ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UN SISTEMA DE INICIO DE SESIÓN ÚNICO (SSO) EN UNA EMPRESA DE TELECOMUNICACIONES DEL ECUADOR"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

FERNANDO JAVIER YÁNEZ SANDOVAL

GUAYAQUIL – ECUADOR

AÑO – 2015

AGRADECIMIENTO

A Dios que con su amor infinito nos permite lograr todo lo que nos propongamos.

A mi Madre y Hermano por su apoyo y confianza en todas las etapas de mi vida.

A mi Padre que desde el lugar de donde me observa se siente feliz y tranquilo.

A mi esposa e hijos por su amor y compresión.

DEDICATORIA

A Dios por sus bendiciones y a mi familia por todo el apoyo brindado para poder culminar esta nueva etapa.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire C.

DIRECTOR DE LA MSIA

Ing. Lenin Freire C.

PROFESOR DELEGADO POR LA MSIA

Ing. Juan Carlos García

PROFESOR DELEGADO POR LA MSIA

RESUMEN

Con la implementación del sistema de Inicio de Sesión Único (SSO), se logra la optimización de la gestión y el correcto manejo de las contraseñas por parte de los usuarios, mejorando el proceso de autenticación a las aplicaciones definidas para su acceso en la Organización.

La Solución SSO brinda el beneficio de tener un único de punto de registro y autenticación en el sistema, esto quiere decir que los mecanismos de seguridad se encuentran consolidados en la misma solución.

Permitir al usuario que en el momento que lo desee pueda acceder a cada una de las aplicaciones o servicios, ya que una implementación correcta de SSO debe encargarse de almacenar estos accesos en una base de datos o directorio protegido.

El proceso de login debe estar configurado para que se realice de manera transparente para el usuario una vez que ya fue autenticado por el Sistema de Inicio de Sesión Único (SSO).

Con la implementación de este sistema se busca disminuir la cantidad de requerimientos por reseteos/desbloqueos u olvidos de contraseñas [2], ya que el usuario tendrá almacenada las credenciales en la billetera del agente y luego de la primera autenticación no tendrá necesidad de ingresar la información, ya que el sistema inyecta automáticamente las credenciales almacenadas en la billetera, por lo tanto disminuirían los errores operativos por intentos fallidos y el usuario tendrá sus accesos definidos disponibles.

Con este sistema se busca disminuir para los usuarios finales el tiempo de No disponibilidad y el tiempo de espera de atención de los requerimientos asignados al área de accesos, ya que con esta aplicación el usuario solo tiene que ingresar la primera vez la contraseña [3] a partir de eso se quedan almacenadas cifradas en su billetera que se encuentra en una base de datos centralizada.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CRM	Software para la administración de la relación con los clientes.
ERP	Sistema de planificación de recursos empresariales
IDM	Administrador de identidades
IT	Tecnología de la Información
RRHH	Recursos Humanos
SSO	Single Sign On

.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Se detalla el proceso que incluye los objetivos, la justificación y los recursos necesarios para la implementación de un Sistema de Inicio de Sesión Único (SSO).

El Sistema SSO es uno de los principales métodos de autenticación, que nos ayuda a mejorar el control de la seguridad y a simplificar en lo que respecta al control de accesos a los sistemas de la Organización.

A través de esta tecnología, las organizaciones pueden brindar un acceso seguro a los recursos empresariales y personales, por lo tanto los usuarios no tendrán que mantener y recordar un amplio número de credenciales para su autenticación en cada uno de los sistemas autorizados.

Es importante señalar, que lo dicho, es altamente recomendado por conceptos de seguridad de la información, tal cual cita la Norma ISO 27002 [1], en el tema de control de accesos.

Dentro de una organización donde se tienen varias aplicaciones, por ejemplo se tienen las aplicaciones Web o aplicación clientes/servidor, en donde el principal problema es tener que recordar varias contraseñas por cada aplicación asignada a su perfil dentro de la empresa, lo ideal sería para los usuarios con una sola autenticación acceder a un sistema de seguridad que almacene las credenciales de los sistemas definidos para su correcto desempeño en la Organización.

Con la implementación de esta solución se busca fortalecer la seguridad de la infraestructura de servicios, mejorar las labores de administración con respecto a la gestión de atención a requerimientos y disminuir el tiempo de espera del usuario por la No disponibilidad de los accesos, mejorando la productividad en la Organización.

