el número de build mínimo requerido para los equipos con sistema operativo Windows.	

Historia de Usuario	
Número: 29	**Usuario:** Jefe Auditor
Nombre de Historia: Cargar Kernel Requerido para Equipos con Linux	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 6**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder cargar en el sistema el número de kernel mínimo requerido para equipos con sistema operativo Linux.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Build Requerido Linux debo poder agregar un nuevo número de kernel mínimo requerido para los equipos con sistema operativo Linux.	

Historia de Usuario	
Número: 30	**Usuario:** Jefe Auditor
Nombre de Historia: Modificar Kernel Requerido para Equipos con Linux	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 6**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar en el sistema el número kernel mínimo requerido para equipos con sistema operativo Linux.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Build Requerido Linux debo poder visualizar el número de kernel mínimo requerido para los equipos con sistema operativo Linux.	

Historia de Usuario	
Número: 31	**Usuario:** Jefe Auditor
Nombre de Historia: Visualizar Kernel Requerido para Equipos con Linux	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada: 6**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Jefe Auditor quiero poder visualizar en el sistema el número de kernel mínimo requerido para equipos con sistema operativo Linux.	
Validación: Dado que he ingresado como usuario Jefe Auditor, al ingresar a la sección Configuración > Build Requerido Linux debo poder visualizar el número de kernel mínimo requerido para los equipos con sistema operativo Linux.	

Historia de Usuario	
Número: 32	**Usuario:** Auditor
Nombre de Historia: Visualizar Alertas no Previstas por Software Prohibido	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema las alertas por Software Prohibido.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Alerta > Alerta No Prevista, debo poder visualizar en la sección Componentes Afectados las alertas por Software Prohibido.	

Historia de Usuario	
Número: 33	**Usuario:** Auditor
Nombre de Historia: Visualizar Incidentes por Software Prohibido	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema los Incidentes por Software Prohibido.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Equipo Informático, debo poder visualizar en la sección Componentes del Equipo los Incidentes por Error en Software Prohibido.	

Historia de Usuario	
Número: 34	**Usuario:** Auditor
Nombre de Historia: Visualizar Sugerencias de acciones correctivas por Software Prohibido	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema la sugerencia de acción a correctiva a tomar ante incidentes por Software Prohibido.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Mensajes, debo poder visualizar la sugerencia del sistema sobre qué acción correctiva se debe tomar ante incidentes por Software Prohibido.	

Historia de Usuario	
Número: 35	**Usuario:** Auditor
Nombre de Historia: Visualizar Alertas no Previstas por Software Sensible	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema solamente las alertas de Software de aquellos que se encuentren en la lista de Software Sensible.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Alerta > Alerta No Prevista, debo poder visualizar en la sección Componentes Afectados las alertas por Software Sensible.	

Historia de Usuario	
Número: 36	**Usuario:** Auditor
Nombre de Historia: Visualizar Incidentes por Software Prohibido	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema solamente los incidentes de Software de aquellos que se encuentren en la lista de Software Sensible.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Equipo Informático, debo poder visualizar en la sección Componentes del Equipo los Incidentes por Error en Software Sensible.	

Historia de Usuario	
Número: 37	**Usuario:** Auditor
Nombre de Historia: Visualizar Sugerencias de acciones correctivas por Software Sensible	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema la sugerencia de acción a correctiva a tomar ante incidentes por Software Sensible.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Mensajes, debo poder visualizar la sugerencia del sistema sobre qué acción correctiva se debe tomar ante incidentes por Software Sensible.	

Historia de Usuario	
Número: 38	**Usuario:** Auditor
Nombre de Historia: Visualizar Alertas no Previstas por Software Necesario	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema las alertas por Software Necesario.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Alerta > Alerta No Prevista, debo poder visualizar en la sección Componentes Afectados las alertas por Software Necesario.	

Historia de Usuario	
Número: 39	**Usuario:** Auditor
Nombre de Historia: Visualizar Incidentes por Software Necesario	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema los Incidentes por Software Necesario.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Equipo Informático, debo poder visualizar en la sección Componentes del Equipo los Incidentes por Error en Software Necesario.	

Historia de Usuario	
Número: 40	**Usuario:** Auditor
Nombre de Historia: Visualizar Sugerencias de acciones correctivas por Software Necesario	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema la sugerencia de acción a correctiva a tomar ante incidentes por Software Necesario.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Mensajes, debo poder visualizar la sugerencia del sistema sobre qué acción correctiva se debe tomar ante incidentes por Software Necesario.	

Historia de Usuario	
Número: 41	**Usuario:** Auditor
Nombre de Historia: Visualizar Alertas no Previstas por Falta de Auditoría Requerida	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema la sugerencia de acción a correctiva a tomar ante alertas por Falta de Auditoría Requerida.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Alerta > Alerta No Prevista, debo poder visualizar en la sección Componentes Afectados las alertas por Falta de Auditoría Requerida.	

Historia de Usuario	
Número: 42	**Usuario:** Auditor
Nombre de Historia: Visualizar Incidentes por Falta de Auditoría Requerida	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema los Incidentes por Falta de Auditoría Requerida.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Equipo Informático, debo poder visualizar en la sección Componentes del Equipo los Incidentes por Falta de Auditoría Requerida.	

Historia de Usuario	
Número: 43	**Usuario:** Auditor
Nombre de Historia: Visualizar Sugerencias de acciones correctivas por Falta de Auditoría Requerida	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema los incidentes por Falta de Auditoría Requerida.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Mensajes, debo poder visualizar la sugerencia del sistema sobre qué acción correctiva se debe tomar ante incidentes por Falta de Auditoría Requerida.	

Historia de Usuario	
Número: 44	**Usuario:** Auditor
Nombre de Historia: Visualizar Alertas no Previstas por Incumplimiento de Build Mínimo.	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema las alertas por Incumplimiento de Build Mínimo.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Alerta > Alerta No Prevista, debo poder visualizar en la sección Componentes Afectados las alertas por Incumplimiento de Build Mínimo.	

Historia de Usuario	
Número: 45	**Usuario:** Auditor
Nombre de Historia: Visualizar Incidentes por Incumplimiento de Build Mínimo	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema los Incidentes por Incumplimiento de Build Mínimo.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Equipo Informático, debo poder visualizar en la sección Componentes del Equipo los Incidentes por Incumplimiento de Build Mínimo.	

Historia de Usuario	
Número: 46	**Usuario:** Auditor
Nombre de Historia: Visualizar Sugerencias de acciones correctivas por Incumplimiento de Build Mínimo.	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 3	**Iteración Asignada: 7**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema los alertas por Incumplimiento de Build Mínimo Requerido.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Incidentes > Listado General > Aplicar Filtro (con o sin valores) > Seleccionar Editar en el Incidente deseado > Mensajes, debo poder visualizar la sugerencia del sistema sobre qué acción correctiva se debe tomar ante incidentes por Incumplimiento de Build Mínimo Requerido.	

Historia de Usuario	
Número: 47	**Usuario:** Auditor
Nombre de Historia: Visualizar Lista de Software Prohibido	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada:** 2
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema los software prohibidos ya cargados en el sistema.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Software Prohibido debo poder visualizar la lista de Software Prohibido.	

Historia de Usuario	
Número: 48	**Usuario:** Auditor
Nombre de Historia: Filtrar Lista de Software Prohibido	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada:** 2
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder filtrar en el sistema la lista de los software prohibidos ya cargados en el sistema.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Software Prohibido debo poder filtrar la lista de Software Prohibido.	

Historia de Usuario	
Número: 49	**Usuario:** Auditor
Nombre de Historia: Visualizar Lista de Software Necesario	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema un software necesario ya cargado en el sistema.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Software Necesario debo poder visualizar la lista de Software Necesario.	

Historia de Usuario	
Número: 50	**Usuario:** Auditor
Nombre de Historia: Filtrar Lista de Software Necesario	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder filtrar en el sistema la lista de software necesario ya cargado en el sistema.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Software Necesario debo poder filtrar la lista de Software Necesario.	

Historia de Usuario	
Número: 51	**Usuario:** Auditor
Nombre de Historia: Visualizar Lista de Software Sensible	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema la lista de software sensible ya cargados.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Software Sensible debo visualizar la lista de Software Sensibles ya cargados.	

Historia de Usuario	
Número: 52	**Usuario:** Auditor
Nombre de Historia: Filtrar la lista de Software Sensible	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada:** 3
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder filtrar en el sistema la lista de software sensible ya cargados.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Software Sensible debo filtrar la lista de Software Sensibles ya cargados.	

Historia de Usuario	
Número: 53	**Usuario:** Auditor
Nombre de Historia: Visualizar Lista de Tipo de Software	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada: 4**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema la lista de tipo de software.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Tipo de Software debo poder visualizar la lista de Tipos de Software previamente cargados.	

Historia de Usuario	
Número: 54	**Usuario:** Auditor
Nombre de Historia: Filtrar Lista de Tipo de Software	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 5	**Iteración Asignada: 4**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder filtrar en el sistema la lista de tipo de software.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Tipo de Software debo poder filtrar la lista de Tipos de Software previamente cargados.	

Historia de Usuario	
Número: 55	**Usuario:** Auditor
Nombre de Historia: Visualizar Periodicidad de Auditorías Necesarias	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada:** 5
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar la periodicidad necesaria para realizar las auditorías	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Auditorías Necesarias debo poder visualizar el periodo en el cual debe realizarse al menos una auditoría.	

Historia de Usuario	
Número: 56	**Usuario:** Auditor
Nombre de Historia: Visualizar Build Requerido para Equipos con Windows	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada: 6**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema el número de build mínimo requerido para equipos con sistema operativo Windows.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Build Requerido Windows debo poder visualizar el número de build mínimo requerido para los equipos con sistema operativo Windows.	

Historia de Usuario	
Número: 57	**Usuario:** Auditor
Nombre de Historia: Visualizar Kernel Requerido para Equipos con Linux	
Prioridad en Negocio: Alta	**Riesgo en Desarrollo:** Baja
Puntos Estimados: 1	**Iteración Asignada: 6**
Programador Responsable: Nabila Gudiño Ochoa	
Descripción: Como Auditor quiero poder visualizar en el sistema el número de kernel mínimo requerido para equipos con sistema operativo Linux.	
Validación: Dado que he ingresado como usuario Auditor, al ingresar a la sección Información > Build Requerido Linux debo poder visualizar el número de kernel mínimo requerido para los equipos con sistema operativo Linux.	

Sprint 1 - Sobre la Investigación, Diseño y Definición de las Políticas de Seguridad Institucional

En esta iteración se busca diseñar y definir la Política de Seguridad de la Información Informatizada.

Como paso inicial se buscó obtener de la normativa IRAM - ISO/IEC 27002 una lista de conceptos que deben obligatoriamente estar incluidos en el documento de Política de Seguridad de una Institución.

Luego de extraer los puntos importantes de la normativa IRAM - ISO/IEC 27002, se procedió a leer las Circulares Informáticas del Instituto Universitario Aeronáutico emitidas por la Fuerza Aérea Argentina.

Completados los pasos anteriores, se procedió a ordenar los títulos que tendría la Política de Seguridad. Finalmente la Política quedó dispuesta de la siguiente manera:

1. **Introducción:** presentación del documento.
2. **Términos y Definiciones:** diccionario de palabras técnicas que serán utilizadas en el documento.
3. **Política de Seguridad de la Información Informatizada:** objetivos y sanciones previstas por incumplimiento del presente documento.
4. **Clasificación y Control de Activos:** se especifica cómo se deben inventariar los activos institucionales.
5. **Seguridad del Personal:** se detalla información sobre la asignación de los activos a cada individuo de la Institución y la respuesta ante incidentes y/o anomalías con los equipos.
6. **Seguridad de la Red y los Equipos:** se informa lo concerniente a la protección contra el software malicioso, restricciones en la instalación y uso de software específico, protección de la

integridad de los equipos, actualización del sistema operativo de los mismos y especificaciones sobre la periodicidad de las auditorías obligatorias. Además detalla cuándo un equipo no puede permanecer en la red y define de quién es la responsabilidad ante este tipo de incidentes.

7. **Anexo 1 - Lista de Software Prohibido:** se enumeran los softwares prohibidos divididos por categoría.
8. **Anexo 2 - Lista de Software Requerido:** se enumeran los softwares requeridos divididos por categoría.
9. **Anexo 3 - Lista de Software Sensible:** se enumeran los elementos software que en caso de ser alterados sin autorización previa, generarán una alerta.
10. **Anexo 4 - Lista de Hardware Sensible:** se enumeran los elementos hardware que en caso de ser alterados sin autorización previa, generarán una alerta.

En la sección de Anexo del presente Trabajo Final de Grado se encuentra la Política de Seguridad creada para este Trabajo Final de Grado.

Sprint 2 - Sobre el Software Prohibido

En esta iteración se busca cumplir la sección 7 de la Política de Seguridad propuesta que trata sobre:

- Sección 7 - Seguridad de la Red y los Equipos

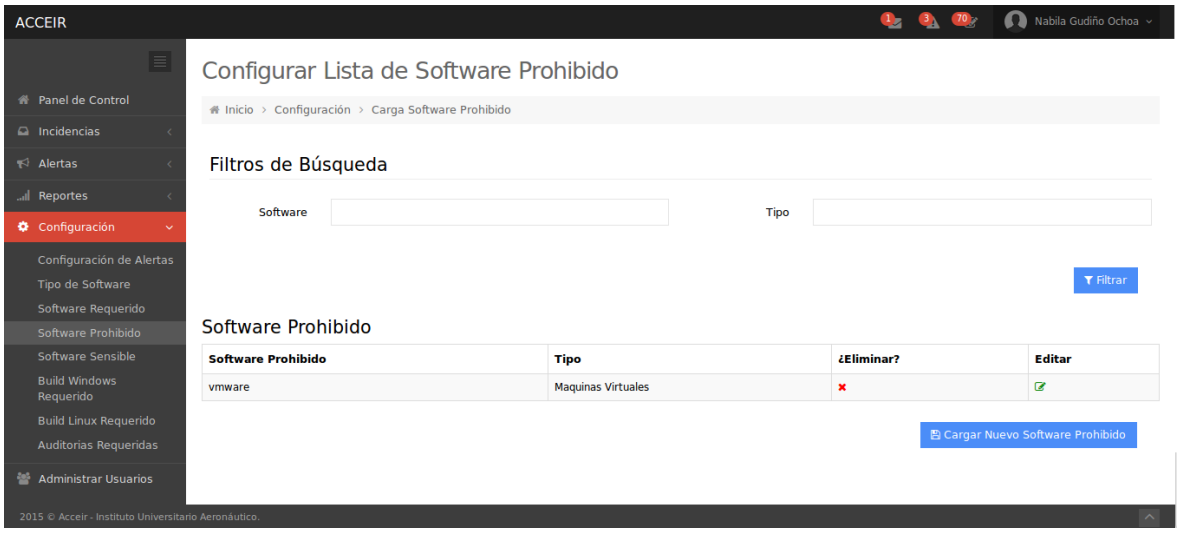
Para lograr esto se creó el Módulo de Software Prohibido. Este módulo tendrá la función de visualizar, crear, modificar y/o eliminar elementos software de la lista de Software Prohibido.

