GESTION DE IDENTIDADES EN UNA COMPAÑÍA DE SEGUROS

TRABAJO DE GRADO

DIANA PATRICIA SÁNCHEZ MORENO.
JOHANNA MARCELA FORERO VARELA
SANDRA PATRICIA CEDIEL BRAVO

Códigos
1612010661
1512011807
1612010429

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

GESTIÓN DE IDENTIDADES EN UNA COMPAÑÍA DE SEGUROS

TRABAJO DE GRADO

PARTICIPANTES
DIANA PATRICIA SÁNCHEZ MORENO.
JOHANNA MARCELA FORERO VARELA
SANDRA PATRICIA CEDIEL BRAVO

Códigos
1612010661
1512011807
1612010429

Asesor
ALEJANDRO CASTIBLANCO CARO

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

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 27 de mayo de 2017

Dedicamos este trabajo a nuestra familia, que nos acompañó durante todo este proceso de aprendizaje.

AGRADECIMIENTOS

Agradecemos a todas aquellas personas que nos apoyaron de manera incondicional ya que permitieron que llegáramos hasta este momento.

CONTENIDO

Pág.
1. INTRODUCCIÓN 13
2. OBJETIVOS 14
2.1 OBJETIVO GENERAL 14
2.2 OBJETIVOS ESPECÍFICOS 14
3. PLANTEAMIENTO DEL PROBLEMA 15
3.1 DEFINICIÓN DEL PROBLEMA 15
3.2 JUSTIFICACIÓN 16
4. ALCANCE 18
5. PLAN DE TRABAJO 19
6. MARCO TEÓRICO Y REFERENTES 20
7. METODOLOGÍA 23
8. RESULTADOS Y DISCUSIÓN 26
8.1 DIAGNÓSTICO DE LAS NECESIDADES ACTUALES DE LA ORGANIZACIÓN 26
8.1.1 ANÁLISIS DE CONTEXTO 27
8.1.2 CONTEXTO INTERNO 27
8.1.3 BENEFICIOS DE LA GESTIÓN DE IDENTIDADES: 31
8.1.4 PROCEDIMIENTOS ACTUALES PARA LA GESTIÓN DE ACCESOS Y CONTROL DE IDENTIDADES 33
8.2 POLÍTICA DE CONTROL DE ACCESOS Y GESTIÓN DE IDENTIDADES 36
8.3 ESQUEMA PARA LA GESTION Y CICLO DE VIDA DE LAS IDENTIDADES. .. 37
8.4 PROGRAMA DE CAPACITACIÓN Y SENSIBILIZACIÓN A LOS USUARIOS FINALES 40
9. CONCLUSIONES 42
10. BIBLIOGRAFIA 43

LISTA DE TABLAS

Pág.

Tabla 1. Plan de trabajo 19

Tabla 2. Buenas Prácticas y Marcos de Referencia 24

Tabla 3. Responsables del Ciclo de Vida de la Identidad 40

LISTA DE GRÁFICOS

Pág.

Gráfico 1. Fases del Proyecto 25

Gráfico 2. Promesa de Valor 28

Gráfico 3. Mapa de Procesos 29

Gráfico 4. Organigrama 30

Gráfico 5. Productos y Servicios 31

Gráfico 6. Ciclo de Vida de la Identidad 38

LISTA DE ANEXOS

Anexo 1. Políticas de Gestión de Accesos

Anexo 2. Procedimientos

Anexo 3. Artículo de Escritorios limpios, responsabilidad de todos

Anexo 4. Artículo de Préstamos de usuarios y claves

Anexo 5. Artículo de uso del correo electrónico

Anexo 6. La seguridad, compromiso de todos - Papel tapiz

Anexo 7. Cronograma de actividades semana de la seguridad

GLOSARIO

ANÁLISIS DE RIESGO: Uso sistemático de una metodología para la identificación fuentes o amenazas a las cuales están expuestos los activos, bienes o recursos de la compañía y estimar el riesgo escribe aquí la definición de la primera palabra ordenada por orden alfabético de forma similar a un diccionario.

CONTROL: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía.

GESTIÓN DEL RIESGO: Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

IDENTIFICACIÓN DEL RIESGO: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo asociados a la seguridad de la información.