El desarrollo y la actualización de aplicaciones corporativas con altos niveles de Seguridad Informática, establece un reto constante para fortalecer los fundamentos de seguridad informática principales como son:

- ✓ La confidencialidad,
- ✓ La integridad
- ✓ La disponibilidad
- ✓ La autenticación
- ✓ La autorización
- ✓ La no repudiación
- ✓ La observancia

CAPÍTULO 1

GENERALIDADES

1.1 Objetivo General

Detallar el proceso de implementación de un sistema de Inicio de Sesión Único en una empresa de telecomunicaciones, con el objetivo principal de que los colaboradores a través de un sistema seguro de autenticación puedan acceder a las aplicaciones definidas en la Organización y que este sistema inyecte automáticamente las credenciales.

Contar con un sistema de Seguridad que almacene el usuario y contraseña en un directorio activo centralizado, que funcione como un repositorio de contraseñas, con esta implementación el usuario ya no tendrá la necesidad de ingresarlas, ya que la herramienta inyecta automáticamente la información, con esta implementación se logra mitigar los errores por contraseñas mal ingresadas. Como adicional también se debe considerar que el sistema debe proveer una interfaz amigable para el usuario final.

Disminuir los requerimientos por cambios de contraseñas en las aplicaciones ya que el usuario tendrá un sistema seguro para poder guardas sus contraseñas, tenerlas disponibles para cuando las requiera y como es un servicio centralizado tendrá accesos desde cualquier punto de la red, con esto se solventaría el problema que se tiene con los usuarios que tienen que moverse de una oficina a otra.

1.2 Descripción del Problema

La gestión de la identidad de los usuarios es uno de los mayores retos para la Seguridad Informática, ya que el mercado informático tiene como prioridad mejorar los niveles de Seguridad en su arquitectura para sus usuarios (clientes internos o externos) trabajando incansablemente para desarrollar iniciativas de control y de Seguridad, que permitan ofrecer servicios de valor agregado con altos niveles de Seguridad y confiabilidad.

El tener diversas aplicaciones y que los colaboradores deban memorizar varios usuarios y/o contraseñas, y tener una política de contraseñas bastante compleja, hacen que en los usuarios con todos estos antecedentes exista la posibilidad de que olviden sus credenciales y esto genera la No disponibilidad de los accesos.

Aumento de la atención requerimientos para el área de accesos por restablecimientos de contraseñas, provocando la reducción de la productividad para la Empresa al no tener los accesos disponibles y esto

amerita que se tenga personal disponible 24x7 solo para la atención de requerimientos de reseteos/desbloqueos por olvidos de contraseñas.

La administración de los usuarios y las contraseñas y el problema que tienen los usuarios al momento que tienen que acceder a los sistemas de la Organización, convirtiéndose en: bloqueos, olvidos de usuarios, post its y lo más importante percibir de los usuarios la disconformidad y angustia por la complejidad de los accesos en la utilización de los sistemas [4].

1.3 Solución Propuesta

Una solución tecnológica que ayude a gestionar el manejo seguro y eficiente de las contraseñas de los colaboradores. Mejorar el tiempo de acceso a la información por parte del colaborador, eliminando o disminuyendo en gran medida el tener que recordar un sin número de contraseñas y el tiempo de espera hasta que sea atendido su requerimiento.

Al tener implementado este Sistema en un entorno empresarial permite que el área de accesos o también conocido como “mesa de ayuda” no se desgasten en la atención de requerimientos de restablecimientos de contraseñas, y a su vez estos recursos puedan ser utilizados para monitorear y controlar otras áreas de la empresa.

De acuerdo a lo revisado actualmente hay muchas organizaciones que han implementando políticas de contraseñas cada vez más rigurosas para el acceso a las aplicaciones por parte de los colaboradores y la complejidad va en aumento, con la implementación de este sistema se

mejora la Seguridad, la productividad y la conformidad normativa con la implementación de un sistema de inicio de sesión único.

La solución debe proveer el acceso seguro y transparente a todas las aplicaciones de la organización compatibles con la solución.

