CONTROLES DE SEGURIDAD EN APLICACIONES ENTIDAD PROMOTORA DE SALUD

TRABAJO DE GRADO

Lyda Janeth Rodríguez Torres

Código 1622010064

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

CONTROLES DE SEGURIDAD EN APLICACIONES ENTIDAD PROMOTORA DE SALUD

TRABAJO DE GRADO

Lyda Janeth Rodríguez Torres

Código 1622010064

Asesor

Ingeniero Alejandro Castiblanco Caro

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá, Septiembre de 2017

ÍNDICE

1. INTRODUCCIÓN

La información es uno de los activos más importante en las empresas y el objetivo principal es preservar su correcto procesamiento y almacenamiento dentro de un adecuado entorno de seguridad.

En la actualidad han aumentado la cantidad de casos de incidentes relacionados con la seguridad de los sistemas de información que comprometen los activos información de las empresas, por esto es necesario estar alerta e implementar sistemas de seguridad basados en un análisis de riesgos para evitar o minimizar las consecuencias no deseadas.

Es importante tener un claro conocimiento sobre los procesos del negocio en cuanto a su composición y su criticidad, esto con el fin de priorizar las acciones de seguridad en los procesos claves o críticos, vinculados al logro de los objetivos de la organización implementando controles de seguridad.

La correcta implementación de las herramientas disponibles para tal fin permite a las compañías y empresas en general alcanzar los objetivos de seguridad y garantizar la disponibilidad, confidencialidad e integridad de la información.

2. RESUMEN EJECUTIVO

Proyecto: Controles de Seguridad en Aplicaciones - Entidad Promotora De Salud

El presente proyecto busca generar una propuesta para brindar solución al problema de seguridad presentado actualmente en la Entidad Promotora de Salud (EPS), la cual maneja varias aplicaciones que son compartidas con sus Instituciones Prestadoras de Salud (IPS) en las cuales prestan los servicio a los usuarios a nivel nacional, muchas personas tienen acceso a las aplicaciones y a la información almacenada, el problema radica en la falta de controles en las aplicaciones, se presenta manipulación indebida de información en algunas aplicaciones ya que los usuarios y claves son genéricos, o no piden clave de acceso, además permiten la modificación o eliminación de la información, esto afecta gravemente la confidencialidad, integridad y disponibilidad como pilares de la seguridad de la información.

Así mismo en los nuevos desarrollos no se contempla la asignación de roles, porque se requiere funcionalidad y puestas en producción inmediatas, con lo que se evidencia que la alta dirección no dimensiona la grave falla de seguridad que hay en la EPS, ya que la prioridad es la prestación de servicios, sin embargo la dirección de sistemas propone implementar el sistema de gestión de seguridad para mitigar los riesgos que se presentan actualmente, implementando un sistema de gestión de contraseñas.

En la presente propuesta se analiza la situación presentada actualmente en la Entidad Promotora de Salud que desencadena en problemas de seguridad, mediante una matriz de valoración estratégica se valoran las posibles acciones que pueden dar solución al problema evidenciado, generando un diagnostico que facilite la toma de decisiones con el fin de lograr una efectiva administración de usuarios y derechos de acceso a las aplicaciones y a la información.

Por lo cual se realiza un análisis de riesgos basado en la norma ISO 31000:2011, donde una vez identificado el problema y las causas, se identifican los activos de información que pueden verse afectados por vulnerabilidades del sistema, se identifican los riesgos a los que se encuentran expuestos los activos, los cuales son analizados y valorados para determinar su impacto y probabilidad de ocurrencia.

Teniendo en cuenta el resultado de la matriz de valoración estratégica y el análisis de riesgos, como plan de tratamiento y gestión de riesgos, se definen los controles a implementar para mitigar los riegos y el impacto que puedan tener para la EPS, estableciendo la necesidad de implementar controles de acceso a las aplicaciones mediante metodologías de desarrollo seguro para los nuevos desarrollos y los que se encuentran en producción, incluyendo inicios de sesión mediante usuario y contraseña, asignando roles dependiendo la función y el cargo para el acceso a las aplicaciones e incluyendo logs de eventos que permitan hacer un seguimiento a las actividades realizadas en las aplicaciones.