IDM: Es una solución que combina estrategia, procesos, políticas, prácticas y tecnologías para proporcionar acceso a los recursos e información a los empleados, canales / socios, clientes y proveedores, basado en reglas de negocios asociadas con roles y perfiles dentro de la organización, de una manera segura y continua.

INFORMACIÓN: Es un activo que, al igual que otros importantes activos de negocios, es esencial para los negocios de la organización y por tanto requiere ser protegida de forma adecuada.

IMPACTO: Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos del negocio.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

POLÍTICA DE SEGURIDAD: Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

PROCEDIMIENTO: Documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

REDUCCIÓN DEL RIESGO: Acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.

TRATAMIENTO DEL RIESGO: Proceso de selección e implementación de medidas para modificar el riesgo.

RESUMEN

En la compañía de seguros actualmente existen grandes falencias en el proceso de administración de identidades y accesos a los diferentes recursos tecnológicos; esta situación se presenta debido a la ausencia de políticas, procedimientos y controles formales que permitan una adecuada gestión. Se presentan entonces riesgos asociados a la pérdida de disponibilidad, confidencialidad e integridad de la información. Principalmente se evidencia que la organización utiliza diversos sistemas de información destinados a apoyar el desarrollo de las actividades de los procesos críticos, y esto dificulta en buena medida una correcta administración en cuanto al establecimiento de roles, perfiles adecuados y la consecuente asignación de usuarios que son la base para la definición del esquema adecuado para la gestión de identidad dentro de una compañía. Una entidad que maneja información de clientes tiene como principal responsabilidad, el cuidado y protección de la confidencialidad y privacidad de los datos personales entregados por los mismos, ya que esto le permite mantener su reputación y dar cumplimiento a la normatividad vigente. El presente proyecto tiene como objetivo principal establecer un procedimiento orientado a la administración de accesos a los diferentes aplicativos y recursos de la compañía, a través de la implementación del esquema para la gestión de identidades, con el fin de mitigar los riesgos asociados a la confidencialidad, integridad, disponibilidad y trazabilidad de la información. Para este fin se requiere contar con el diagnóstico de las necesidades de la organización, respecto a la gestión de identidades. Posteriormente definir políticas y procedimientos para la gestión y control de accesos de los usuarios y finalmente diseñar y establecer los lineamientos generales del plan de entrenamiento y sensibilización de los usuarios internos de la compañía, logrando así una eficiente administración de los accesos a los diferentes sistemas de información.

PALABRAS CLAVE: Seguridad de la Información, riesgos, gestión de identidades.

1. INTRODUCCIÓN

Actualmente toda compañía busca día a día mejorar sus procesos internos, rentabilidad e imagen frente a sus clientes y para lograr este objetivo requiere conocerse, identificar sus procesos críticos y evaluar sus resultados. Este proyecto se desarrolla para apoyar algunos de estos objetivos, por lo cual se ha analizado un problema identificado en una de las áreas que maneja información crítica de la compañía, con el fin de efectuar un diagnóstico de la situación actual, a través de la aplicación de una metodología específica enmarcada en un modelo de planeación estratégica situacional. En la primera parte se efectúa el planteamiento inicial del problema y se determinan sus cadenas causales, para obtener un mayor entendimiento de la situación que se presenta internamente.

Así mismo se presenta el diagnóstico de la situación actual de manera clara, y se plantea el diseño de una solución de gestión de identidades controlando el acceso a los diferentes recursos, con el fin de mitigar los riesgos asociados a la seguridad de la información.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer un proceso orientado a la administración de accesos a los diferentes aplicativos y recursos de la compañía, a través del diseño e implementación de un esquema para la gestión de identidades, con el fin de mitigar los riesgos asociados a la confidencialidad, integridad, disponibilidad y trazabilidad de la información que surgen a partir de la misma.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico de las necesidades de la organización, respecto a la gestión de identidades así como los recursos actuales, para seleccionar una solución que se ajuste a la misma.

- Definir las políticas y procedimientos para la gestión y control de usuarios y accesos.

- Definir el esquema y ciclo de vida para la gestión de identidades.