La solución debe poseer una interfaz de usuario intuitiva que permita la fácil utilización por los usuarios y brindando los siguientes beneficios adicionales para la organización:

- ✓ Reducción de costos de Administración de la Seguridad y de la operativa asociada con la administración de accesos.
- ✓ Aumento de los niveles de seguridad personal y empresarial
- ✓ Ofrece administración centralizada
- ✓ Permitir el acceso desde cualquier PC previa autenticación.
- ✓ Permitir el bloqueo de la estación de trabajo por inactividad.
- ✓ Debe brindar la opción de gestionar la billetera
    - Exportar
    - Eliminar

- Editar

✓ Al inyectar el usuario y contraseña debe brindar la opción de configurar la entrada de la contraseña:

- Iniciar automáticamente
- Nunca

✓ Billetera cifrada con algoritmo de 256 bits.

✓ Reportes de equipos activos/inactivos

✓ Instalación masiva del agente

✓ Que se compatible con los exploradores autorizados en la Organización.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 Definición de la información necesaria para la integración de la solución.

En esta fase de la implementación se definen cuáles son los procesos necesarios que se utilizan en la Organización con el fin de obtener los mejores resultados de acuerdo a las bondades que ofrece la solución con respecto a los servicios de gestión de accesos.

Para continuar con el proceso de implementación es necesario definir los siguientes Inventarios.

- ✓ Aplicaciones personales y empresariales.

- ✓ Maquinas en el dominio.
- ✓ Estadísticas de requerimientos.
- ✓ Personas.
- ✓ Políticas de contraseñas.

Con esta información definida se puede tomar la decisión de que activo se integra a la solución para su configuración y monitoreo.

A continuación se detallan ejemplos de inventarios con información básica concerniente para la definición de la información:

Tabla 1. Inventario de máquinas en el dominio

NOMBRE	USER NAME	SISTEMA OPERATIVO	DIRECCIÓN IP
PC_0001	Maquina_1	Microsoft Windows 7	192.168.1.1
PC_0002	Maquina_2	Microsoft Windows 7	192.168.1.2
PC_0003	Maquina_3	Microsoft Windows 7	192.168.1.3
PC_0004	Maquina_4	Microsoft Windows 7	192.168.1.4
PC_0005	Maquina_5	Microsoft Windows 7	192.168.1.5
PC_0006	Maquina_6	Microsoft Windows 7	192.168.1.6

Tabla 2. Inventario de Aplicaciones

SISTEMA	DESCRIPCIÓN DEL SISTEMA	TECNOLOGÍA APLICADA
CRM	Información de Clientes y Servicios contratados	Oracle Forms
Inventario	Disponibilidad de Productos	Java
ERP	Sistema Financiero	Oracle Forms
Facturación	Facturación de Productos	.Net
Nómina	Sistema de Recursos Humanos	.Net

Tabla 3. Política de contraseñas

SISTEMA	LONGITUD MÍNIMA	LONGITUD MÁXIMA	DÍGITOS MÍNIMOS	CARACTERES EN MAYÚSCULA MÍNIMOS	CARACTERES EN MÍNUSCULA MÍNIMOS	HITORIAL DE CONTRASEÑAS	CARÁCTERES ESPECIAL MÍNIMO
CRM	8	15	3	1	1	5	1
Inventario	8	15	3	1	1	3	1
ERP	8	15	3	1	1	3	1
Nómina	8	15	3	N/A	N/A	5	1
Facturación	8	15	3	1	1	5	1

2.2 Selección y evaluación de soluciones para el Sistema SSO.

Existen diferentes tipos de arquitecturas que permiten implementar un Sistema de Inicio de Sesión Único, la aplicación de una ellas depende de cuáles son las características que se están buscando y obviamente que sean compatibles con la solución disponible.

Una arquitectura SSO está compuesta por tres componentes básicos:

- ✓ **Interface:** Es el modo en que el SSO interactúa con una determina aplicación, generalmente se encuentra instalada en el cliente y se la conoce también como el Agente SSO.

- ✓ **Administración:** Es el mecanismo que permite administrar, configurar, monitorear, gestionar y mantener la solución SSO.

- ✓ **Credenciales:** Acceso por el agente de forma cifrada.

Para la selección de soluciones SSO se pueden consideran diferentes aspectos como:

- ✓ Seleccionar las empresas que garanticen que cuentan con la experiencia en este tipo de soluciones y que cuentan con personal capacitado para poder implementarla.