Con el objetivo de implementar los controles planteados, la propuesta se basará en la norma internacional ISO/IEC 27002:2013, con las buenas prácticas para la Gestión de la Seguridad de la Información, por lo que se centra en el dominio N° 11. CONTROL DE ACCESOS, específicamente el ítem 11.6 Control de acceso a las aplicaciones y a la información, para lo cual se presenta la Propuesta Metodología de Desarrollo Seguro y Gestión de Contraseñas buscando que todo el proceso de acceso y manipulación de aplicaciones de software sea gestionado de forma segura, han de tomarse una serie de medidas y buenas prácticas encaminadas a mejorar la seguridad en las mismas.

La siguiente propuesta consiste en brindar las indicaciones a seguir para implementar controles de acceso a las aplicaciones, en los nuevos desarrollos y los que se encuentran en producción, con el fin de garantizar que las aplicaciones de software y las utilidades son seguras y fiables.

Posterior a la implementación de los controles definidos para el tratamiento de los riesgos, estos se evalúan de nuevo en cuanto a impacto a probabilidad determinando que el riesgo es mitigado, cumpliendo así con los objetivos del proyecto.

Se definieron las actividades de monitoreo y revisión a realizar para identificar la efectividad de los controles implementados y para detectar nuevas vulnerabilidades que requieran tratamiento.

Con la implementación de las acciones propuestas en cuanto a controles de seguridad, se disminuye el porcentaje de incidentes de seguridad notablemente lo cual se evidencia en la revisión de los indicadores de gestión.

Frente al riesgo residual posterior al tratamiento, se define que La EPS asume estos riesgos en caso de materializarse, pero se buscará mitigar y eliminar por completo con la creación de una política de manejo de la información y programas de capacitación y formación a los funcionarios frente a la seguridad de la información.

3. JUSTIFICACIÓN

Cada vez son más frecuentes los incidentes de seguridad presentados en la EPS, esto se ha evidenciado mediante la Herramienta de Gestión de Incidencias donde se han reportado en el último semestre 100 casos de alteración de la información, evidenciando un alto nivel de afectaciones a la integridad de la misma, de igual forma durante el mismo periodo se han evidenciado en el log de eventos la eliminación de 30 registros de información de los afiliados a la EPS generando indisponibilidad de la información y afectación en la prestación del servicio al usuario.

Las aplicaciones no tienen controles que limiten su uso e impidan modificar o eliminar información, así mismo se evidencia que no cuentan con control de acceso ya que emplean usuarios genéricos o no solicitan clave de acceso, analizando el último semestre se ha evidenciado que la entidad cuenta con 2 aplicaciones en fase de desarrollo y 4 aplicaciones en producción en la EPS e IPS, las cuales no cuentan con control de acceso y no tienen definidos roles con permisos establecidos de consulta, modificación o borrado, esto evidencia un alto nivel de vulnerabilidad a la seguridad de la información.

Por lo anterior y teniendo en cuenta la información obtenida mediante encuestas realizadas a diferentes funcionarios de la EPS y sus IPS vinculadas, en cuanto a las falencias y vulnerabilidades evidenciadas en la seguridad de la información, se determinaron y establecieron los siguientes indicadores con el fin de que se convierta en un sistema de alertas tempranas, para diagnosticar problemas y medir la situación de riesgo de la empresa.

Indicador de Integridad, permite medir el porcentaje de incidentes que afectan la integridad de la información.

Indicador de Disponibilidad, permite medir el porcentaje de registros de afiliados que son eliminados por error de las bases de datos y que afectan la disponibilidad de la información.