- Establecer los lineamientos y recomendaciones para generar el plan de sensibilización y entrenamiento dirigido a los usuarios finales.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

En la actualidad las empresas deben cuidar de manera importante todos sus activos de información ya que están expuestos a múltiples vulnerabilidades, dentro de las cuales podemos encontrar los ataques ejecutados por personas que buscan cometer delitos informáticos o adquirir la información de la empresa con fines fraudulentos.

Adicionalmente, una entidad que maneja información de clientes tiene como principal responsabilidad, el cuidado y protección de la confidencialidad y privacidad de los datos personales entregados por los mismos, ya que esto le permite mantener su reputación y dar cumplimiento a la normatividad vigente.

De acuerdo con el análisis realizado en la organización, actualmente existen grandes falencias en el proceso de administración de identidades y accesos a los diferentes recursos de la misma, debido a la ausencia de políticas, procedimientos y controles formales que permitan una adecuada gestión, generando así riesgos asociados a la pérdida de disponibilidad, confidencialidad e integridad de la información.

Una de las debilidades identificadas es que debido a que en la organización se utilizan diversos sistemas de información destinados a apoyar el desarrollo de las actividades de los procesos, se dificulta en buena medida una correcta administración de los mismos con el establecimiento de roles y perfiles adecuados y la consecuente asignación de usuarios.

La mayoría de estos sistemas de información tienen sus propios controles o sistemas de autenticación, lo que conlleva a que los usuarios deban manejar varias contraseñas de usuario con diferentes características dificultando en consecuencia el acceso a las aplicaciones.

Así mismo, se ocasionan sobrecargas en la administración de los sistemas de información al tener que desarrollar las labores administrativas (creación,

eliminación, cambios de usuarios, asignación de perfiles, etc.) para cada uno de ellos.
Todo esto origina la problemática identificada en la compañía, presentándose situaciones graves que exponen los activos de información a diversos riesgos de seguridad.

Dado lo anterior y con el fin de mitigar estos riesgos, se considera pertinente implementar soluciones que le permitan a la compañía protegerse internamente, reducir costos y, en consecuencia, ser mas competitiva dentro del mercado.

3.2 JUSTIFICACIÓN

La seguridad informática cada vez ocupa un lugar más privilegiado en las organizaciones ya que con los avances de la tecnología durante los últimos años, se brinda mayor accesibilidad a la información, situación que ha traído sus ventajas pero también sus desventajas toda vez que surge la necesidad mayor de proteger dicha información de accesos no autorizados.

La información es el activo más importante que posee una organización y por ende, debe protegerse de las diversas amenazas del entorno; la información juega un papel fundamental en las compañías y es el corazón de todo tipo de negocios y teniendo en cuenta que hoy día existe mayor dependencia de los usuarios y la tecnología, es imperativo establecer medidas para que no sea vulnerada.

Dados los riesgos de seguridad de la información identificados en la compañía, relacionados con la gestión de acceso de los usuarios a las diferentes herramientas tecnológicas, causados entre otros por la inexistencia de políticas, procedimientos y controles que contribuyan a su mitigación, es fundamental buscar una solución que conjugue lo anterior con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información, garantizando el control de acceso a la misma y de la misma forma a los recursos de la empresa.

De otra parte, no solo basta con controlar el acceso a los recursos sino que es imprescindible administrar de forma correcta los privilegios de los usuarios, sin afectar la usabilidad de los sistemas, y por tal razón se definió que la articulación de un buen sistema de gestión de accesos y gobierno de identidades es imprescindible para la organización.

Esto con el fin de posibilitar de forma segura, que las personas adecuadas dispongan del acceso adecuado a los recursos adecuados, en el momento adecuado y por los motivos adecuados (Gartner).

Ahora bien, la implementación de un sistema de gestión de identidades y un control de accesos trae grandes beneficios a la organización, entre los cuales se destacan los siguientes:

- Cumplimento normativo: Al ser una sociedad sujeta a control y supervisión de la Superintendencia Financiera de Colombia y teniendo en cuenta que maneja información privada de los clientes, está obligada al cumplimiento de los requerimientos legales impuestos para garantizar la confidencialidad y privacidad de la información. Así mismo incrementa la capacidad de respuesta ante las auditorias efectuadas.