La pantalla principal está compuesta por dos secciones. La primera es una sección de filtros de búsqueda donde el Jefe Auditor o Auditor puede ingresar filtros para que se apliquen en la Lista de Software Prohibido. La segunda sección es la Lista de Software Prohibido propiamente dicha. El usuario Auditor sólo puede visualizar la lista. El usuario Jefe Auditor tiene habilitado un botón para agregar nuevos valores a la lista actual y en la misma tabla donde visualiza los elementos ya cargados en la lista, tiene habilitados botones que le permitirán Eliminar o Editar un valor de la lista.

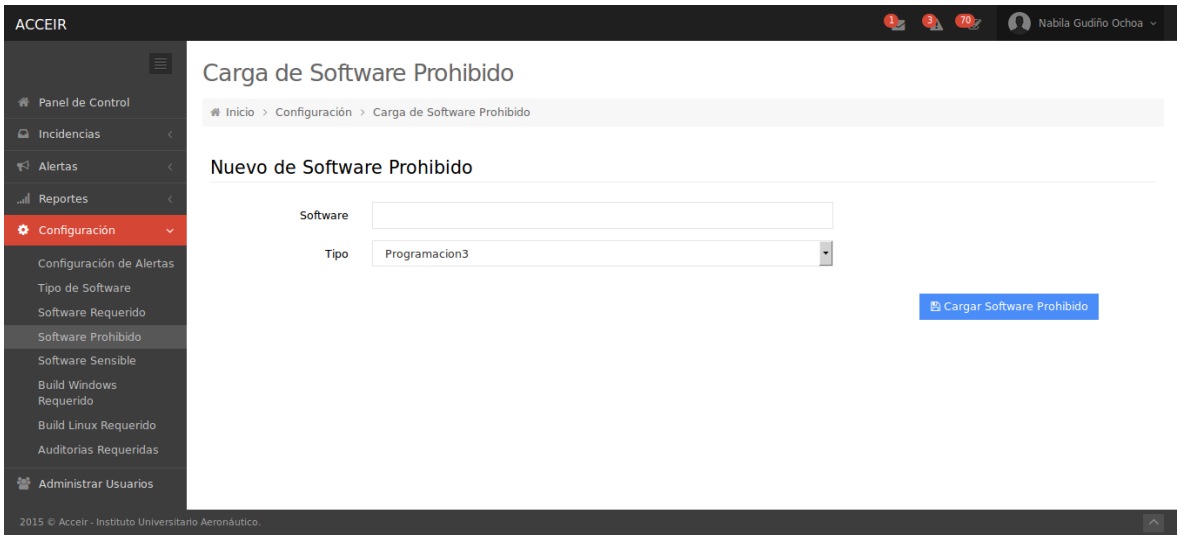
Al finalizar esta iteración quedan completadas las siguientes historias de usuario:

- 1: Cargar Software Prohibido
- 2: Eliminar Software Prohibido
- 3: Editar Software Prohibido
- 4: Visualizar Software Prohibido ya cargado
- 5: Filtrar Software Prohibido ya cargado
- 47: Visualizar Lista de Software Prohibido
- 48: Filtrar Lista de Software Prohibido

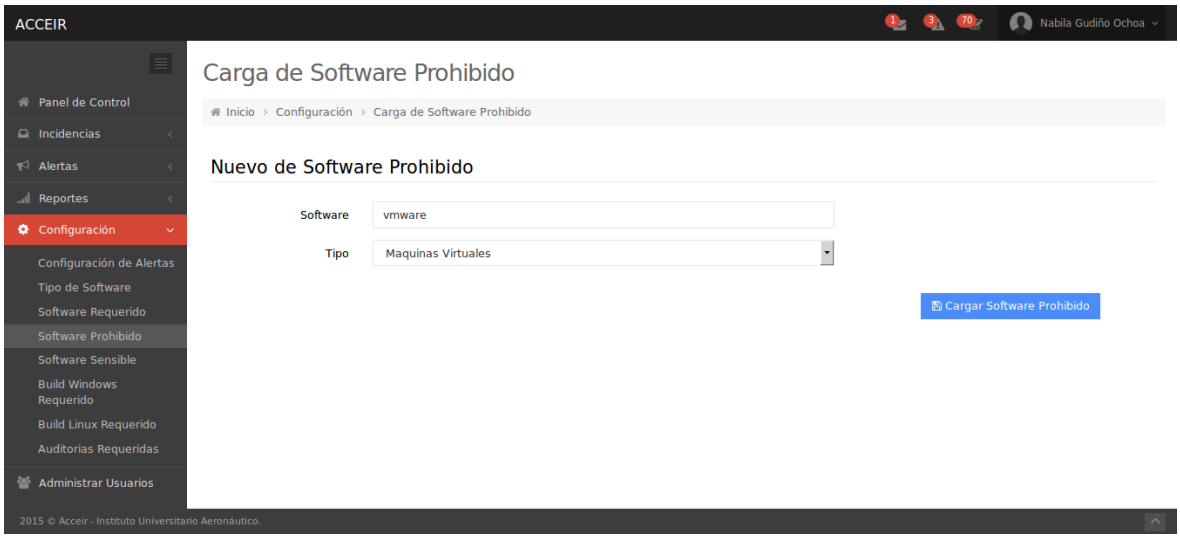
A continuación se presentan las pantallas que serán visibles para el Jefe Auditor desde Configuración > Software Prohibido y para los Auditores desde Información > Software Prohibido:



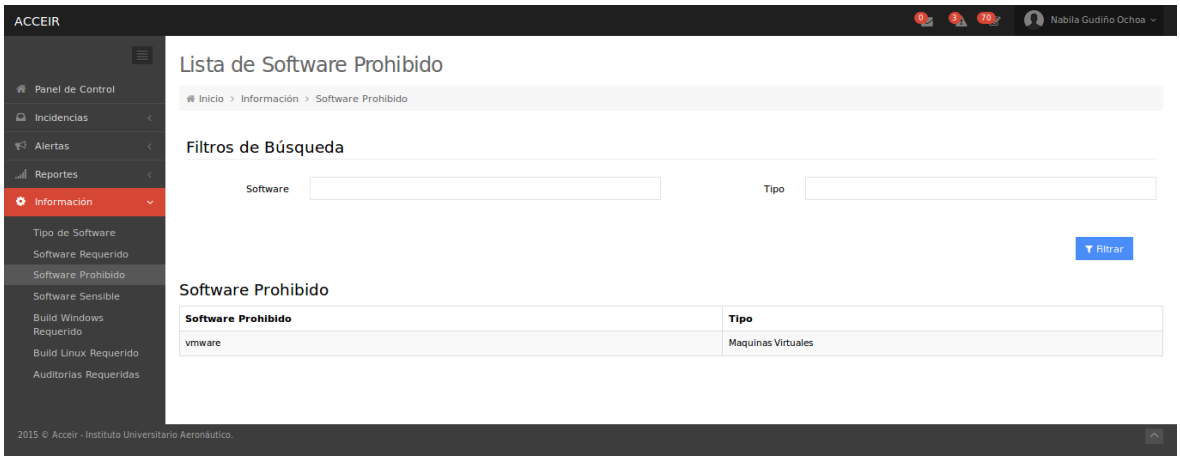
Captura 1 - Software Prohibido (Jefe Auditor)



Captura 2 - Carga de Nuevo Software Prohibido (Jefe Auditor)



Captura 3 - Edición de Software Prohibido (Jefe Auditor)



Captura 4 - Software Prohibido (Auditor)

Sprint 3 - Sobre el Software Necesario

En esta iteración se busca cumplir la sección 7 de la Política de Seguridad propuesta que trata sobre:

- Sección 7 - Seguridad de la Red y los Equipos

Para lograr esto se creó el Módulo de Software Necesario. Este módulo tendrá la función de visualizar, crear, modificar y/o eliminar elementos software de la lista de Software Necesario.

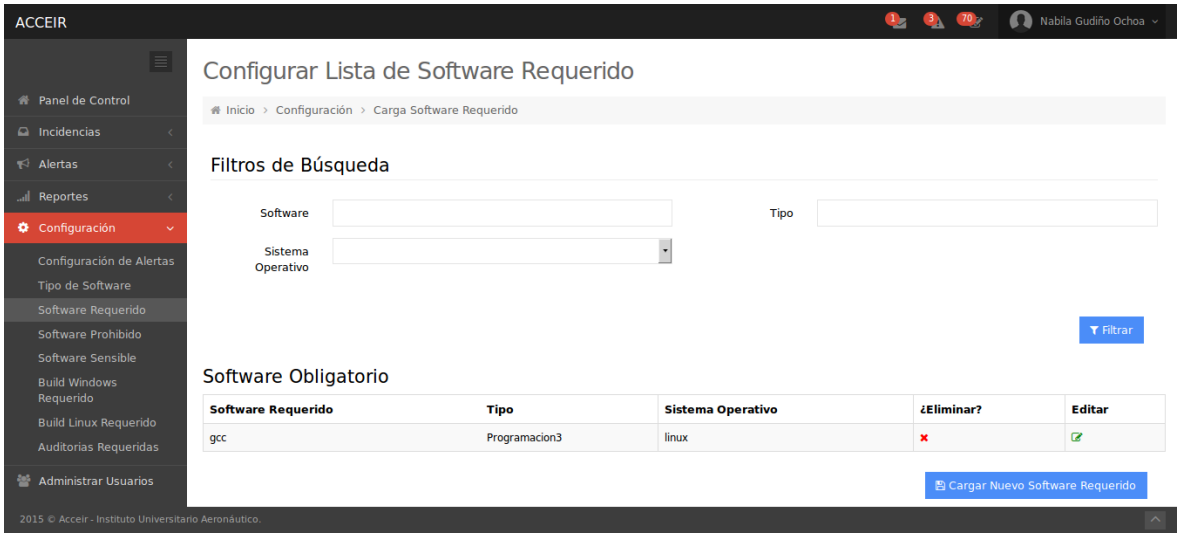
La pantalla principal está compuesta por dos secciones. La primera es una sección de filtros de búsqueda donde el Jefe Auditor o Auditor puede ingresar filtros para que se apliquen en la Lista de Software Necesario. La segunda sección es la Lista de Software Necesario propiamente dicha. El usuario Auditor sólo puede visualizar la lista. El usuario Jefe Auditor tiene

habilitado un botón para agregar nuevos valores a la lista actual y en la misma tabla donde visualiza los elementos ya cargados en la lista, tiene habilitados botones que le permitirán Eliminar o Editar un valor de la lista.

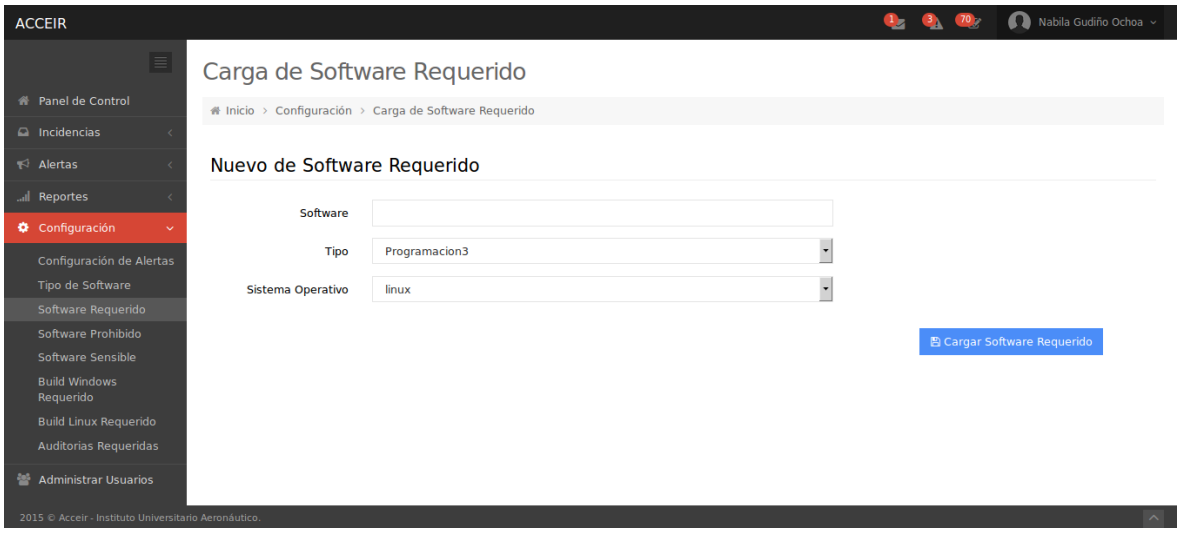
Al finalizar esta iteración quedan completadas las siguientes historias de usuario:

- 6: Cargar Software Necesario
- 7: Eliminar Software Necesario
- 8: Editar Software Necesario
- 9: Visualizar Software Necesario ya cargado
- 10: Filtrar Software Necesario ya cargado
- 49: Visualizar Lista de Software Necesario
- 50: Filtrar Lista de Software Necesario

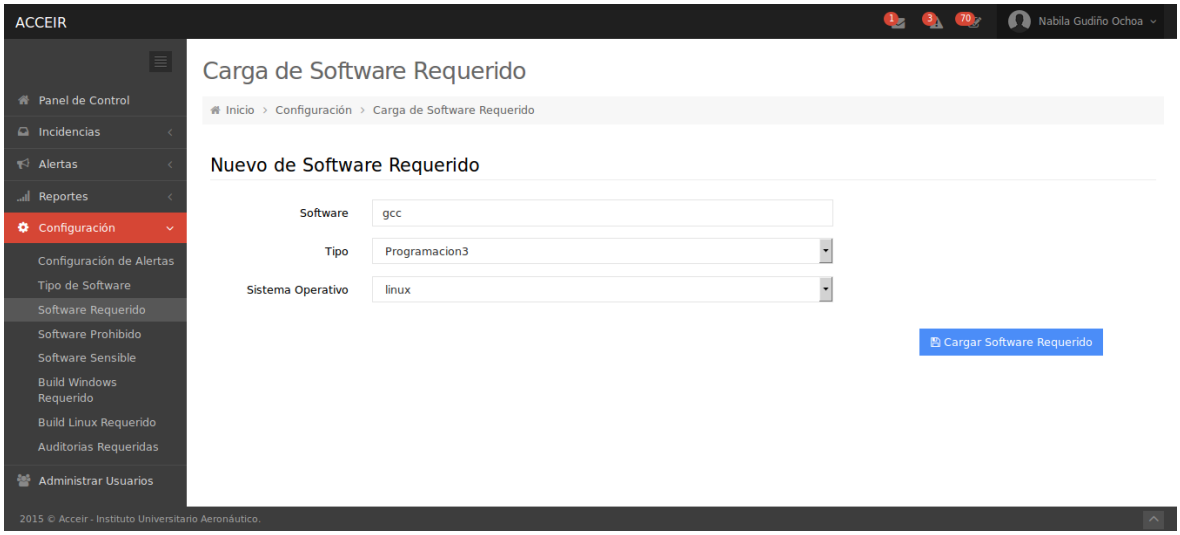
A continuación se presentan las pantallas que serán visibles para el Jefe Auditor desde Configuración > Software Requerido y para los Auditores desde Información > Software Requerido:



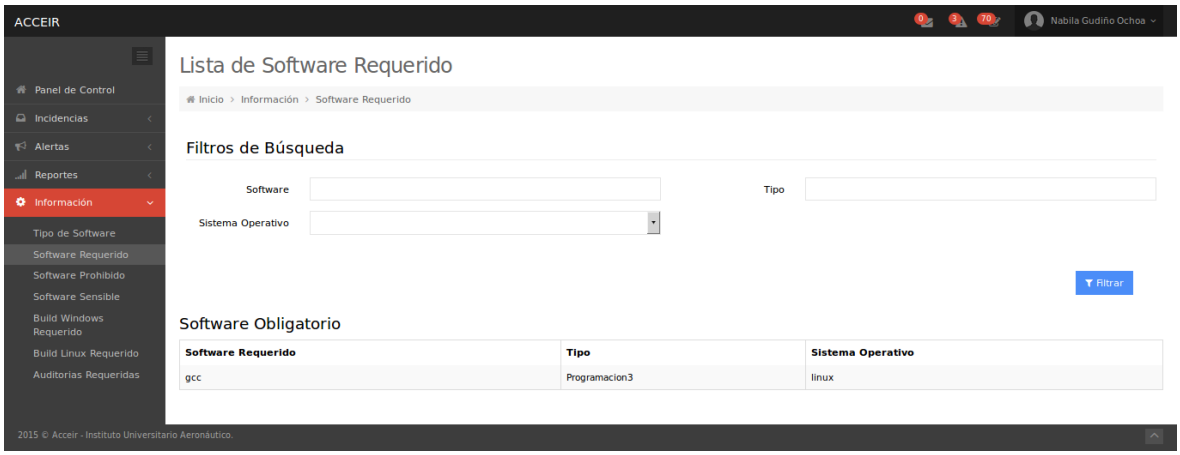
Captura 5 - Software Requerido (Jefe Auditor)



Captura 6 - Carga de Software Requerido (Jefe Auditor)



Captura 7 - Edición de Software Requerido (Jefe Auditor)



Captura 8 - Software Requerido (Auditor)

Sprint 4 - Sobre el Software Sensible

En esta iteración se busca cumplir la sección 7 de la Política de Seguridad propuesta que trata sobre:

- Sección 7 - Seguridad de la Red y los Equipos

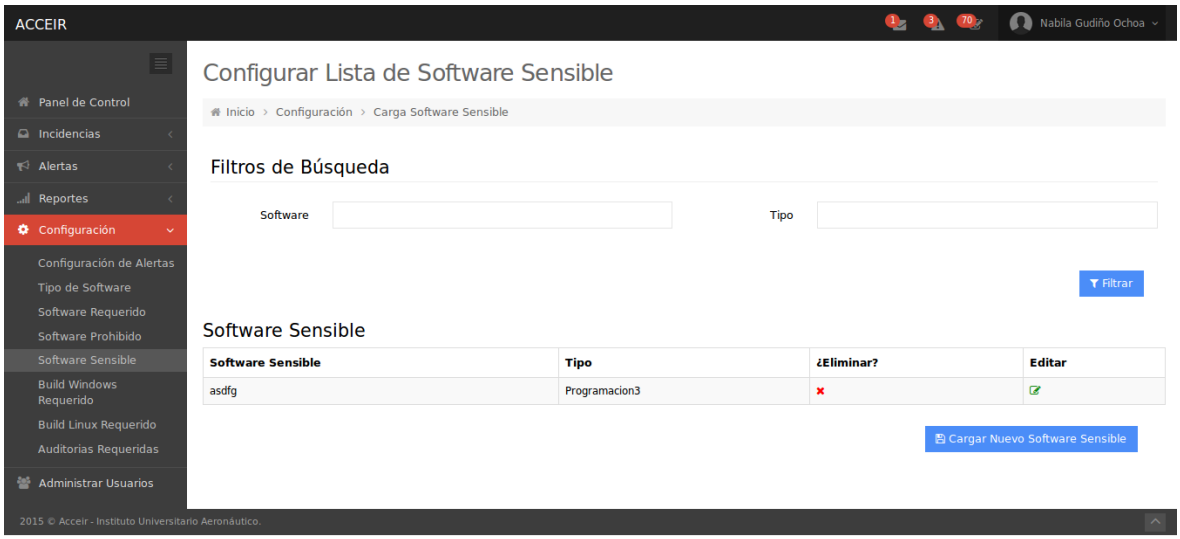
Para lograr esto se creó el Módulo de Software Sensible. Este módulo tendrá la función de visualizar, crear, modificar y/o eliminar elementos software de la lista de Software Sensible.

La pantalla principal está compuesta por dos secciones. La primera es una sección de filtros de búsqueda donde el Jefe Auditor o Auditor puede ingresar filtros para que se apliquen en la Lista de Software Sensible. La segunda sección es la Lista de Software Sensible propiamente dicha. El usuario Auditor sólo puede visualizar la lista. El usuario Jefe Auditor tiene habilitado un botón para agregar nuevos valores a la lista actual y en la misma tabla donde visualiza los elementos ya cargados en la lista, tiene habilitados botones que le permitirán Eliminar o Editar un valor de la lista.

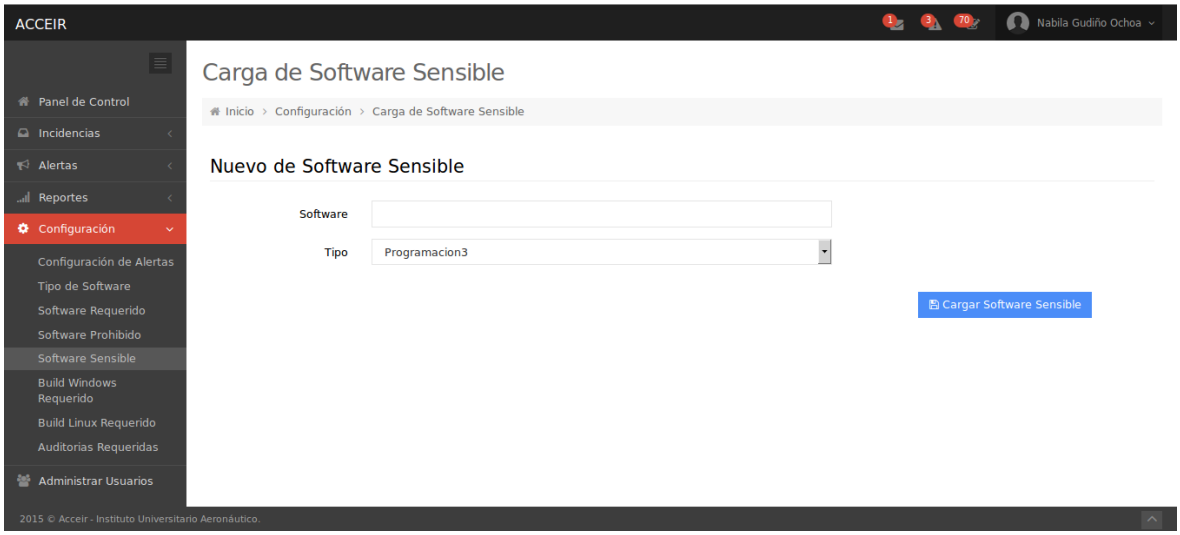
Al finalizar esta iteración quedan completadas las siguientes historias de usuario:

- 11: Cargar Software Sensible
- 12: Eliminar Software Sensible
- 13: Editar Software Sensible
- 14: Visualizar Software Sensible ya cargado
- 15: Filtrar Software Sensible ya cargado
- 51: Visualizar Lista de Software Sensible
- 52: Filtrar la lista de Software Sensible

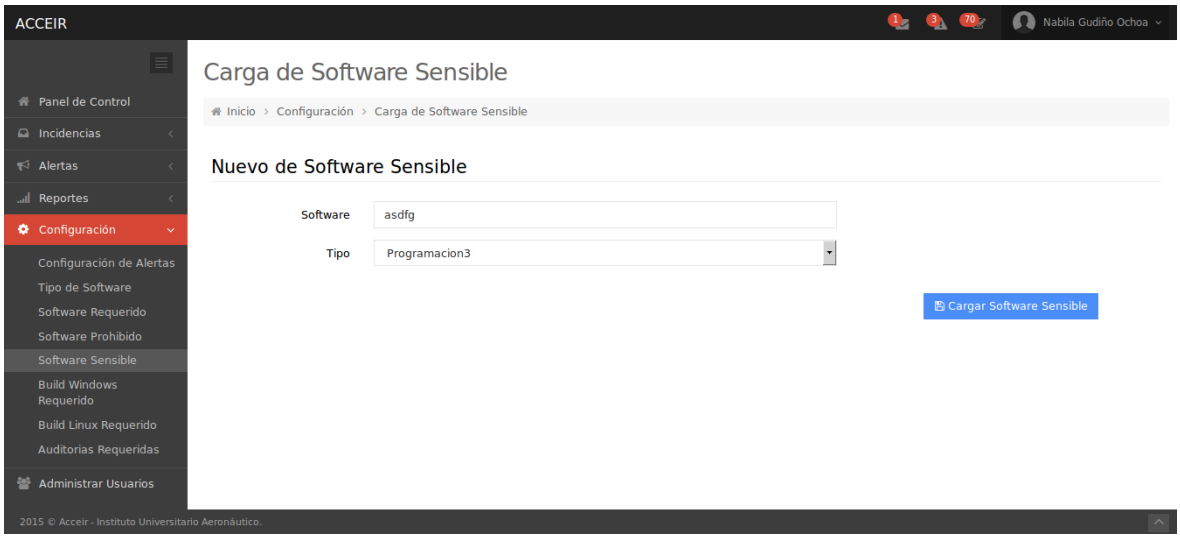
A continuación se presentan las pantallas que serán visibles para el Jefe Auditor desde Configuración > Software Sensible y para los Auditores desde Información > Software Sensible:



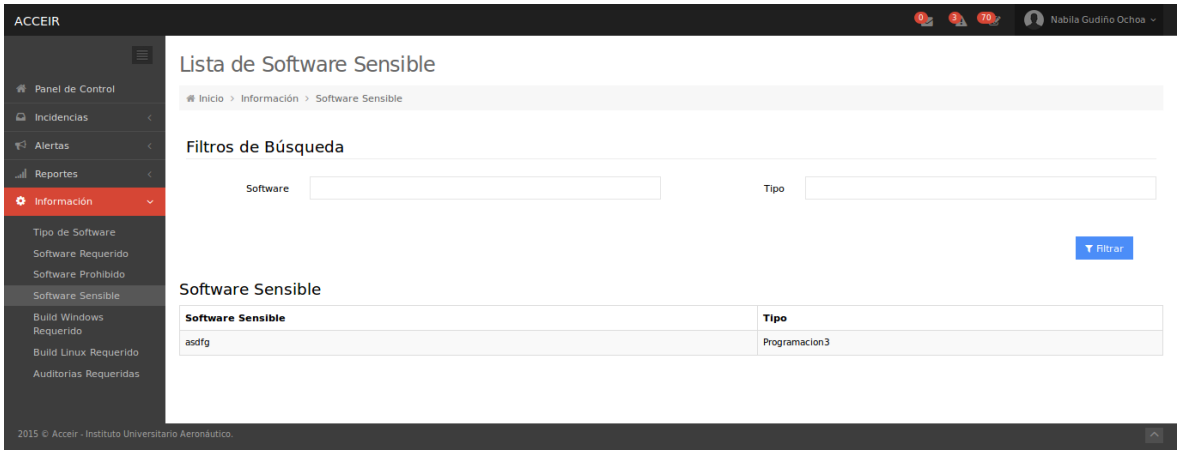
Captura 9 - Software Sensible (Jefe Auditor)



Captura 10 - Carga de Software Sensible(Jefe Auditor)



Captura 11 - Edición de Software Sensible (Jefe Auditor)



Captura 12 - Software Sensible (Auditor)

Sprint 5 - Sobre el Tipo de Software y Configuración de Alertas

En esta iteración se busca cumplir la sección 7 de la Política de Seguridad propuesta que trata sobre:

- Sección 7 - Seguridad de la Red y los Equipos

Para que las secciones anteriores tuvieran la capacidad de ser aplicadas a equipos de manera conjunta, se creó el Módulo de Tipo de Software. Este módulo tendrá la función de visualizar, crear, modificar y/o eliminar elementos de la lista de Tipos de Software.

La pantalla principal está compuesta por dos secciones. La primera es una sección de filtros de búsqueda donde el Jefe Auditor o Auditor puede ingresar filtros para que se apliquen en la Lista de Tipo de Software. La segunda sección es la Lista de Tipo de Software propiamente dicha. El usuario Auditor sólo puede visualizar la lista. El usuario Jefe Auditor tiene habilitado un

botón para agregar nuevos valores a la lista actual y en la misma tabla donde visualiza los elementos ya cargados en la lista, tiene habilitados botones que le permitirán Eliminar o Editar un valor de la lista.

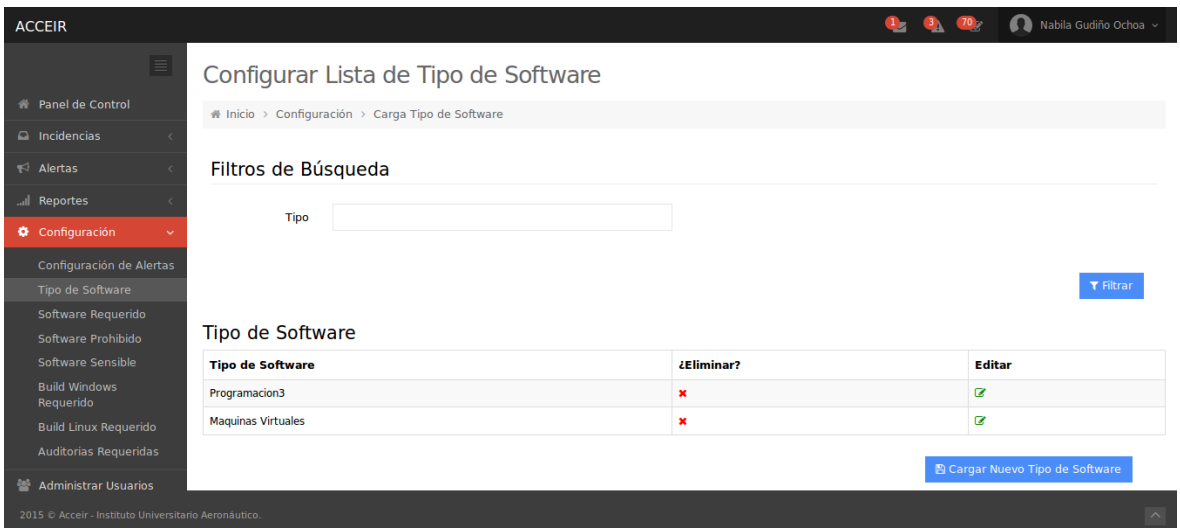
Por otro lado, se necesitaba que las Alertas pudieran ser personalizables, es decir, por ejemplo, si el Jefe Auditor decidía que no era necesario que el sistema genere alertas por Falla en el Build Requerido, debería poder deshabilitar esa alerta en particular de la lista y, el sistema, solo generará alertas sobre los elementos habilitados.