Indicador de Riesgo de Acceso, permite medir el porcentaje de aplicaciones que no tienen controles de acceso, generando un alto nivel de riesgo y vulnerabilidad en la seguridad de la información.

4. MARCO TEÓRICO Y REFERENTES

La seguridad informática actualmente es un tema en el que toda empresa necesita invertir, puesto que las consecuencias de no hacerlo pueden ser catastróficas, las empresas almacenan información de sus clientes, usuarios y proveedores en bases de datos y esta debe ser correctamente protegida, ya que se puede ver expuesta a riesgos como lo son las amenazas humanas, tecnológicas y eventos naturales.

Los datos y la información de las organizaciones se deben conservar en un entorno seguro donde se mantengan los niveles de riesgos informáticos en un nivel aceptable, garantizando el cumplimiento de los tres principios básicos: confidencialidad, integridad y disponibilidad.

Con el fin de implementar controles de seguridad, inicialmente es importante contar con una metodología para realizar un análisis de riesgos e identificar claramente vulnerabilidades, riesgos y amenazas presentes en los activos de información, la norma Internacional ISO 31000 es un sistema eficiente para la gestión de riesgos, la cual establece un conjunto de principios que se deben satisfacer para que la gestión del riesgo sea eficaz y es una metodología apta para identificar los riesgos que deben ser gestionados permitiendo optimizar los procesos organizacionales.

La seguridad de la información según la norma internacional ISO/IEC 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, esta norma ofrece una guía donde especifica los requisitos para establecer, implementar, supervisar y mejorar un sistema de seguridad de la información y establece un enfoque por procesos basado en el ciclo Deming, que plantea la gestión de la seguridad como un proceso de mejora continua, mediante cuatro fases que son planificar, hacer, verificar y actuar.

Con el objetivo de implementar controles para impedir el acceso no autorizado a las aplicaciones esta propuesta se basará en la norma internacional ISO/IEC 27002:2013, con las buenas prácticas para la Gestión de la Seguridad de la Información y teniendo en cuenta los siguientes conceptos:

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO 27000)

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO 27000)

Análisis de riesgo: proceso llevado a cabo para comprender la naturaleza del riesgo y determinar el nivel de riesgo (ISO 27000)

Autenticidad: Aseguramiento de la identidad u origen (ISO 27000).

Confidencialidad: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso (ISO 27000).

Control: medida que modifica al riesgo (ISO 27000).

Disponibilidad Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados (ISO 27000).

Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (ISO 31000:2011)

Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc. (ISO 27000)

Integridad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento

ISO 31000: Gestión de Riesgos, Principios y Guías es una Norma Internacional que pudiera manejar cualquier organización interesada en tratar los riesgos a los que está expuesta.

ISO/IEC 27001: 2013 Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información

ISO/IEC 27002: guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Probabilidad: es la oportunidad de que algo suceda (ISO 31000 :2011)

Riesgo: Efecto de la incertidumbre sobre los objetivos. (ISO 31000:2011)

Seguridad De La Información: consiste en la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en el tratamiento de la información dentro de una organización.

Sistema De Gestión De La Seguridad De La Información: conjunto de políticas de administración de la información, diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. METODOLOGÍA

Mediante una matriz de valoración estratégica se analizan desde el punto de vista de los interesados las causas que ocasionan el problema identificado y se proponen las posibles acciones para buscar solución al problema, dichas acciones son valoradas en cuanto a su gobernabilidad, el impacto y la pertinencia que tendría su implementación, (ver Matriz de Valoración Estratégica).

Posteriormente se realiza un análisis de riesgos basado en la norma ISO 31000:2011, en el cual una vez identificado el problema y las causas, se identifican los activos de información que pueden verse afectados por vulnerabilidades del sistema, se identifican los riesgos a los que se encuentran expuestos los activos, los cuales son analizados y valorados para determinar su impacto y probabilidad de ocurrencia.