- Acceso sencillo y seguro a las aplicaciones: Esto garantiza mayor productividad al disminuir el tiempo de aprovisionamiento de usuarios, así como la certeza de la asignación de los roles y perfiles de acceso apropiados según el cargo y funciones de los usuarios.

- Mayor control sobre el acceso a las aplicaciones y reducción de errores humanos en la asignación de privilegios.

- Reducción de costos de administración de usuarios: Gracias a la optimización de las funciones de administración del sistema.

Así las cosas, con la implementación de este proyecto se mitigan los riesgos de seguridad de la información asociados al acceso a los recursos en una compañía.

4. ALCANCE

El alcance del proyecto consiste en efectuar el diagnóstico de la situación actual respecto a la gestión de identidades y accesos dentro de la organización, para proceder a diseñar la política y procedimientos adecuados en relación con este tema, la definición del ciclo de vida de la gestión de identidades y la capacitación a los usuarios.

Este diseño se realiza con el fin de contar con un esquema para la gestión de identidades que contribuya a mitigar los riesgos existentes actualmente asociados a la confidencialidad, integridad y disponibilidad de la información.

Se establecerá el proceso de asignación, modificación y eliminación de usuarios de las aplicaciones, de manera controlada y documentada para proteger los activos críticos de información por medio de la gestión de identidades y control de acceso en un área que maneja la información crítica de la compañía, para lo cual:

- Se definirán políticas y procedimientos de control de accesos y gestión de identidades
- Se establecerá el esquema y ciclo de vida de la gestión de identidades
- Se planteará el plan de entrenamiento y sensibilización a los usuarios finales respecto a las responsabilidades frente a la autogestión y a la auto-administración de usuarios y accesos.

5. PLAN DE TRABAJO

PLAN DE TRABAJO		
FASE	**ACTIVIDADES**	**TIEMPO DE DURACION**
PLANEACION ORGANIZACIÓN Y PREPARACION	Reuniones con altos directivos y empleados de la organización.	**360 Horas**
	Visita técnica y levantamiento de información	
	Identificación de necesidades de la organización	
	identificación de riesgos y vulnerabilidades	
	Presentación de propuesta	
CONSTRUCCIÓN Y DISEÑO	Definición de políticas	**240 horas**
	Definición de procedimientos y controles	
	Definición del ciclo de vida de identidades	
SENSIBILIZACIÓN Y CAPACITACIÓN	Diseño del plan de sensibilización y capacitación	**80 horas**
	Ejecución del plan de acuerdo con el público objetivo definido	

Tabla 1. Plan de trabajo

6. MARCO TEÓRICO Y REFERENTES

Actualmente la información dentro de las organizaciones representa el activo más importante, por consiguiente el control de acceso a la misma ha cobrado una gran relevancia; el trafico global de la información y los avances tecnológicos han permitido generar soluciones que automaticen el acceso, no obstante, ante los peligros y amenazas que se descubren diariamente, es imprescindible implementar medidas de protección y procedimientos que aseguren la continuidad de la operación normal del negocio, evitando un acceso no autorizado y las consecuencias que esto conlleve para la organización.

Un Sistema de Gestión de Identidad o Identity Management System es un sistema integrado de procesos, políticas y tecnologías que permiten a las organizaciones facilitar y controlar el acceso de los usuarios a sus recursos y aplicaciones, permitiendo a la vez proteger su información confidencial, tanto personal como profesional, de usuarios no autorizados.(techtarget, 2016). Cualquier organización necesita proteger la identidad de sus datos, como cuánta gente hay, qué derechos y recursos tiene cada persona, que infraestructura le soporta y qué aplicaciones está utilizando; es vital por tanto, que la organización posea una estrategia IdM (Identity Management).

Según Microsoft[1] la correcta implementación de una estrategia IdM proporciona un ahorro de costos inmediato y a largo plazo, al utilizar el aprovisionamiento automático, la delegación de la administración y las aplicaciones de autoservicio. De esta forma son los usuarios quienes administran sus propias cuentas, y la carga de trabajo de las mesas de ayuda se ve reducida, lo que proporcionaría un aumento de la eficacia de la gestión de las mismas dentro de las organizaciones. El núcleo de toda estrategia IdM es la seguridad, específicamente la gestión de quién puede acceder a qué. Sin una estrategia IdM, el riesgo de que se hagan cosas mal o de que individuos no autorizados tengan acceso a datos sensibles es extremadamente alto, y su costo catastrófico.