- ✓ Las características principales y beneficios que brinda la solución, que inciden directamente en la decisión de la adquisición de la solución:

    - **Inteligencia**: Que tengan las herramientas necesarias que permitan el monitoreo de todos los eventos ocurridos, de forma confiable y fácil, permitiendo que se puedan realizar auditorías para la corrección de eventos.

    - **Administración**: Consiste en el manejo integral de la solución, permitiendo el control del flujo general de la solución de autenticación.

    - **Autenticación**: Se refiere a todo lo que tenga relación con el proceso de la autenticación.

La evaluación de las soluciones se realizó por medio del análisis de los siguientes aspectos [2] y funcionamientos de la solución:

- ✓ Herramientas Standard para la integración
- ✓ Administración y Gestión centralizada
- ✓ Reportes y Auditorias
- ✓ Seguridad Personal
- ✓ Seguridad Empresarial
- ✓ Billetera cifrada con algoritmo de 256 bits
- ✓ Despliegue centralizado
- ✓ Reportes de los agentes
- ✓ Permitir establecer perfiles de accesos
- ✓ Aplicaciones Personales y Empresariales
- ✓ Todo gira al nivel de la contraseña del dominio

2.3 Aplicabilidad en las Aplicaciones

De acuerdo a las aplicaciones que serán integradas a la herramienta SSO se detalla lo siguiente:

- ✓ **Aplicaciones Web:** Para el correcto funcionamiento de la herramienta deben soportar aplicaciones de terceros. Si el aplicativo no fue desarrollado con las mejores prácticas de programación, el SSO no podrá inyectar las credenciales, ya que para que se realice este proceso primero tiene que identificar ciertos valores o botones configurados en la aplicación (usuario/contraseña/ingresar), una vez identificado estos valores en la aplicación se procede con la creación y generación del perfil, también se deben analizar la aplicación de algún complemento en el explorador.

- ✓ **Aplicaciones Cliente/Servidor:** Para este tipo de aplicaciones no es factible que el SSO ingrese a la programación de la aplicación, por lo tanto el perfil debe ser creado y generado

(usuario/contraseña/ingresar) desde la misma herramienta del SSO.

Además, la herramienta debe proveer la funcionalidad de realizar un test de las aplicaciones que van a integrarse a la solución para poder visualizar si las pruebas fueron exitosas o en que proceso presentaron errores para su respectiva revisión y solución.

2.4 Integración del Sistema SSO

Siguiendo la metodología de proyectos se detallan las siguientes fases y entregables:

- ✓ **Inicio**: Definir los objetivos del negocio, las iniciativas a corto y mediano plazo y se establecen objetos claros y detallados para la solución.

- ✓ **Elaboración:** Evaluar cuidadosamente los requisitos del negocio y tecnológicos, define el alcance del despliegue y alinea con áreas funcionales específicas.

- ✓ **Construcción:** Implica la configuración e instalación de la solución SSO en un entorno de laboratorio aislado, desarrollando un plan de trabajo de validación y despliegue de la solución detallada y la realización de pruebas exhaustivas de integración.

- ✓ **Transición**: luego de que está construida y validada en el entorno de laboratorio se desplegará la solución final en el entorno de producción.

Adicionalmente, son importantes en esta fase los siguientes aspectos:

- ✓ Cronograma de instalación del agente en las PCs definidas en el dominio.
- ✓ Pruebas unitarias para las aplicaciones definidas en la integración (criticas y no criticas).
- ✓ Pruebas de aceptación de los usuarios finales y tener la disponibilidad del proveedor sobre cualquier ajuste que sea necesario para que la solución funcione correctamente.