Teniendo en cuenta el resultado de la matriz de valoración estratégica y el análisis de riesgos, como plan de tratamiento y gestión de riesgos, se definen los controles a implementar para mitigar los riegos y el impacto que puedan tener para la EPS, estableciendo la necesidad de implementar controles de acceso a las aplicaciones mediante metodologías de desarrollo seguro para los nuevos desarrollos y los que se encuentran en producción, incluyendo inicios de sesión mediante usuario y contraseña, asignando roles dependiendo la función y el cargo para el acceso a las aplicaciones e incluyendo logs de eventos que permitan hacer un seguimiento a las actividades realizadas en las aplicaciones, (ver Gestión de Riesgos).

Con el objetivo de implementar los controles planteados, la propuesta se basará en la norma internacional ISO/IEC 27002:2013, con las buenas prácticas para la Gestión de la Seguridad de la Información, por lo que se centra en el dominio N° 11. CONTROL DE ACCESOS, específicamente el ítem 11.6 Control de acceso a las aplicaciones y a la información, para lo cual se presenta la Propuesta Metodología de Desarrollo Seguro y Gestión de Contraseñas.

6. RESULTADOS Y DISCUSIÓN

Posterior a la implementación de los controles definidos para el tratamiento de los riesgos, estos se evalúan de nuevo en cuanto a impacto a probabilidad determinando que el riesgo es mitigado, cumpliendo así con los objetivos del proyecto.

Se definieron las actividades de monitoreo y revisión a realizar para identificar la efectividad de los controles implementados y para detectar nuevas vulnerabilidades que requieran tratamiento.

Con la implementación de las acciones propuestas en cuanto a controles de seguridad, se disminuye el porcentaje de incidentes de seguridad notablemente lo cual se evidencia en la revisión de los indicadores de gestión.

Frente al riesgo residual posterior al tratamiento, se define que La EPS asume estos riesgos en caso de materializarse, pero se buscará mitigar y eliminar por completo con la creación de una política de manejo de la información y programas de capacitación y formación a los funcionarios frente a la seguridad de la información, (ver Gestión de Riesgos)

7. CONCLUSIONES

Como resultado del análisis realizado al problema de seguridad presentado en la Entidad Promotora de Salud, es posible concluir que es necesario implementar controles eficientes que permitan mitigar el riesgo al que se encuentra expuesta la información.

Así mismo es de vital importancia contar con el compromiso y apoyo de la Alta Dirección para la implementación de las medidas propuestas, en aras de garantizar la confidencialidad, integridad y disponibilidad de la información.

8. BIBLIOGRAFÍA

1. Fortalecimiento de la gestión TI en el estado, Sistemas de Gestión de la Seguridad de la Información (SGSI), MINTIC http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

2. Lineamientos de Administracion de Seguridad – Tics, Presidencia de la Republica, Junio de 2016, http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/L-TI-03-Administracion-Seguridad.pdf

3. ISO 27000, glosario http://www.iso27000.es/glosario.html

4. ISO27002.es, Control de acceso a sistemas y aplicaciones http://www.iso27000.es/iso27002_9.html

5. We live secutiry, Los 10 principios básicos para un desarrollo seguro, https://www.welivesecurity.com/la-es/2014/02/28/10-principios-basicos-para-desarrollo-seguro/

9. ANEXOS

9.1 PROPUESTA METODOLOGÍA DE DESARROLLO SEGURO Y GESTIÓN DE CONTRASEÑAS.

Con el objetivo de que todo el proceso de acceso y manipulación de aplicaciones de software sea gestionado de forma segura, han de tomarse una serie de medidas y buenas prácticas encaminadas a mejorar la seguridad en las mismas.

La siguiente propuesta consiste en brindar las indicaciones a seguir para implementar controles de acceso a las aplicaciones, en los nuevos desarrollos y los que se encuentran en producción, con el fin de garantizar que las aplicaciones de software y las utilidades son seguras y fiables.