La gestión de identidad involucra algunos conceptos que se deben tener claros dentro de la organización para su desarrollo e implementación:

1. Artículo publicado: Administración de identidad, en el sitio oficial de la compañía.https://www.microsoft.com/es-es/cloud-platform/identity-management

Activo de información: Bienes o recursos de información que tienen valor para la compañía.

Amenaza: Origen, fuente potencial de afectación que causa un incidente no deseado y puede resultar en un daño a un sistema u organización y/o a sus activos.

Autenticación: Es la verificación que un usuario es quien dice ser.

Autorización: Es la verificación del nivel de acceso de un usuario en un sistema de información.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

Control de acceso: Es la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular

Disponibilidad: Propiedad que determina que la información sea accesible y utilizable bajo solicitud por individuos, entidades o procesos autorizados.

Gestión de identidad: Conjunto de procesos, herramientas y estándares utilizados para la creación, mantenimiento, y utilización de identidades digitales por parte de personas, sistemas y servicios.

Identidad digital: Corresponde al conjunto de atributos, derechos y rasgos que identifican a un usuario.

Identificación: Es la verificación que una cuenta de usuario existe en un sistema de información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

ISO / IEC 27001：Es el estándar más conocido en la familia que proporciona los requisitos para un sistema de gestión de la seguridad de la información.(ISO, s.f.)

Permiso / Privilegio: Consiste en las autorizaciones o aprobaciones que tienen los usuarios para tener derecho a realizar una tarea, actividad o acción sobre un archivo, un servicio, la red o información. Por ejemplo, acceder a documentos, aplicaciones, realizar acciones sobre archivos, entre otros.

Riesgo en la seguridad de la información: Es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño a la organización.

Rol: Se refiere a la función que alguien o algo cumple. Con base en el rol, se asignan los permisos y privilegios.

Seguridad de la información - si: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Identidad: Es un sistema integrado de procesos, políticas y tecnologías que permiten a las organizaciones facilitar y controlar el acceso de los usuarios a sus recursos y aplicaciones

Vulnerabilidad: Debilidad asociada con los procesos, recursos o infraestructura de una organización. Una vulnerabilidad frecuentemente aumenta la probabilidad de que se materialice una amenaza.

Finalmente después de conocer la gestión de identidad, es vital implementarla en las organizaciones para reducir los accesos no autorizados, que puedan comprometer la información relevante del negocio, aunque la implementación requiere de recursos y cambios en los procesos organizacionales, al mismo tiempo proporciona beneficios considerables para la organización que apoyarán el control del acceso a la información de forma segura proporcionando integridad, confidencialidad y disponibilidad.

7. METODOLOGÍA

La metodología utilizada para el desarrollo del proyecto, contempla en su núcleo temático la revisión de la literatura existente, las investigaciones y publicaciones de los autores con gran trayectoria y experiencia en el tema, así como las firmas consultoras, evaluando el conocimiento existente a través de las fuentes de información más representativas, teniendo en cuenta los elementos clave.

En cuanto a normas y procedimientos, se tienen en cuenta los lineamientos establecidos de la norma ISO: 27001, respecto a la gestión de identidad a saber:

A.11 Control de Acceso

A11.1 Requisitos del negocio para el control de acceso

- Objetivo: Controlar el acceso a la información.
- Establecer documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

A 11.2 Gestión del acceso de los usuarios.

- Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información. Registro de usuarios, gestión de privilegios, gestión de contraseñas de usuarios y revisión de derechos de acceso.

Adicionalmente existen las buenas prácticas y marcos de referencia frente a la gestión de un sistema de gestión de identidad:

Nombre	Descripción
ISO/IEC 24760-1	Es aplicable a cualquier sistema de información que procese información de identidad. En esta primera parte se define la terminología y definiciones

ISO/IEC 24760-2	Proporciona directrices para la implementación de sistemas para la gestión de la información de identidad, y especifica los requisitos para la implementación y operación de un marco para la gestión de la identidad
ISO/IEC 24760-3	Proporciona orientación para la gestión de la información de identidad y para garantizar que el sistema de gestión de identidad cumple con ISO / IEC 24760-1 ISO / IEC 24760-2.
ISO/IEC 29115:2013	Gestión de acceso pruebas y verificación de identidad. Proporciona orientación sobre los controles que se deben utilizar para mitigar las amenazas de autenticación.