A continuación, se adjunta la arquitectura básica del Sistema de Inicio de Sesión Único:

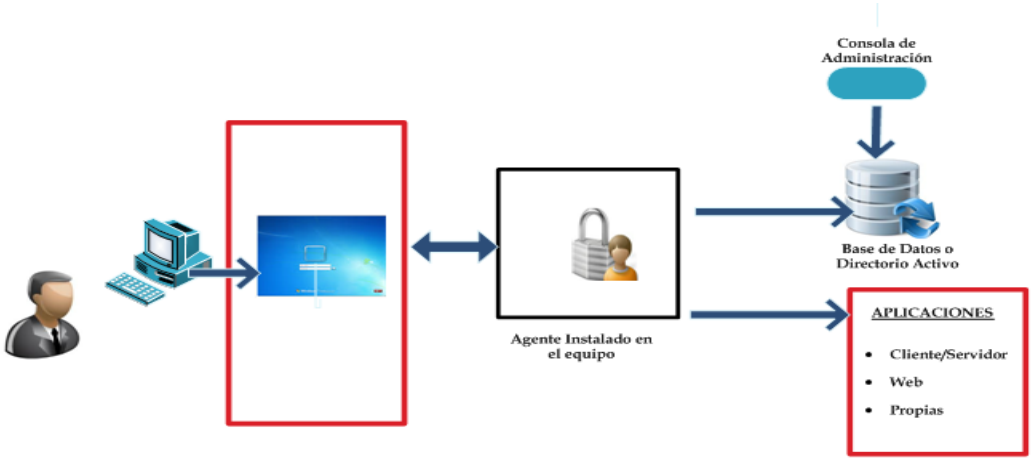

Figura 2.1 Arquitectura Básica del Sistema SSO

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 Tiempos de respuesta y satisfacción del usuario

Para los departamentos de accesos la gestión o administración de los usuarios y contraseñas donde cada uno de los usuarios tienen accesos definidos a un amplio número de aplicaciones, esto se transforma en un en grave problema ya que el usuario aparte de tener en consideración la política de contraseñas deben tener que recordar todas sus contraseñas para poder ingresar a los aplicativos.

Con la implementación de esta solución el usuario solo debe recordar la contraseña que autentica la billetera donde se encuentran sus accesos autorizados de forma cifrada, permitiendo que disminuya el impacto de no disponibilidad al no recordar sus credenciales y de insatisfacción por el usuario [5]:

- ✓ La resolución de requerimientos por problemas presentados con las contraseñas de los usuarios son administrados de una mejor manera.
- ✓ Disminución de los tiempos no productivos.
- ✓ Interfaz intuitiva y de fácil administración.
- ✓ Administración y monitoreo centralizado.
- ✓ Aceptación de la solución por parte de los usuarios de la Organización.
- ✓ Reducción de costos de administración de la Seguridad.
- ✓ Disminución de la operatividad asociada con la gestión de contraseñas.
- ✓ Incremento en los niveles de seguridad existentes.
- ✓ Mantener actualizado el Inventario de los usuarios y maquinas en el Dominio.

3.2 Evolutivo de atención de requerimientos

Culminado el proceso de estabilización y capacitación de la nueva herramienta al personal, se realizó el análisis de los requerimientos generados por reseteos/desbloqueos de las contraseñas tomando como fechas de análisis desde cuando no se contaba con la solución (Jul-14) hasta 6 meses después de la implementación de la solución (Jun-15) se logra apreciar que este tipo de requerimientos han disminuido en una **80**% a causa de que el usuario ya no tiene que ingresar el usuario y contraseña, sino que, el sistema inyecta automáticamente esa información.

Tabla 4. Evolutivo de atención de requerimientos

Mes	jul-14	ago-14	sep-14	oct-14	nov-14	dic-14	ene-15	feb-15	mar-15	abr-15	may-15	jun-15
Cantidad	1000	950	980	900	970	800	600	450	500	350	300	200