A fin de cumplir con este requerimiento se creó la sección Configuración de alertas. Esta sección es sólo accesible para el Jefe Auditor y se trata de una Lista de todas las alertas disponibles por el sistema, con una casilla de verificación a su lado. Si el Jefe Auditor quiere que el sistema genere alertas por cierto elemento, debe dejar la casilla tildada, en caso contrario, la debe destildar. Finalmente, cuando guarde los cambios haciendo clic en el botón situado bajo la tabla, el sistema solo va generar alertas de los elementos habilitados.

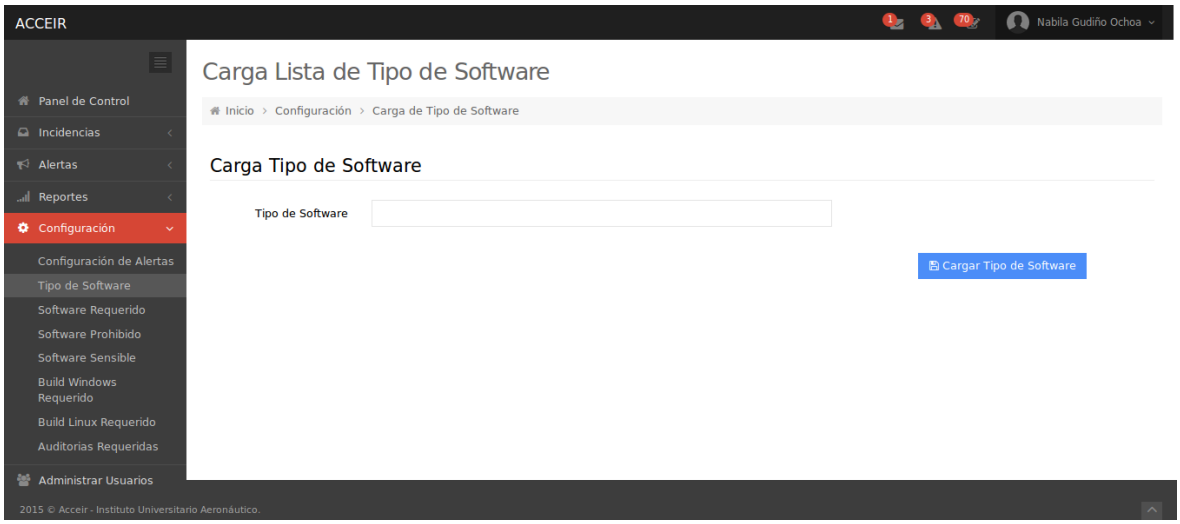
Al finalizar esta iteración quedan completadas las siguientes historias de usuario:

- 18: Cargar Tipo de Software
- 19: Eliminar Tipo de Software
- 20: Editar Tipo de Software
- 21: Visualizar Tipo de Software
- 22: Filtrar Tipo de Software
- 53: Visualizar Lista de Tipo de Software
- 54: Filtrar Lista de Tipo de Software
- 16: Editar Alertas Disponibles
- 17: Visualizar Alertas Disponibles

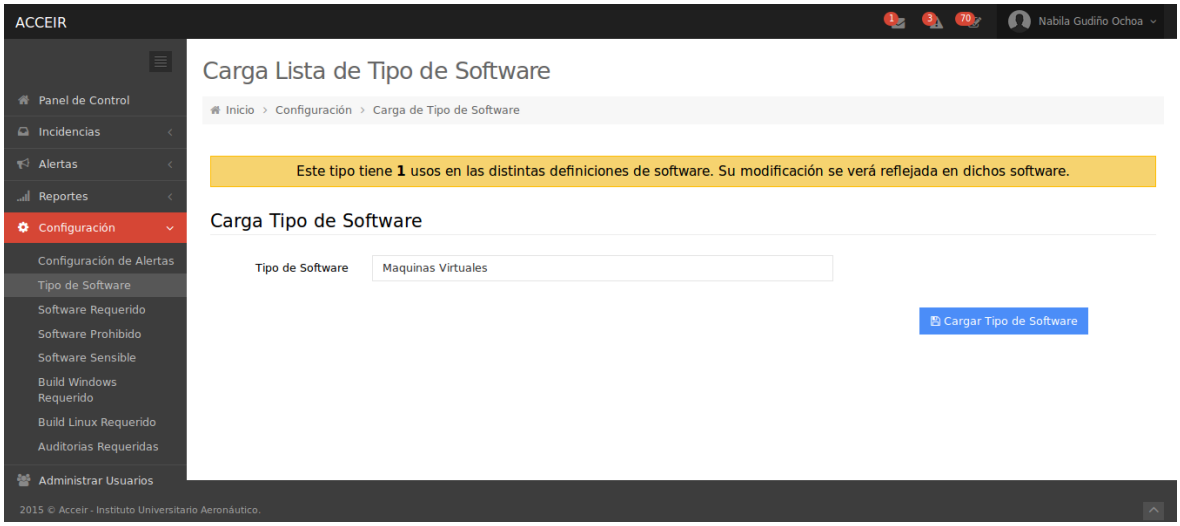
A continuación se presentan las pantallas que serán visibles para el Jefe Auditor desde Configuración > Tipo de Software y para los Auditores desde Información > Tipo de Software:



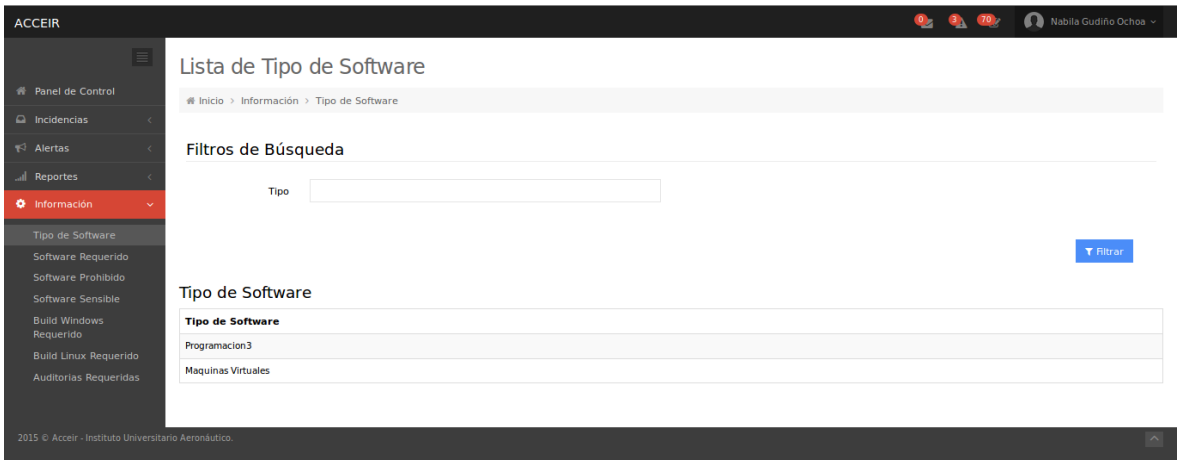
Captura 13 - Tipo de Software (Jefe Auditor)



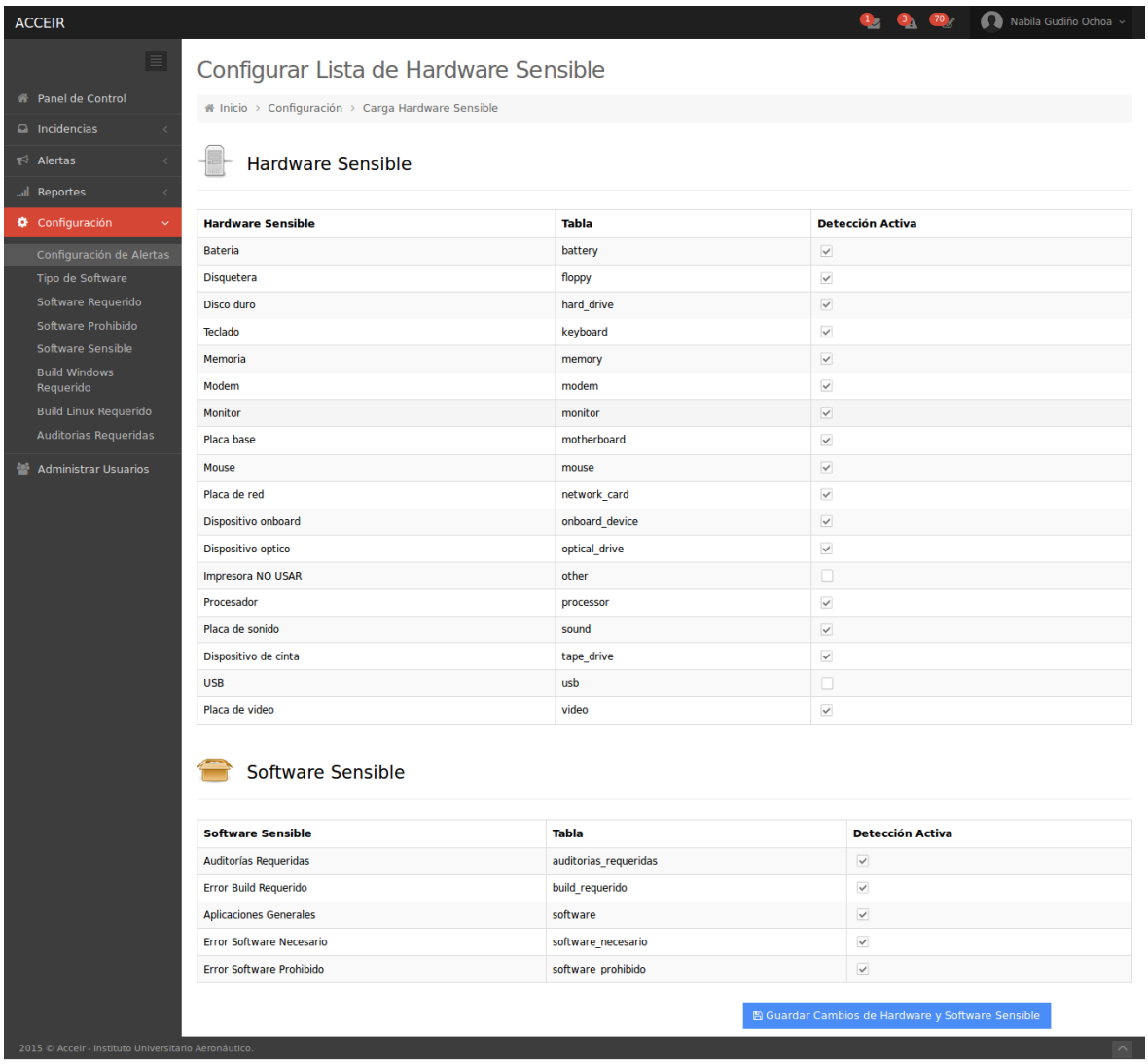
Captura 14 - Carga de Tipo de Software (Jefe Auditor)



Captura 15 - Edición de Tipo de Software (Jefe Auditor)



Captura 16 - Tipo de Software (Auditor)



Captura 17 - Configuración de Alertas (Jefe Auditor)

Sprint 6 - Sobre las Auditorías Necesarias

En esta iteración se busca cumplir la sección 5 y 9 de la Política de Seguridad propuesta que trata sobre:

- Sección 5 - Clasificación y Control de Activos
- Sección 9 - Auditorías Obligatorias

Para lograr esto se creó el Módulo de Auditorías Necesarias. Este módulo tendrá la función de visualizar, asentar por primera vez y/o modificar el periodo en que un equipo de la red debe hacer al menos una auditoría. Este módulo incluye una funcionalidad programada en PHP que se ejecutará en el equipo servidor periódicamente y comprobará si algún equipo de todos los auditados se encuentra por fuera del periodo estipulado.

En este módulo, el periodo está compuesto por *cantidad* y *periodo*. Por ejemplo, si el Jefe Auditor quiere que los equipos se auditen al menos una vez cada 2 meses, en este módulo podrá definir ese periodo ingresando *cantidad 2 y periodo MES*.

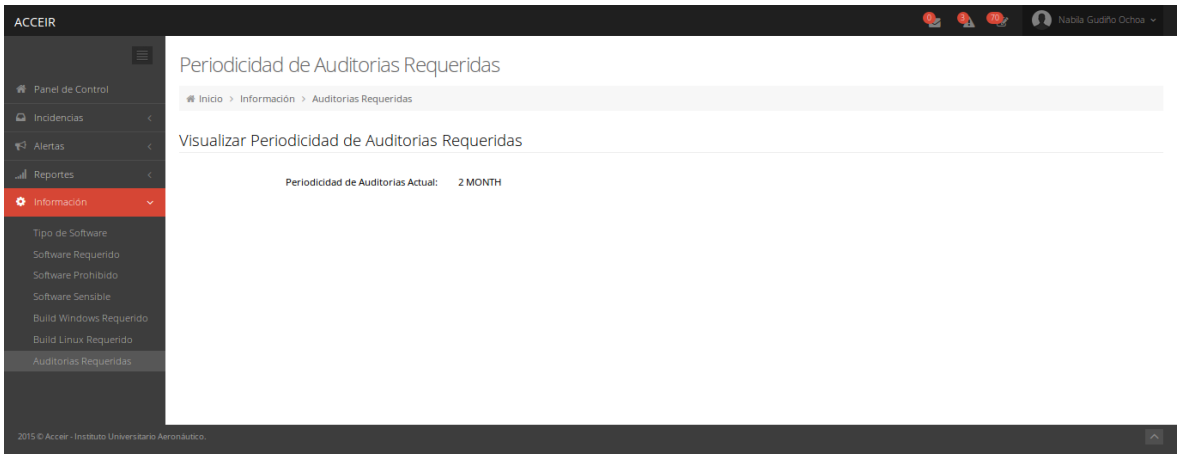
La pantalla principal está compuesta por dos secciones. La primer sección indica, si hay un periodo definido previamente, cuál es el periodo activo actual. La segunda sección solo la tiene habilitada el Jefe Auditor y es para modificar el periodo actual.