Los usuarios deberán registrarse e identificarse para acceder a dichos servicios mediante una contraseña y con determinados permisos de acuerdo a su cargo y perfil, por lo tanto se debe garantizar:

- Impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.
- Asignación y administración de usuarios por cada funcionario, no pueden existir usuarios genéricos.
- Creación de matriz de roles asignando permisos dependiendo la función y el cargo asignado.
- Incluir logs de eventos que permitan hacer un seguimiento a las actividades realizadas en las aplicaciones.
- Asignación de permisos para consulta, modificación o eliminación de información.

La mayoría de los procesos y operaciones requieren autenticación por lo que es importante la correcta gestión y creación de las contraseñas, por lo tanto se define la siguiente política:

Política de gestión de contraseñas:

- El usuario se creará con una clave genérica que será cambiada en el primer inicio de sesión y que solo debe conocer el propietario del mismo.
- La longitud de las contraseñas no debe ser inferior a ocho caracteres.
- Las contraseñas deben incluir mayúsculas, minúsculas, números y caracteres especiales.
- Usar contraseñas diferenciadas en función del uso (no debe usarse la misma contraseña de red para el acceso a las aplicaciones de la EPS).
- Las contraseñas caducan cada mes por lo que debe solicitar cambio antes de finalizar el mes, en caso de no cambiarla la cuenta será bloqueada.
- Las aplicaciones deben tener opción de cambio de contraseña voluntario.
- No debe contener el usuario (ni viceversa).
- No debe contener la contraseña anterior (ni viceversa).
- Debe diferenciarse del usuario en al menos 3 caracteres.
- Debe diferenciarse de la contraseña anterior en al menos 3 caracteres.
- No debe coincidir con las últimas 4 contraseñas usadas.
- Las contraseñas no deben estar embebidas en el código, para permitir la posibilidad de cambiarlas y que puedan caducar.
- Las aplicaciones no deben permitir para las contraseñas utilizar secuencias básicas de teclado (por ejemplo:”qwerty”, “asdf”, “1234” o “98765”)

Así mismo se deberán tener en cuenta los siguientes principios para realizar un desarrollo de software seguro, recomendado por “we live security”:

1. Partir siempre de un modelo de permisos mínimos, es mejor ir escalando privilegios por demanda de acuerdo a los perfiles establecidos en las etapas de diseño.
2. Si se utiliza un lenguaje que no sea compilado, asegurarse de limpiar el código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.
3. Nunca confiar en los datos que ingresan a la aplicación, todo debe ser verificado para garantizar que lo que está ingresando a los sistemas es lo esperado y además evitar inyecciones de código.
4. Hacer un seguimiento de las tecnologías utilizadas para el desarrollo. Estas van evolucionando y cualquier mejora que se haga puede dejar obsoleta o inseguras versiones anteriores.
5. Todos los accesos que se hagan a los sistemas deben ser validados.
6. Para intercambiar información sensible utilizar protocolos para cifrar las comunicaciones, y en el caso de almacenamiento la información confidencial debería estar cifrada utilizando algoritmos fuertes y claves robustas.
7. Cualquier funcionalidad, campo, botón o menú nuevo debe agregarse de acuerdo a los requerimientos de diseño. De esta forma se evita tener porciones de código que resultan siendo innecesarias.
8. La información almacenada en dispositivos móviles debería ser la mínima, y más si se trata de contraseñas o datos de sesión. Este tipo de dispositivos son los más propensos a ser que se pierdan y por lo tanto su información puede ser expuestas más fácilmente.
9. Cualquier cambio que se haga debería quedar documentado, esto facilitará modificaciones futuras.
10. Poner más cuidado en los puntos más vulnerables, no hay que olvidar que el nivel máximo de seguridad viene dado por el punto más débil.

Se realizará la planificación de pruebas, la creación de conjuntos de pruebas y la ejecución de las mismas con el fin de validar la funcionalidad desarrollada y sus niveles de seguridad.

Documentos Anexos:

- Matriz de valoración estratégica
- Gestión de Riesgos
- Resumen Ejecutivo