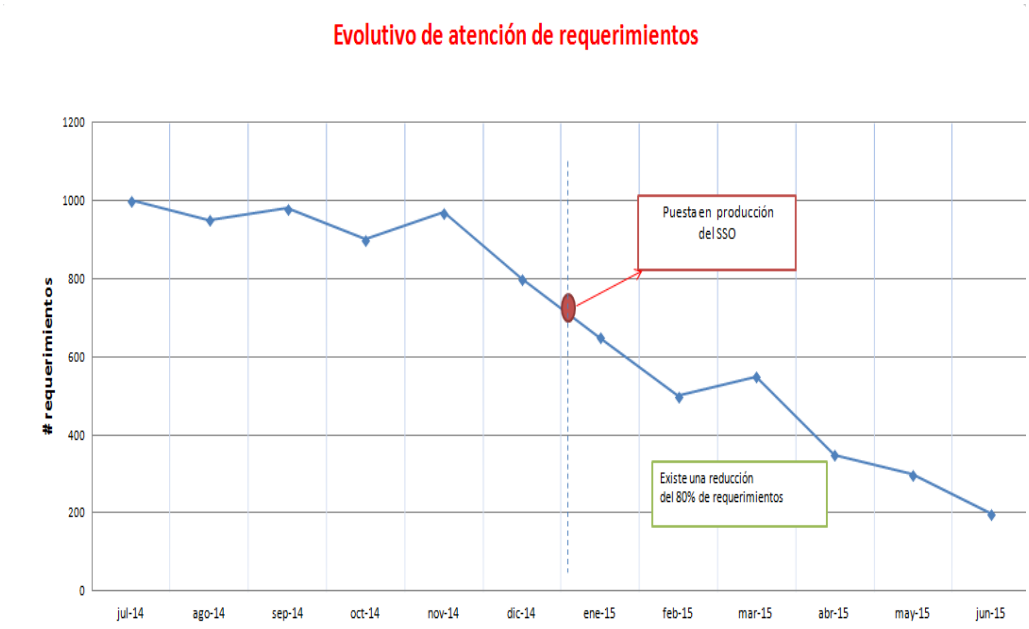

Figura 3.1 Evolutivo de atención de requerimientos

Esta operativa se vuelve más compleja cuando no se cuenta un Administrador de Accesos y el proceso se lo realiza manualmente.

Como se puede observar en la grafica sin esta solucion la atencion de los requerimientos se transformaba en una situacion critica, ya que aparte de tener que atender varios requerimientos se debe cumplir con los tiempos de respuesta estipulados por la Organización para estos tipos de requerimientos.

3.3 Estadística de atención de requerimientos por Sistema

En base a la revisión de los requerimientos asignados al departamento de accesos desde el mes de Jul-14 hasta el mes de Junio-15 se realizó la siguiente clasificación de requerimientos por sistemas críticos y no críticos.

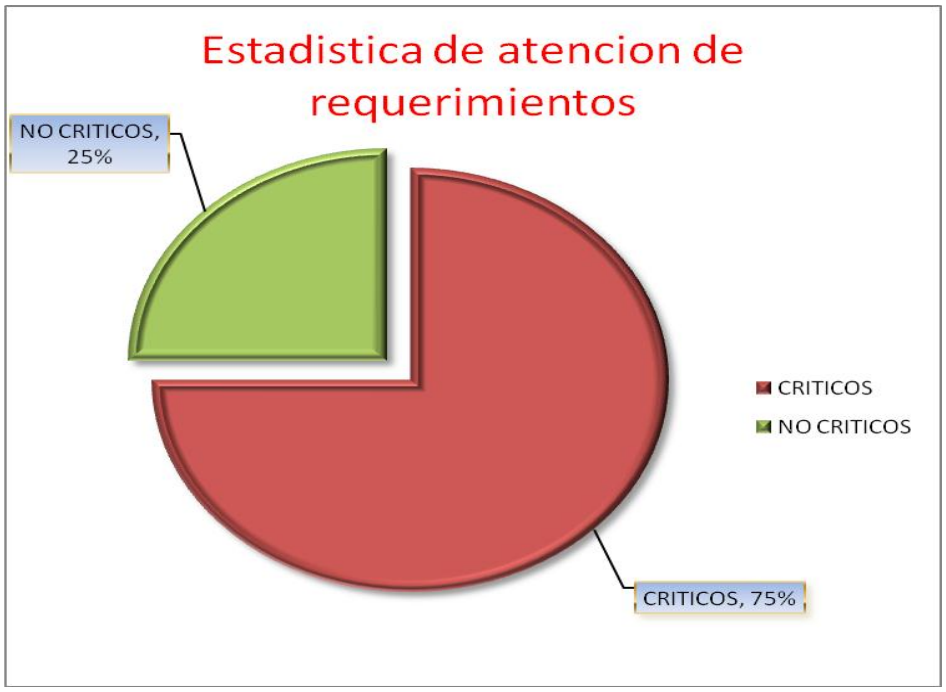

Figura 3.2 Estadística de atención de requerimientos por Sistema

Para los requerimientos de los sistemas No críticos el porcentaje del tiempo utilizado por el personal para la atención de estos requerimientos

es bastante considerable ya que estos sistemas no cuentan con un Administrador de Accesos y la operativa se la realiza manualmente.