Al finalizar esta iteración quedan completadas las siguientes historias de usuario:

- 23: Definir Periodicidad de Auditorías Necesarias
- 24: Modificar la Periodicidad de Auditorías Necesarias
- 25: Visualizar Periodicidad de Auditorías Necesarias
- 55: Visualizar Periodicidad de Auditorías Necesarias

A continuación se presentan las pantallas que serán visibles para el Jefe Auditor desde Configuración > Auditorías Requeridas y para los Auditores desde Información > Auditorías Requeridas:

Captura 18 - Auditorías Requeridas (Jefe Auditor)



Captura 19 - Auditorías Requeridas (Auditor)

Sprint 7 - Sobre el Build Requerido para Windows y Linux

En esta iteración se busca cumplir la sección 8 de la Política de Seguridad propuesta que trata sobre:

- Sección 8 - Actualización de Sistema Operativo de los Equipos

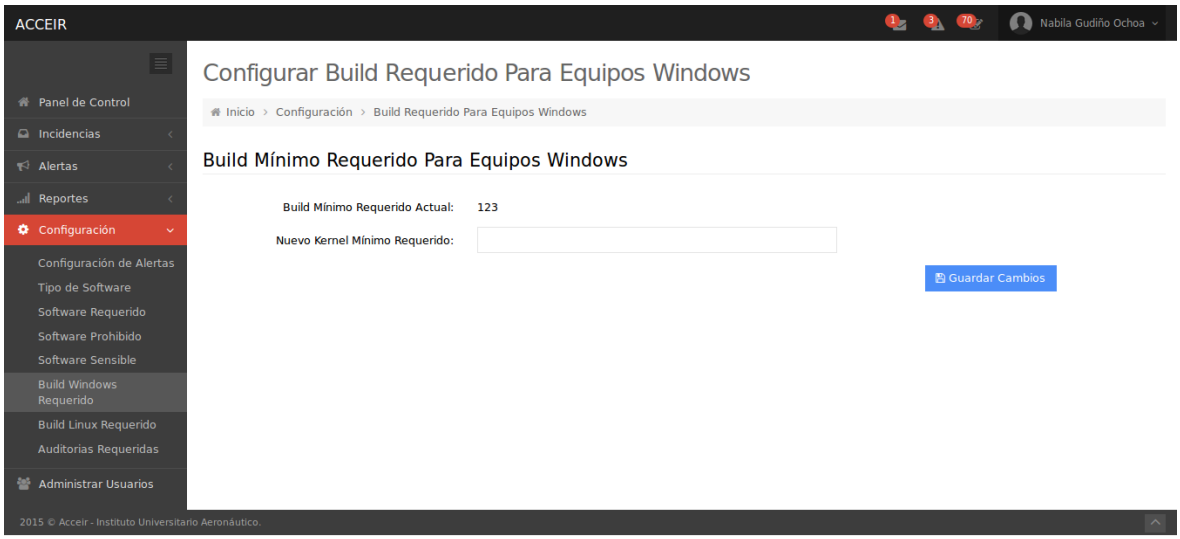
Para lograr esto se creó los Módulos de Build Requerido Windows y Kernel Requerido Linux que funcionan de manera similar, con algunas diferencias debido a que son sistemas operativos diferentes. Estos módulos tendrán la función de visualizar, crear, y/o modificar el número de Build mínimo de Windows o Kernel mínimo de Linux para los equipos de la red.

Las pantallas principales se ven similares entre ellas. Están compuestas por dos secciones. La primer sección indica, si hay un build/ kernel mínimo definido previamente, cuál es el build/ kernel mínimo actual. La segunda sección solo la tiene habilitada el Jefe Auditor y es para modificar el build/kernel actual.

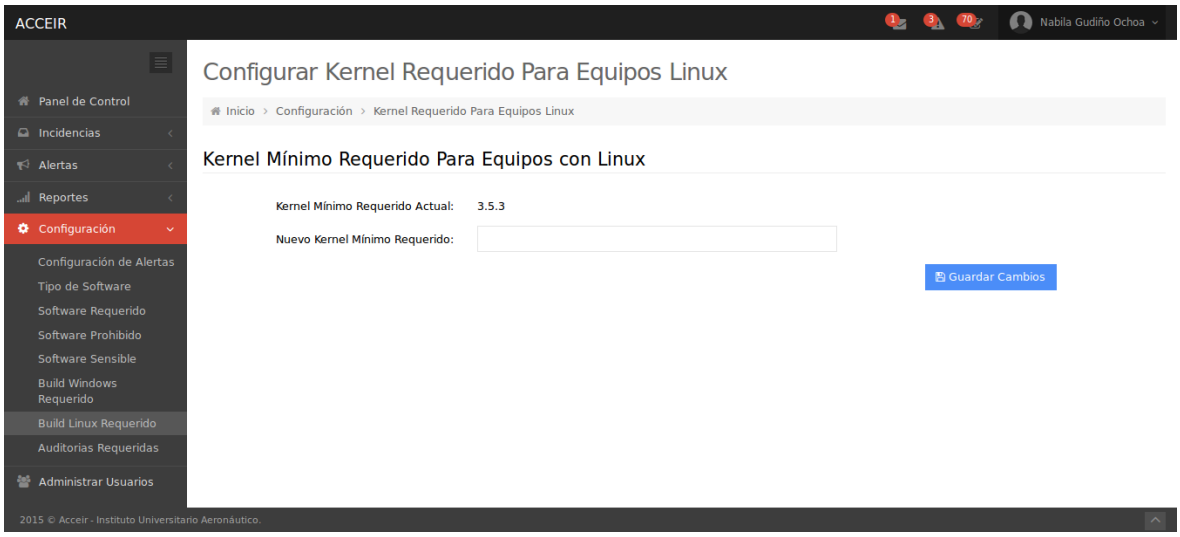
Al finalizar esta iteración quedan completadas las siguientes historias de usuario:

- 26: Cargar Build Requerido para Equipos con Windows
- 27: Modificar Build Requerido para Equipos con Windows
- 28: Visualizar Build Requerido para Equipos con Windows
- 29: Cargar Kernel Requerido para Equipos con Linux
- 30: Modificar Kernel Requerido para Equipos con Linux
- 31: Visualizar Kernel Requerido para Equipos con Linux
- 56: Visualizar Build Requerido para Equipos con Windows
- 57: Visualizar Kernel Requerido para Equipos con Linux

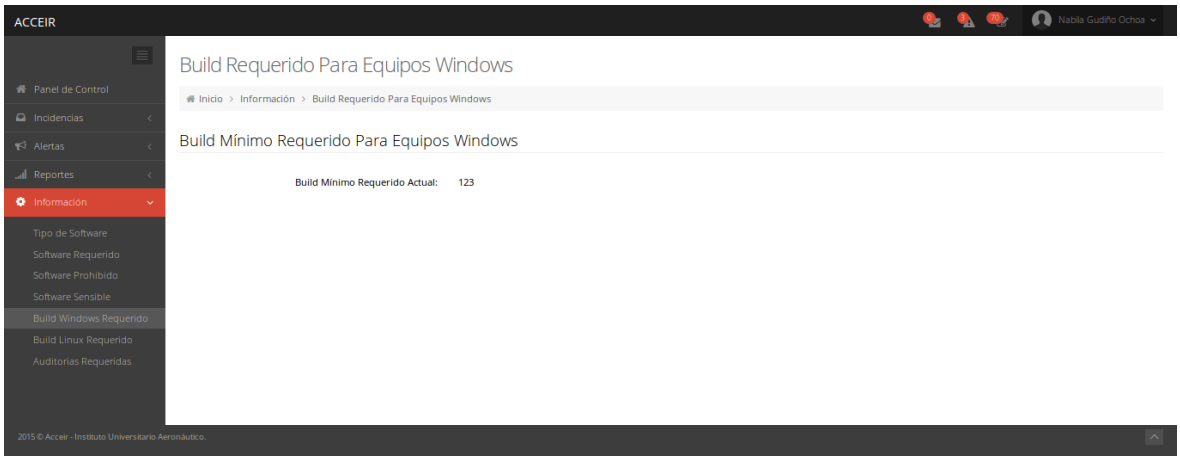
A continuación se presentan las pantallas que serán visibles para el Jefe Auditor desde Configuración > Build Windows Requerido o Configuración > Build Linux Requerido y para los Auditores desde Información > Build Windows Requerido o Información > Build Linux Requerido:



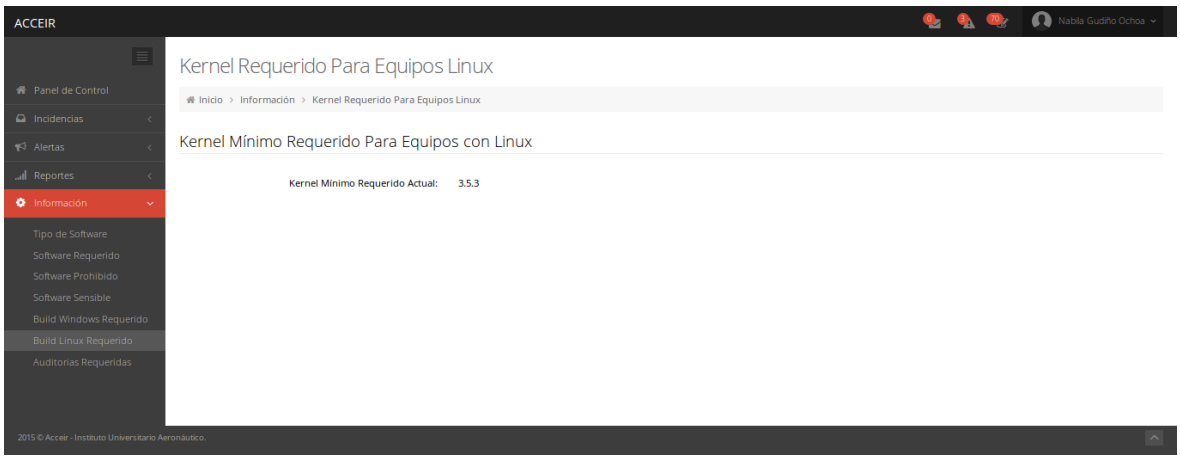
Captura 20 - Build Windows Requerido (Jefe Auditor)



Captura 21 - Build Linux Requerido (Jefe Auditor)



Captura 22 - Build Windows Requerido (Auditor)



Captura 23 - Build Linux Requerido (Auditor)

Sprint 8 - Sobre las Visualizaciones de Alertas, Incidentes y Sugerencias

En esta iteración se busca incluir las nuevas alertas al Proyecto Acceir, si bien en las iteraciones anteriores se podían visualizar las nuevas alertas como parte de las “Alertas por Software”, se creyó útil que las nuevas alertas fueran un tipo de alerta nuevo y distinto de los ya existentes.

Luego de estudiar el Proyecto Acceir y cómo este proyecto creaba alertas nuevas, se decidió crear tablas auxiliares que permitirían al Proyecto Acceir ver a los nuevos módulos como si se trataran de un tipo de alerta más, con una importancia equivalente a las alertas originales por cambios en componentes hardware o software.

Los cambios en el código se verían reflejados en las siguientes secciones:

- **Configuración de Alertas:** aparecerán nuevas alertas disponibles las cuales son: Software Prohibido, Software

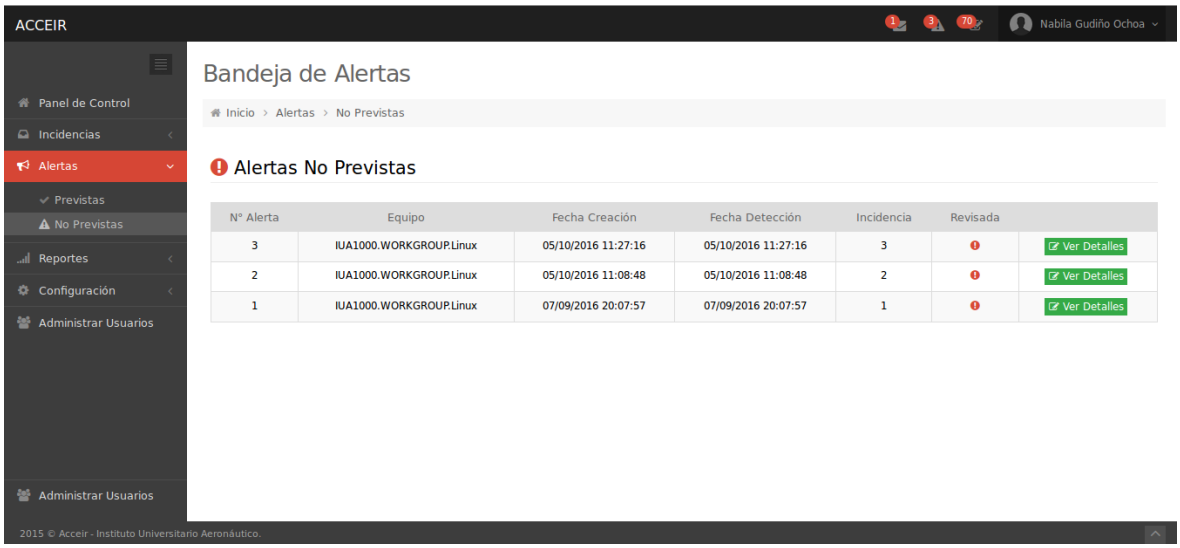
Requerido, Software Sensible, Auditorías Requeridas, Build Requerido Windows, Kernel Requerido Linux.

- **Visualización de Alertas:** en caso de ocurrir, se visualizarán las nuevas alertas mencionadas en el punto anterior.
- **Visualización de Incidentes:** en caso de ocurrir, se visualizarán las nuevas alertas mencionadas en el primer punto.
- **Visualización de Sugerencias:** como punto a favor de la modificación de esta iteración, se podía definir mensajes que complementen a la descripción de alerta. Se utilizó esta sección para poder indicar sugerencias de acción para el Auditor responsable para atender dicha alerta. Por ejemplo, en caso de una alerta por Build Requerido de Windows, el mensaje dirá que se sugiere que el auditor actualice la versión de sistema operativo por la mínima requerida.

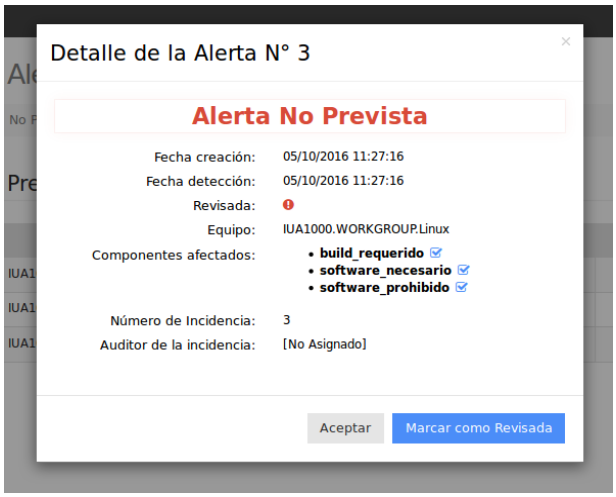
Al finalizar esta iteración quedan completadas las siguientes historias de usuario:

- 32: Visualizar Alertas no Previstas por Software Prohibido
- 33: Visualizar Incidentes por Software Prohibido
- 34: Visualizar Sugerencias de acciones correctivas por Software Prohibido
- 35: Visualizar Alertas no Previstas por Software Sensible
- 36: Visualizar Incidentes por Software Prohibido
- 37: Visualizar Sugerencias de acciones correctivas por Software Sensible
- 38: Visualizar Alertas no Previstas por Software Necesario
- 39: Visualizar Incidentes por Software Necesario
- 40: Visualizar Sugerencias de acciones correctivas por Software Necesario
- 41: Visualizar Alertas no Previstas por Falta de Auditoría Requerida
- 42: Visualizar Incidentes por Falta de Auditoría Requerida
- 43: Visualizar Sugerencias de acciones correctivas por Falta de Auditoría Requerida
- 44: Visualizar Alertas no Previstas por Incumplimiento de Build Mínimo
- 45: Visualizar Incidentes por Incumplimiento de Build Mínimo
- 46: Visualizar Sugerencias de acciones correctivas por Incumplimiento de Build Mínimo

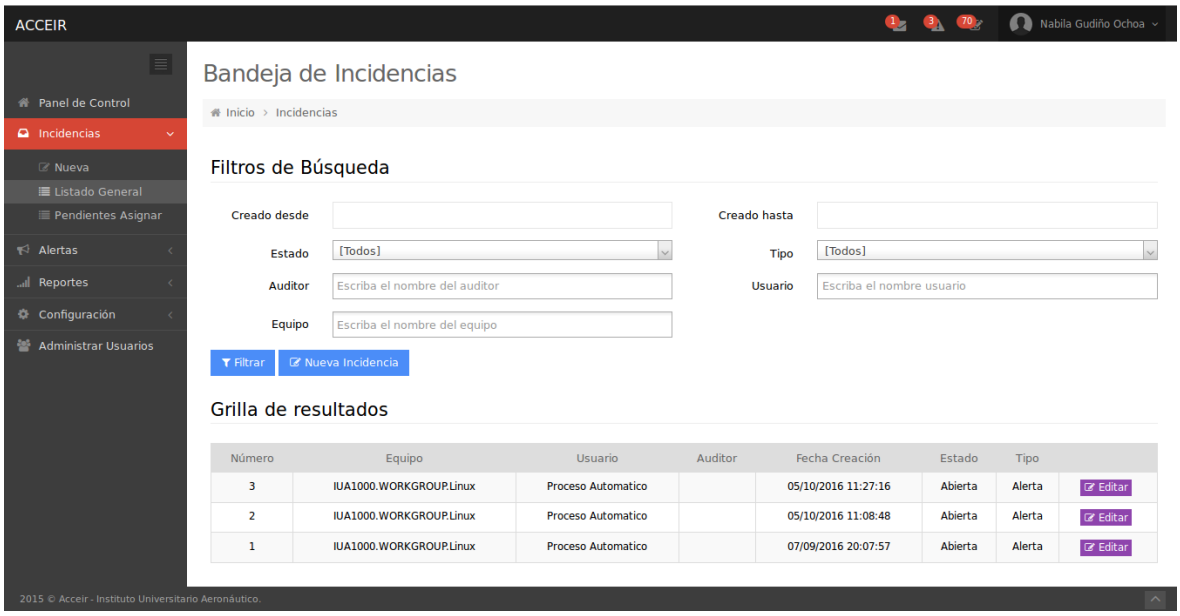
A continuación se presentan las pantallas que serán visibles desde los Menú de Alertas e Incidentes para los usuarios de tipo Jefe Auditor y Auditor.



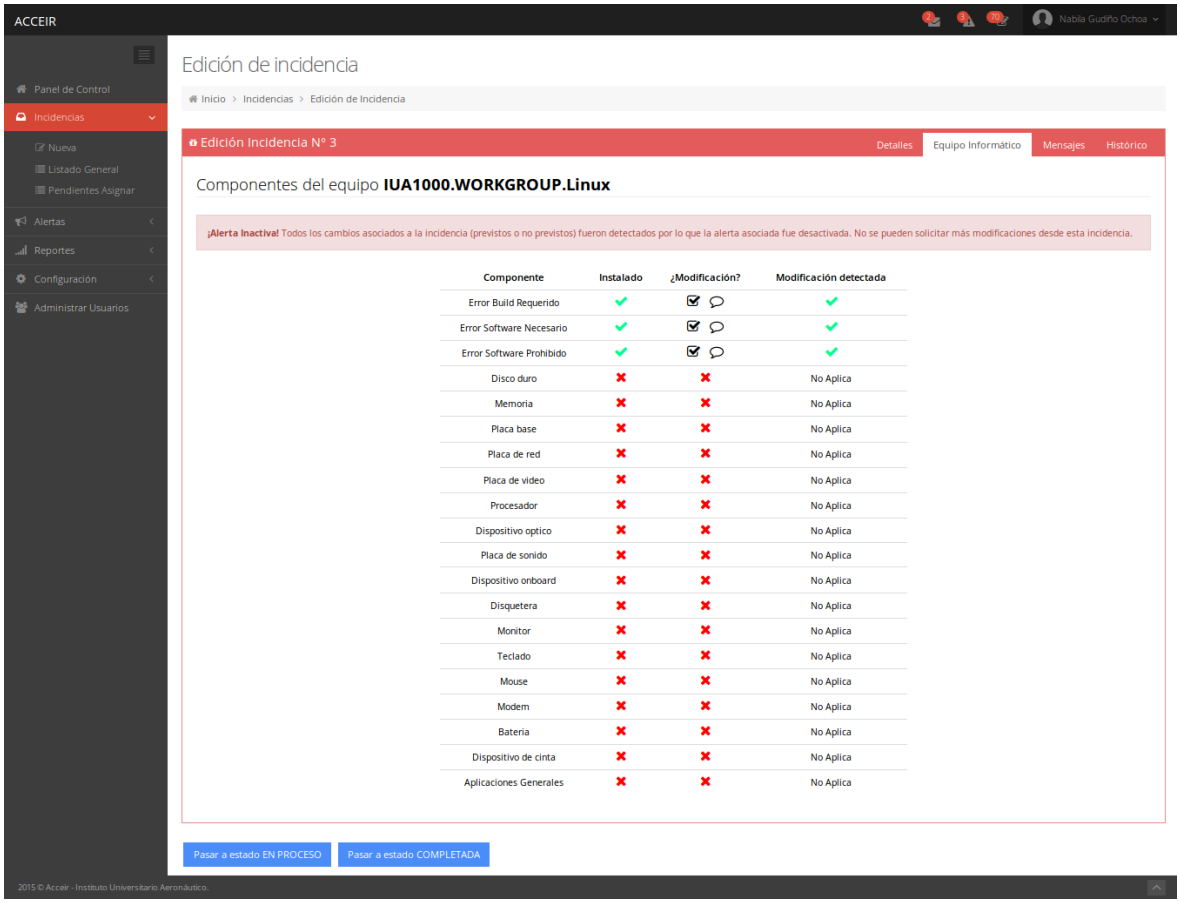
Captura 24 - Visualización de Alertas



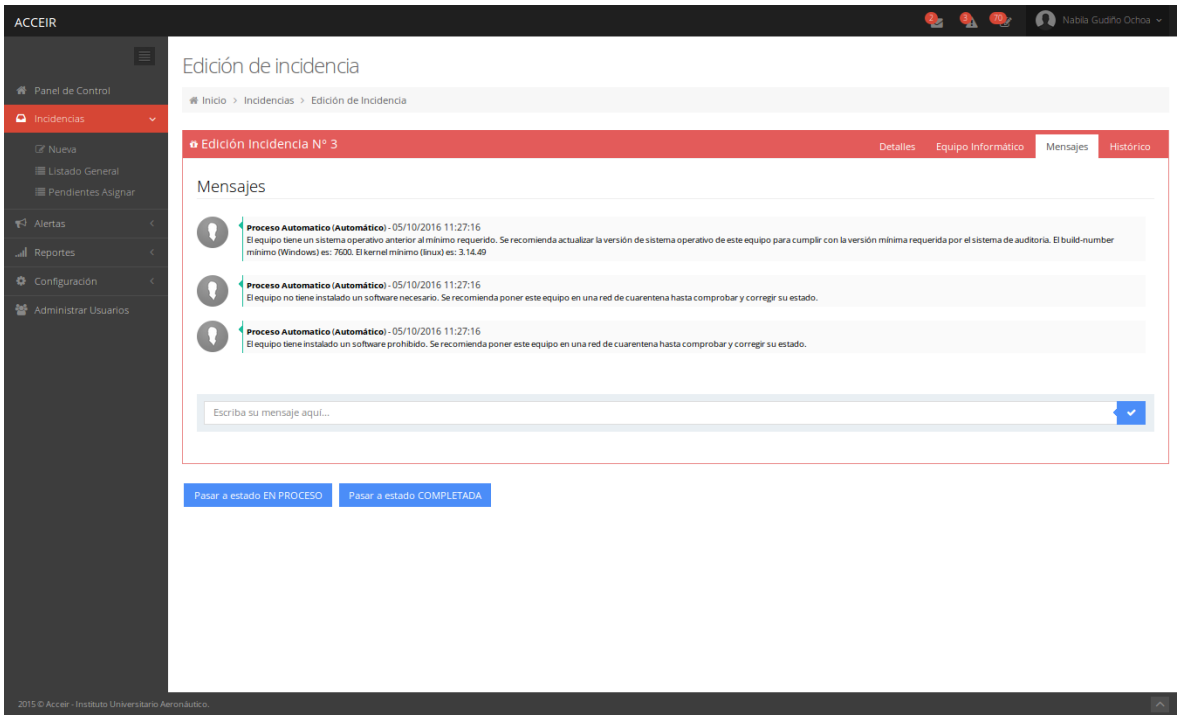
Captura 25 - Visualización de los nuevos tipos de alertas (al hacer clic en Ver Detalles)



Captura 26 - Visualización de Incidencias



Captura 27 - Visualización del detalle del incidente (al hacer clic en Editar > Equipo Informático del Incidente Seleccionado)



Captura 28 - Visualización de Sugerencias (sección Editar > Mensajes del Incidente Seleccionado)

Sprint 9 - Puesta en Marcha y Pruebas Finales

Infraestructura Necesaria

Para cumplir con los objetivos planteados la solución desarrollada tiene una fuerte dependencia con el Proyecto MASI y el Proyecto Acceir. Esta integración hace obligatoria la instalación previa de MASI y Acceir para poder utilizarlo ya que comparten servidor web y servidor de base de datos como se especifica en el diagrama de despliegue. Por esta razón los requerimientos de infraestructura son los mismos que para MASI y Acceir.

Tecnologías y requerimientos a nivel de usuarios

Las mejoras en el sistema Acceir se desarrollaron siguiendo las tecnologías y requerimientos originales dado que fue un requerimiento propio del presente Trabajo Final de Grado. El sistema fue desarrollado con tecnología web, utilizando los últimos estándares de la industria para evitar dependencias que puedan comprometer el uso, mantenimiento o modificaciones en el futuro. Por esta razón a nivel de usuarios el único requerimiento que existe es el uso de un navegador web en versiones iguales o superiores a Internet Explorer 11, Firefox 36 o Chrome 41. Los requerimientos de hardware y sistema operativo van a depender del navegador que se utilice para acceder al sistema.

Además, el sistema tiene diseño web responsive, lo que significa que se adaptará al tamaño de pantalla de cualquier dispositivo que se utilice, es decir, computadoras de escritorio, tablets y celulares inteligentes.

Selección e instalación de la Base de Datos

Tanto MASI como Acceir utilizan el mismo sistema de base de datos: MySql. El proyecto actual no necesita de una base de datos diferente a la utilizada por MASI y Acceir, de hecho, solo se agregaron procedimientos almacenados, funciones y algunas tablas a las base de datos mencionadas anteriormente.

Los procedimientos almacenados creados fueron diseñados de manera similar a los ya creados por el sistema Acceir para detectar cambios en los componentes. Lo que se buscaba era no agregar complejidad a la estructura del sistema total al mantener la misma línea de diseño y desarrollo de procedimientos. De esta manera, los procedimientos nuevos generados en este proyecto se agregaron al procedimiento de Acceir que recorre los componentes para detectar cambios y generar alertas.

Las bases de datos de OpenAudit (MASI) y Acceir se encuentran en el mismo servidor y ambas son visibles entre sí, es decir, tienen permisos de ejecución de procedimientos almacenados, funciones y modificación de datos en las tablas de la otra base de datos.

Los requerimientos mínimos para instalar Mysql son los siguientes:

- **Memoria RAM:** 512 MB
- **Memoria Virtual:** 1024 MB
- **Espacio en disco duro:** 1 GB
- **Sistema Operativo:** Windows Server, Windows 7 o Linux
- **Arquitectura:** Compatible con arquitecturas de 32 y 64 bits

En el servidor MySql se debe modificar los siguientes componentes de la base de datos “**acceir**”:

- Tablas
  - deteccion_cambios_componentes_setup

Se deben agregar a la base de datos “**openaudit**” (MASI) los siguientes elementos:

- Procedimientos almacenados y funciones
  - acceir_detectar_cambios_build
  - acceir_detectar_cambios_software_prohibido
  - acceir_detectar_cambios_software_requeridoTablas
  - generar_entrada_build_requerido
  - generar_entrada_software_necesario
  - generar_entrada_software_prohibido
- Tablas
  - Build_requerido
  - Software_necesario
  - Software_prohibido
  - Tb_auditorias_requeridas

- Tb_build_requerido
- Tb_software_necesario
- Tb_software_prohibido
- Tb_software_sensible
- Tb_so_habilitados
- Tb_tipo_software

Se deben modificar en la base de datos "**openaudit**" (MASI) los siguientes elementos:

- Procedimientos almacenados y funciones
  - acceir_detectar_cambios
  - acceir_generar_alerta
  - acceir_get_cambio_descripcion
  - acceir_procesar_cambio
  - acceir_detectar_cambios_software

Los scripts para la modificación de las bases de datos "openaudit" y "acceir" forman parte de un anexo que se entrega junto con este documento.

Instalación de aplicaciones necesarias

El proyecto actual no necesita la instalación de aplicaciones ni herramientas adicionales de las ya instaladas para el correcto funcionamiento de OpenAudit (MASI) y Acceir, por lo que si el servidor ya está en funcionamiento, las mejoras de este proyecto funcionarán sin instalaciones adicionales.