Para la atención de los requerimientos de los sistemas críticos el porcentaje del tiempo utilizado por el personal es menor ya que estos sistemas si cuentan con un Administrador de Accesos y el proceso se encuentra automatizado.

Con la implementación de este sistema se puede confirmar a través de las graficas luego del tiempo de estabilización del mismo, que ha existido una disminución de requerimientos considerables ya que la mejora que ofrece este producto es a nivel de seguridad y a nivel de gestión de requerimientos.

Adicionalmente se recomienda que la integración se lo haga paulatinamente para poder disminuir el impacto del cambio con respecto a la Organización.

CONCLUSIONES

1. La implementación del SSO no tiene impacto en la arquitectura de las aplicaciones, topologías siendo una solución que no impacta a los procesos del negocio.

2. Se cubre la simplificación de accesos y la administración de la seguridad de los sistemas informáticos.

3. SSO se presenta como una estrategia de seguridad, la cual puede prestar amplios beneficios, como incrementar el contexto de seguridad y proveer un inicio de sesión único a través de todas las aplicaciones.

4. Se logra una mejora significativa desde el punto de vista de la seguridad de la información, puesto que cuando no se tenía implementada esta solución el usuario estaba obligado a recordar varias contraseñas para el acceso a diferentes aplicaciones que cuentan con políticas diferentes de

contraseñas lo que derivaba en la utilización de contraseñas fáciles de adivinar o escritas en papel cerca de los puestos de trabajo.

5. Es compatible con un amplio rango de dispositivos de autenticación soportando tarjetas inteligentes, infraestructuras de llave pública, biometría.

6. Proporciona un alto retorno de la inversión, ya que ahorra tiempo y dinero en las mesas de ayuda al responder solicitudes de usuarios para que restablezcan sus contraseñas olvidadas.

7. Soporta la autenticación convencional (usuario/contraseña).

8. Reduce el tiempo utilizado al introducir la información de usuario/contraseña, ya que el sistema las inyecta automáticamente.

9. Los usuarios de la organización se vuelven productivos de manera más rápida mediante el acceso inmediato a las aplicaciones y sistemas.

RECOMENDACIONES

1. Debe soportar los dos esquemas de manejo de contraseñas, la gestión local y la gestión centralizada.

2. Se recomienda que la información de la billetera (usuarios/contraseñas) que permiten acceder a las aplicaciones autorizadas se las guarde en una base de datos o directorio activo.

3. Debe tener la opción de manejar varias contraseñas en las aplicaciones integradas en la solución (no solo una clave para todas las aplicaciones).

4. Como en todos los sistemas debe disponer de un plan de contingencia para garantizar la continuidad del negocio.

5. Las contraseñas deben estar cifradas.

6. Debe incorporar la funcionalidad en la billetera de poder visualizar las contraseñas por olvido solicitando alguna autenticación para poder acceder.

7. Se debe poder acceder a la billetera desde cualquier computadora conectada a la red y también permitir exportar las contraseñas almacenadas.

8. Revisar detalladamente los requerimientos con respecto al consumo que genere el agente en las PCs instaladas.

9. Con la implementación de la solución SSO, se recomienda que también se adquiera una tecnología de Administrador de Identidades (IDM).

BIBLIOGRAFÍA

[1] ISO/IEC 27002:2005, http://www.iso27000.es/download/ControlesISO27002-2005.pdf, fecha de consulta Julio del 2015.

[2] Enterprise Single Sign On (SSO) Manager, http://www.tools4ever.es/software/enterprise-single-sign-on-manager/, fecha de consulta Julio del 2015

[3] Enterprise Single Sign-on, http://www.dell.com/mx/empresas/p/dell-software-enterprise-single-sign-on/pd, fecha de consulta Julio del 2015

[4] Implementación Interservices de Oracle Enterprise Single Sign On, http://www.oracle.com/technetwork/es/articles/idm/tutorial-implementar-single-sing-on-1836115-esa.html, fecha de consulta Julio del 2015

[5] Single Sign On, https://www.prise.es/es/services/digid/sso/, fecha de consulta Julio del 2015.