Capacitación

La capacitación es una de las etapas más importantes para la puesta en marcha del proyecto ya que sin esta etapa, el proyecto no se utilizaría y, por lo tanto, sería un fracaso.

En el caso del presente Trabajo Final de Grado, la capacitación no incluye a los usuarios de los equipos pero sí incluye a los usuarios que cumplirán el rol de auditores y jefes auditores.

Capacitación de perfil "Auditor"

El perfil Auditor tiene algunas modificaciones en cuanto a los tipos de alertas que podrán manejar. Los temas a tratar serían los siguientes:

- Visualización de Listas de:
  - Tipo de Software
  - Software Prohibido
  - Software Requerido
  - Software Sensible
- Visualización de Alertas Habilitadas
- Visualización de Build/Kernel Mínimo
- Visualización de Periodicidad Mínima de Auditorías
- Nuevas alertas no previstas
- Sugerencias según tipo de alertas

Capacitación de perfil "Jefe Auditor"

Este es el perfil más importante en cuanto a las modificaciones del sistema debido a que ahora el Jefe Auditor será capaz de personalizar el sistema de auditoría. Los temas de la capacitación tienen que ser los mismos que los del perfil auditor y además sumar los siguientes ítems:

- Definición de Listas de:
  - Tipo de Software
  - Software Prohibido
  - Software Requerido
  - Software Sensible
- Configuración de Alertas Habilitadas
- Definición de Build/Kernel Mínimo
- Definición de Periodicidad Mínima de Auditorías

Factibilidad

El proyecto es factible. Se dispuso del presupuesto, condiciones técnicas, económicas y operativas para el desarrollo del mismo.

Factibilidad Técnica

La existencia de diferentes tecnologías adaptables, permitió brindarle a este proyecto una alta viabilidad. Las tecnologías y herramientas de desarrollo que se utilizaron son PHP, tecnología WEB (html, css, javascript y otras relacionadas) y MySQL.

Recursos tecnológicos para el desarrollo del proyecto:

- Requerimientos mínimos de Hardware:
  - 1 PC
  - CPU Intel Core i7
  - 8GB RAM
  - Disco Rígido de 1TB
- Requerimientos Mínimos de Software para el servidor:
  - GNU/Linux.
  - Servidor de base de datos MySQL.
  - Servidor Web Apache.
- Requerimientos Mínimos de Software para el desarrollo:
  - PHP.
  - Servidor de base de datos MySQL.
  - Servidor Web Apache.

Factibilidad Operativa

El producto de la tesis se probó e implementó en una maqueta de prueba, en ese sitio se hicieron todas las modificaciones necesarias hasta lograr una versión estable. Luego se subieron las modificaciones al servidor para poder ver su uso en la red auditada real en el Instituto Universitario Aeronáutico (IUA), en la provincia de Córdoba. Los resultados fueron los esperados y no se presentaron inconvenientes.

Factibilidad Económica

Las horas de desarrollo y el hardware necesario para llevar a cabo este proyecto fueron auto financiadas por la autora de esta tesis. El hardware para

el servidor será proporcionado por la organización que vaya a implementar la solución existiendo la posibilidad de utilizar un servidor virtual.

A continuación se detalla en una tabla el análisis de costos donde se detallan materiales, personal y costos:

Análisis de Costos	
Materiales	**Precio**
Servidor	$6100
Manuales y Documentación	Sin Costo
Costo Total	***$6100***
Personal	**Horas**
Nabila Gudiño Ochoa	610
Horas de Trabajo Totales	***610***

Conclusiones

En este capítulo final vamos a presentar una síntesis de la tesis y la conclusión a la que se ha llegado.

Problemas Afrontados

Los problemas afrontados se presentaron en dos momentos clave del desarrollo de la solución:

- Generación de nuevas alertas
- Procesamiento de archivos de log de Switchs
- Cambio en el sistema de gestión de la base de datos.

El primer problema se presentó al momento de querer generar nuevos tipos de alertas se presentó el problema de que, para que el sistema Acceir detecte cambios, se debía imitar el comportamiento natural de la herramienta OpenAudit para elementos que en realidad no son auditados de manera directa. Por ejemplo, para detectar Software Prohibido, en realidad lo que se hace es auditar todo el software de cada equipo y luego ejecutar un procedimiento almacenado dentro de la base de datos que determina si hay algún Software Prohibido instalado, si lo hace, inserta un valor en una tabla (homólogo a lo que haría OpenAudit cuando detecta un software nuevo, pero en una tabla diferente) y de esa manera, Acceir puede detectar que hubo un cambio y ejecutar su lógica para generar una alerta. Como se puede apreciar, es un proceso largo pero gracias a hacerlo de esta manera, no se necesitó hacer cambios sustanciales en el sistema Acceir, solo agregar una tabla en la base de datos de OpenAudit por cada nueva alerta.

El siguiente problema se presentó a la hora de querer procesar los archivos de log. Se obtuvo el archivo de log de los modelos de Switch que se encontraban en la Institución, el HP2920/48 y el Micronet SP1684b/48. A simple vista lucían similares pero, al no existir una estandarización sobre qué debe decir un log de un switch, los dos presentan información similar pero presentada de maneras muy diferentes. Por ejemplo, el Switch HP indica si algún dispositivo se conectó a un puerto mediante el tag PORTS, en cambio el Switch Micronet muestra esos eventos bajo el tag INFO; el problema es que este último switch tiene otros eventos que también utilizan este mismo tag, como por ejemplo, cuando informa desde qué IP se logueó el usuario admin del switch, cuándo se inició el sistema, por nombrar algunos. La forma de diferenciar los diferentes tipos de eventos del tag INFO es bajo el uso de sub-tags, en el caso de los ejemplos mencionados los sub-tags son PORT (eventos de puertos), WEB (login de admin) y SYSTEM (inicio del sistema).

Lamentablemente no se pudo lograr una solución estándar para cualquier Switch debido a la falta de estandarización en la forma en que estos muestran su información. Se crearon Scripts que analizan los logs de los Switchs HP y Micronet presentes en la Institución, pero si en algún momento se decide incorporar algún Switch diferente de los mencionados anteriormente, se deberá elaborar un Script que lea e interprete específicamente ese archivo de log y genere las alertas correspondientes.

Por último, al comenzar este Trabajo Final de Grado se creó una máquina virtual con una configuración similar a la configuración del servidor a fin de lograr una integración más ágil y sencilla de los nuevos módulos. El tercer problema se originó debido a que cuando se actualizó la versión de PHPMyAdmin en el servidor no se tuvo en cuenta que dicho software había cambiado su Sistema de Gestión de Base de Datos (cambió de uno MySQL puro a MariaDB). Si bien el nuevo Sistema de Gestión de Base de Datos está basado en MySQL, posee diferencias en cuanto a manejo de variables y algunas funciones. Luego de invertir más tiempo del planificado, se logró llegar a una versión compatible en donde los módulos funcionaban correctamente en el servidor.

Objetivos Logrados

Los objetivos planteados al comienzo de este Trabajo Final de Grado fueron claros desde su concepción. Se buscaba *automatizar las órdenes de trabajo para proteger los activos basando dichas órdenes en la política de seguridad de la información que define las acciones necesarias.* De lo cual se puede obtener que los objetivos generales del Trabajo Final de Tesis cumplidos fueron los siguientes:

- Lograr un mayor nivel de automatización en el sistema de auditoría en uso: se requería que el sistema fuera capaz de filtrar de alguna forma todas las posibles alertas por cambios y limitarlas solo a aquellas que realmente ponen en peligro la integridad del sistema.
- Generar órdenes de trabajo para los auditores, se requería que el sistema guíe a los auditores sobre qué acción tomar ante cierto tipo de alertas “conocidas” a fin de agilizar esas acciones.
- Mantener la seguridad de los activos de la Institución: se requería que el tratamiento de las alertas fuera ágil para evitar que la red permanezca en un estado no-seguro por demasiado tiempo.
- Seguir una Política de Seguridad que exponga acciones necesarias para volver el sistema a un estado seguro: se requería crear un documento de Política de Seguridad que fuera capaz de unir lo expuesto en las Circulares Informáticas en uso con lo sugerido por la IRAM - ISO/IEC 27002 a fin de exponer cómo se debe mantener los equipos y la red y sugerir acciones en caso de estar en una situación de peligro potencial.

Objetivos Específicos Iniciales	Forma en que se concretó durante el TFG
Estudio de sugerencias expuestas por la serie de normas ISO 27000 para solucionar esta problemática.	Se investigó el objetivo de cada norma IRAM - ISO/IEC 27000 y se llegó a la conclusión que la norma que iba a ser útil para el objetivo de este proyecto era la norma IRAM - ISO/IEC 27002 ya que presenta una serie de sugerencias sobre cómo tratar los temas principales de seguridad.
Definición de una Política de	Se estudiaron las Circulares Informáticas del

Seguridad de la información basada en la serie de circulares CI 1997 a CI 2015.	Instituto Universitario Aeronáutico. Luego, teniendo en cuenta además los puntos principales de la IRAM - ISO/IEC 27002, se diseñó y definió una Política de Seguridad para la Información Informatizada.
Análisis de las tablas necesarias para este proyecto de la herramienta OpenAudiT para auditoría remota de hardware y software.	Se analizaron los datos relevados por los Proyectos MASI (herramienta OpenAudit) y Acceir. Se estudió especialmente cómo releva los datos OpenAudit para que luego Acceir los tome en cuenta para generar alertas por cambios. De esta manera, se podrían generar nuevas alertas sin hacer cambios sustanciales en Acceir.
Análisis de las tablas necesarias para este proyecto de la herramienta ACCEIR de control de cambios de hardware y software instalado.	
Desarrollo de un módulo para procesamiento de información obtenida del Proyecto MASI, OpenAudit, Acceir y syslog.	Los datos obtenidos de OpenAudit, se procesaron a fin de lograr información más relevante que sería la base de las nuevas alertas diseñadas y desarrolladas en este Trabajo Final de Grado: Software Prohibido, Requerido y Sensible, Build/Kernel Mínimo Necesario y Auditorías Periódicas Requeridas. Además se desarrollaron Scripts PHP para leer los logs de los Switch HP y Micronet presentes en la Institución. Todos estos generan alertas en el Sistema Acceir en caso de situaciones peligrosas o de incumplimiento.
Definición de órdenes de trabajo del sistema las cuales se dividirán en: acciones automáticas realizadas por el propio sistema de forma remota y acciones asignadas a auditores humanos.	
Desarrollo de un módulo para la realización de las órdenes de trabajo mencionadas en el punto anterior.	Las órdenes de trabajo se ven reflejadas en el Incidente que se asigna a un auditor. Ahí el auditor no solo recibe información sobre el problema de un equipo de la red, sino que, con las modificaciones realizadas en este Trabajo Final, el auditor recibirá sugerencias respecto a cada tipo de alerta particular según lo expuesto como plan de acción en la Política de Seguridad desarrollada.

Conclusión Final

A lo largo de este proyecto se estudió la normativa IRAM - ISO/IEC 27002. Se comprendió sus conceptos básicos y necesarios de manera indispensable si se desea lograr sentar las bases de un sistema de auditoría

informática. Luego se estudiaron las Circulares Informáticas del Instituto Universitario Aeronáutico. Con ambos estudios, se elaboró el documento de Políticas de Seguridad Informática.

Se buscaron proyectos previos en el Instituto Universitario Aeronáutico sobre la temática de Auditoría Informática. Finalmente se encontraron los proyectos MASI (OpenAudit) y Acceir y se comenzó a listar, junto al equipo de auditores, los requerimientos para la modificación del sistema.

Finalmente, uniendo la nueva Política de Seguridad y los conocimientos de los Proyectos MASI y Acceir, se desarrollaron varios módulos para el sistema actual tendientes a solucionar, por un lado, la falta de capacidad del sistema para ser personalizado por parte del Jefe Auditor, y por otro, con esas personalizaciones, ayudar a encaminar al Jefe Auditor a configurar el sistema de modo tal que cumpla con todos los puntos requeridos por la Política de Seguridad.

Se tuvo que enfrentar tres problemas que marcaron el curso del proyecto. El primero se pudo sortear exitosamente debido a que se encontró la manera de generar información adicional de la obtenida por la herramienta OpenAudit. El segundo problema del proyecto se presentó al buscar una solución estándar para la interpretación de logs de los switchs, ya que si bien se llegó a una solución funcional para la Institución, fue imposible lograr una solución que pueda ser aplicable a cualquier switch disponible en el mercado (solución estándar). El tercero se pudo solventar con la inversión de tiempo adicional al planificado originalmente debido a que demandó investigación y pruebas adicionales para lograr compatibilidad de los módulos programados en la versión antigua de PHPMyAdmin (con un SGBD basado en MySQL puro) y la versión del servidor (con MariaDB como SGBD).

Con lo mencionado anteriormente, se da por cumplido el objetivo general planteado al inicio de este proyecto.

Referencias Externas

- Roger S. Pressman. **Ingeniería del Software; un enfoque práctico**. Quinta Edición. Madrid: McGraw-Hill 2002.
- María Elena Ciolli, Claudio Porchietto, Roberto Rossi, Juan Sapolski. **Monitoreo remoto de sistemas y redes para la auditoría informática**.
    - http://sedici.unlp.edu.ar/bitstream/handle/10915/31337/Documento_completo.pdf?sequence=1
- Auditoría Informática
    - https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
    - http://www.monografias.com/trabajos14/auditoria/auditoria.shtml
    - https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
    - http://es.slideshare.net/luismarlmg/auditoria-informatica-12602907
- ISO 27000
    - http://www.iso27001standard.com/es/que-es-iso-27001/
    - https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf
    - https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf
- Open Audit
    - http://www.open-audit.org/
    - https://community.opmantek.com/display/OA/Home
- Php
    - http://php.net/
    - http://www.desarrolloweb.com/articulos/producir-json-desde-php.html
- Slim Framework
    - http://www.slimframework.com/
    - http://docs.slimframework.com/
    - http://www.elserver.com/slim-mini-framework-rest-para-php/
    - http://www.ibm.com/developerworks/xml/library/x-slim-rest/index.html?ca=drs-
- ADOdb Database Abstraction Library for PHP
    - http://adodb.sourceforge.net/
- Bootstrap
    - http://getbootstrap.com/
- Knockout JS
    - http://knockoutjs.com/
    - http://learn.knockoutjs.com/
    - http://sebys.com.ar/2013/08/05/introduccion-a-knockout/
- MySql
    - http://dev.mysql.com/doc/

Anexos

Anexo A - Políticas de Seguridad

Políticas de Seguridad – Auditoría Informática

1 - Introducción

La información, ya sea en datos transportados por la red o almacenados en los equipos de la Institución, tienen valor para la comunidad universitaria. Por esta razón debe ser debidamente protegida para poder garantizar la continuidad de los sistemas de información, minimizando riesgos de daño o pérdida de la misma para, de esta forma, mejorar la gestión de la Universidad.

Para que estos principios de la Política de Seguridad de la Información sean efectivos, resulta necesaria la implementación de una Política de Seguridad de la Información Informatizada que forme parte de la cultura organizacional de la Universidad con el fin de obtener el compromiso de todas las personas involucradas de una u otra manera a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

Como consecuencia de lo expuesto, el Instituto Universitario Aeronáutico se ha abocado a la tarea de implementar sus propias políticas de seguridad de la información, basándose en las características establecidas por las Circulares Informativas de la Fuerza Aérea Argentina y las sugerencias expuestas por la serie de normativas ISO 27000.

2 - Términos y definiciones

- **Software Sensible:** son aquellos que deben ser instalados, actualizados y quitados necesariamente por un auditor.
- **Hardware Sensible:** son aquellos que deben ser instalados, actualizados y quitados necesariamente por un auditor.
- **Software Requerido:** son aquellos que deben estar instalado en el equipo para no infringir la Política de Seguridad y poder garantizar su permanencia en la red interna. Por ejemplo, un antivirus, un firewall.
- **Software Prohibido:** son aquellos que no pueden ser instalados ni por los usuarios ni por los auditores. En caso de ser necesaria la instalación de algún software presente en esta lista, se debe realizar un pedido por escrito según CI 01/15 inc 24.
- **Cuarentena:** se refiere a quitar a un dispositivo de la red de manera virtual. Implica colocarlo en la VLAN de cuarentena. Cuando el sistema ingresa a un dispositivo al estado de cuarentena debe informar a un auditor.
- **Informar al auditor:** es una acción automática del sistema. Se manda un reporte a un auditor detallando los siguientes datos:
    - qué equipo generó la alerta,
    - quién es su propietario,
    - a qué departamento está asignado,
    - qué alerta detonó el equipo,
    - cuál fue la razón por la que se detonó la alerta.

Puede suceder que el sistema no posea alguno de los datos anteriores, como por ejemplo, un nuevo equipo conectado en la red que nunca fue auditado y, por ende, no tiene datos sobre su propietario y departamento.

- **Usuario:** cualquier persona física de la Institución contratada por la Fuerza Aérea Argentina que haya sido autorizada para hacer uso de los recursos informáticos.
- **Recursos Informáticos:** también llamados Activos Institucionales, son todos aquellos elementos de tecnología de la información disponibles para el Usuario que son propiedad de la Fuerza Aérea Argentina o que están licenciados a su nombre.
- **Proxy Anónimo:** es un servidor que sirve de intermediario en las peticiones de recursos que realiza un cliente a otro servidor. Un proxy de estas características permite mantener el anonimato de las conexiones.
- **Hacking:** técnicas y procedimientos utilizados por un individuo para lograr un objetivo determinado. Normalmente son procedimientos ilegales, cuyo objetivo es ingresar a lugares prohibidos y tener acceso a información restringida.
- **Phreaking:** disciplina estrechamente vinculada al hacking convencional. Es un tipo específico de hacking informático que está orientado a los medios telefónicos.
- **Cracking:** acción de modificar el código fuente a un programa, llevado a cabo por un cracker, que es quien viola la seguridad de una sistema informático de forma similar a como lo haría un hacker. La diferencia con este último es que el cracker realiza la intrusión en busca de un beneficio personal.
- **Malware:** es un software dañino para la computadora diseñado para insertar virus, gusanos, troyanos o spyware, intentando conseguir algún objetivo, por ejemplo recoger información sobre el usuario o sobre la computadora en sí.
- **DHCP:** Protocolo de Configuración Dinámica de Host. Este protocolo permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.
- **RIP:** Protocolo de Información de Enrutamiento. Es el protocolo de puerta de enlace interna utilizado por los routers para intercambiar información acerca de redes IP a las que se encuentran conectados.
- **FTP:** Protocolo de Transferencia de Archivos entre sistemas conectados a una red TCP (Protocolo de Control de Transmisión).
- **SQL:** Lenguaje de Consulta Estructurado. Es un lenguaje de acceso a bases de datos relacionales.

3 - Objetivos de la Política de Seguridad de la Información Informatizada

Proteger los recursos de información de la Universidad y la tecnología utilizada para su procesamiento frente a amenazas tanto internas como externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política.

Mantener la Política de Seguridad de la Universidad actualizada a efectos de asegurar su vigencia y nivel de eficacia.

4 - Sanciones Previstas por Incumplimiento

El incumplimiento de las disposiciones establecidas por las Políticas de Seguridad de la Información Informatizada tendrá como resultado la aplicación de diversas sanciones conforme a la magnitud del daño y la característica del aspecto no cumplido.

5 - Clasificación y Control de Activos

Inventario de Activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información tal como lo indica la Circular Informática 04/98 en el Artículo 23 inc 2.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

Seguridad del Personal

Seguridad en la Asignación de Recursos

Como parte de asegurar la confidencialidad de los datos que maneja cada usuario de la red, se dispone que cada persona tendrá un usuario propio dentro de la red, al cual podrá acceder por medio de su contraseña personal.

Asimismo, es deber del personal de Auditoría registrar a nombre del usuario los activos que le sean asignados.

Cuando un usuario, por cualquier causa, deje de utilizar el equipo que se le asignó, deberá comunicar esta situación al equipo de Auditoría para que quiten su nombre del registro del equipo; de esta manera, el usuario queda desligado del equipo.

6 - Respuesta a Incidentes y Anomalías en los equipos

Comunicación de Anomalías en el Hardware y/o Software

Es deber del usuario comunicar al personal de Auditoría sobre cualquier anomalía o desperfecto ya sea en el Hardware o en el Software de su equipo.

Si el usuario necesita instalar algún tipo de Hardware o Software es preferible que consulte primero con el personal de Auditoría para no violar alguna Política de Seguridad, dado que algunas modificaciones pueden ser causal de que dicho equipo quede en cuarentena por violar alguna Política de Seguridad aquí expuesta.

Respuesta a incidentes imprevistos

En caso de ocurrir alguna violación a la presente Política de Seguridad, cualquiera sea su gravedad, la respuesta automática será solicitar al equipo de auditores poner el equipo infractor en una red de cuarentena. Posterior a esta acción se analizará el incidente ocurrido y se propondrán acciones a seguir.

7 - Seguridad de la Red y los Equipos

Protección contra Software Malicioso

A fin de cumplir lo expuesto en la Circular Informática 01/2015 art. 28, es decir, evitar un ataque por Software Malicioso o Malware, se creó en la Lista de Software Requerido un apartado de Antivirus y Firewall. Cada equipo conectado a la red interna deberá obligatoriamente poseer algún Antivirus y algún Firewall de los mencionados en dicha Lista. El equipo deberá permanecer en la red de cuarentena hasta tener lo requerido en dicha lista.

El equipo de Auditoría es el único con los permisos necesarios para agregar elementos en la Lista de Software requerido.

Según lo expuesto en la Circular Informática 01/2015 art. 20 cualquier acto con intención de vulnerar los sistemas de protección del equipo o la red está considerado una falta grave.

Restricciones de Instalación y Uso de Software Específico

La lista de Software Prohibido enumera todos los elementos software que obligatoriamente no deben estar presentes en un equipo conectado a la red interna. Las secciones de dicha lista son las listadas en las siguientes secciones según lo expuesto en la Circular Informática 01/2015 art. 23 inc. 1 y 2, art. 25 inc. 1 - 5, art. 27 y art. 28.

El equipo de Auditoría es el único con los permisos necesarios para agregar elementos en la Lista de Software Prohibido.

En caso de ser necesaria la instalación y uso de algún software de los citados a continuación, se deberá solicitar la autorización pertinente y pedir al personal de Auditoría la instalación de dicho software según lo expuesto en la Circular Informática 01/2015 art. 26.

Software de Entretenimiento

Estas restricciones definidas en la Circular Informática 01/2015 art. 23 inc. 1 están destinadas a mantener constante el ancho de banda de la red a todos sus usuarios y evitar la descarga de archivos que puedan estar corruptos. Se prohíbe la instalación y el uso de programas para la descarga y/o distribución de música y videos, que permitan el acceso a redes P2P y/o programas de mensajería instantánea, cibercharla, videoconferencia o similar.

Software de Redes

Estas restricciones definidas en la Circular Informática 01/2015 art. 23 inc. 2 están destinadas a proteger el tráfico de paquetes transmitidos en la red evitando que los mismos sean vistos o violados por terceros. Se prohíbe la instalación y el uso de programas para captura de paquetes, enmascarar IP, utilizar proxys anónimos, programas para la denegación de servicios (DoS), inundación de paquetes en la red, comportamiento abusivo de la red (repetición desmesurada de paquetes en un corto periodo de tiempo o flooders), programas para escaneo de puertos y/o vulnerabilidades, programas de función oculta (troyanos), descifradores de contraseñas (crackers), programas para envío masivo de mails (mail bomber), programas para monitoreo de computadoras y/o para grabar movimientos de teclado, pantalla u otros

dispositivos (keyloggers), programas para forzar deficiencias (bugs) o vulnerabilidades de otro programa (xploits), cualquier software para hacking, phreaking, cracking o actividades similares, programas para la administración remota de equipamiento informático institucional, programas para acceder a servicios de la nube para subir archivos de la FAA, o cualquier actividad similar o sucedánea a las previamente descriptas.

Protocolos e Interfaces

Estas restricciones definidas en la Circular Informática 01/2015 art. 25 inc. 1 - 5 están destinadas a proteger el tráfico de paquetes transmitidos en la red. Los protocolos e interfaces restringidas son DHCP, RIP, SQL Resolver, FTP y cualquier otro protocolo o interfaz similar o sucedánea a las previamente descriptas.

Protección de la Integridad de los Equipos

Para evitar que los equipos sean alterados de forma no autorizada, modificando el valor de los activos de la Institución, se creó la Lista de Hardware Sensible y Software Sensible.

Los usuarios no tienen permitido cambiar ningún hardware y/o software presente en dichas listas. Si se efectúa un cambio no autorizado, se debe alertar al personal de Auditoría sobre el cambio efectuado de forma tal que dicho equipo sea puesto en la red de cuarentena hasta verificar su nuevo estado.

El equipo de Auditoría es el único con los permisos necesarios para agregar elementos en la Lista de Hardware Sensible y Software Sensible.

8 - Actualización del Sistema Operativo de los Equipos

Es responsabilidad del personal de Auditoría la actualización del Sistema Operativo de los Equipos de la red interna. Por consiguiente, el usuario no tiene el nivel de autorización para realizar actualizaciones del Sistema Operativo. En caso de necesitar una actualización, debe solicitarlo al personal de Auditoría.

Es responsabilidad del jefe de soporte definir la versión del sistema operativo más antiguo con los requerimientos mínimos para ejecutarse correctamente en un equipo que se permite conectar a la red.

De existir estaciones de trabajo auditadas que cumplan con dichos requerimientos del hardware, deben ser actualizados a la nueva versión de Sistema Operativo. Es responsabilidad de soporte realizar el resguardo de la información del equipo a actualizar y efectuar la actualización del sistema operativo de forma manual. En caso que dicho equipo no cumpla con los requerimientos de hardware para la nueva versión de Sistema Operativo, se generará la orden de compra y la orden de trabajo para que soporte actualice dicho equipo.

9 - Auditorías obligatorias

Es deseable realizar una auditoría cada vez que un equipo se autentica en la red. En conformidad con lo expuesto en la Circular Informática 01/2015 art. 29 que expresa la necesidad de mantener una revisión constante de los equipos de la red a fin de detectar irregularidades, software ilegal y/o

vulnerabilidades que pueden perjudicar a la Fuerza Aérea Argentina y a la Institución, es necesario que estas auditorías se hagan al menos una vez cada tres meses, si esto no ocurre, es responsabilidad del Personal de Auditoría verificar si pueden haber ocurrido alguna de las siguientes situaciones: el usuario que tiene asignado ese equipo no lo ha encendido por tres meses o el equipo tiene un problema con el script automático de auditoría y no ha podido ejecutarlo. Se sugiere que algún auditor verifique el estado de ese equipo.

Si transcurren seis meses sin realizarse auditorías automáticas, se pide al personal de auditoría poner ese equipo en la red de cuarentena hasta regularizar y comprobar su estado.

Permanencia de los Equipos en la Red Interna

Los equipos deben ser monitoreados para comprobar que permanecen conectados a la red. Para esto, el personal de auditoría debe monitorear los archivos de log generado por los switch a donde se conectan los equipos.

Si un equipo auditado aparece no conectado a la red, se seguirá monitoreando su estado por 30 minutos esperando a que este aparezca. En caso de superar ese periodo y que el equipo siga desconectado se informará al personal de Auditoría acerca de este evento.

Si por el contrario, un equipo no auditado aparece conectado a la red, se informará al personal de Auditoría que un equipo nuevo se ha conectado a la red y no ha sido previamente auditado, por lo que debe ser colocado en la red de cuarentena hasta que regularice su situación.

10 - Responsabilidades ante Incidentes

Cualquier incidente que provoque algún equipo será responsabilidad del usuario al que se le fue asignado. Queda a discreción del usuario cuidar el activo que se le asignó para evitar sanciones.

11 - Anexos

Anexo 1: Lista de Software Prohibido

Son aquellos que no pueden ser instalados ni por los usuarios ni por los auditores. En caso de ser necesaria la instalación de algún software presente en esta lista, se debe realizar un pedido por escrito según CI 01/15 inc 24.

Analizadores de Paquetes, Denegadores de Servicios, Flooders, Crackers, Mail Bombers, Xploits

- Wireshark
- P2P
- Ares
- Kazaa
- Emule
- uTorrent
- Tribler
- Vuze

KeyLoggers

- Revealer KeyLogger

Chat

- Microsoft Lync
- Skype
- Facebook Messenger
- Line

Administración Remota de Equipos

- Team Viewer

Servicios de la Nube

- Drive
- Box

Anexo 2: Lista de Software Requerido

Es un grupo de listas que enumeran cada tipo de software que debe estar instalado en todos los equipos. Por ejemplo, se tendrá una lista de Antivirus, una lista de Firewall, etc.

Antivirus

- Avast
- AVG

Firewall

- Windows
- AVG
- Avast

Anexo 3: Lista de Software Sensible

Son aquellos que deben ser instalados, actualizados y quitados necesariamente por un auditor. El grupo de auditores debe definir esta lista.

Anexo 4: Lista de Hardware Sensible

Son aquellos que deben ser instalados, actualizados y quitados necesariamente por un auditor.

- Disco Duro
- Memoria
- Placa Base (madre)
- Placa de red
- Placa de video
- Procesador
- Dispositivo Óptico
- Placa de Sonido
- Dispositivo on board
- Disquetera
- Monitor
- Teclado
- Mouse