Tabla 2. Buenas Prácticas y Marcos de Referencia

Teniendo en cuenta las buenas prácticas y los marcos de referencia en el tema anteriormente mencionado, se desarrolla el proyecto en tres fases:

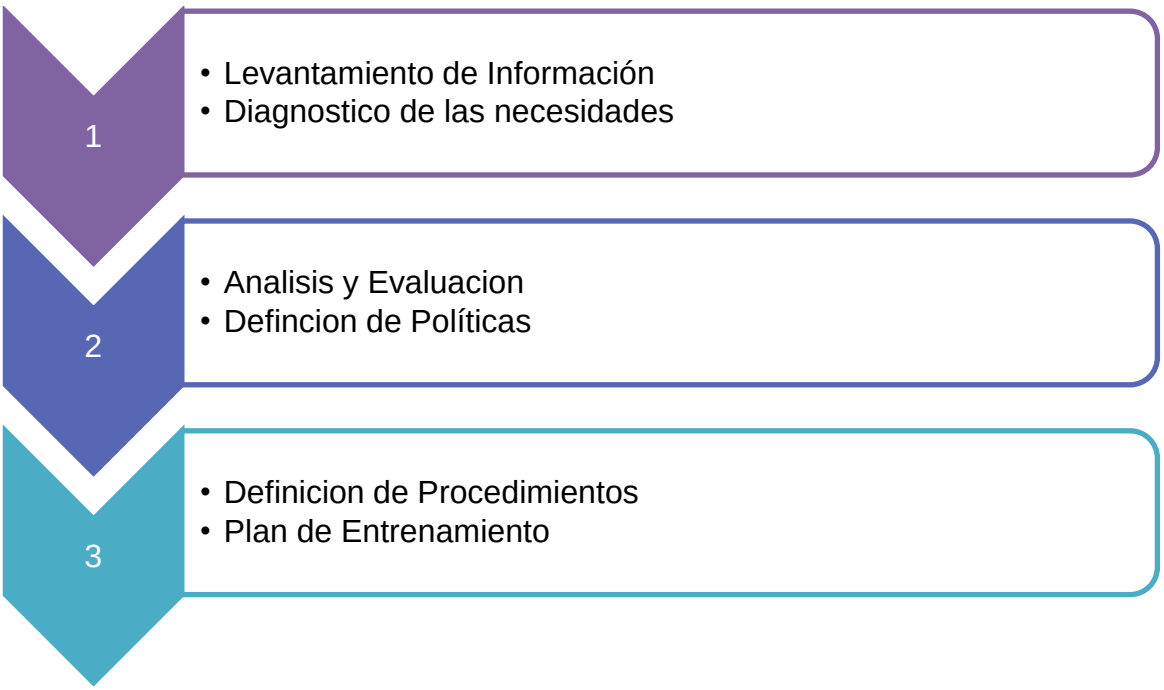

Gráfico 1. Fases del Proyecto

- ✓ La primera fase se desarrolla a través de un levantamiento de información con el fin de contar con el diagnóstico de la situación actual de la compañía en cuanto al manejo de los usuarios y el esquema de gestión de identidades el cual se constituye en el punto de partida para el desarrollo del proyecto.

- ✓ En una segunda fase se realiza un análisis, evaluación y generación de mecanismos de control a través del planteamiento de las políticas y procedimientos para la organización basadas en el diagnóstico realizado y en el Anexo A de la norma ISO 27001 11.1, Requisitos del negocio para el control de acceso.

- ✓ En la tercera y última fase se definen los lineamientos generales para la construcción del plan de entrenamiento y sensibilización de los usuarios finales.

8. RESULTADOS Y DISCUSIÓN

A continuación se procederá a explicar los resultados del desarrollo del proyecto, de acuerdo con los objetivos planteados y se detallaran los entregables generados:

- Entregable 1. Diagnóstico de las necesidades actuales de la organización.
- Entregable 2. Procedimientos de Gestión de accesos y Gestión de identidades.
- Entregable 3. Política de control de accesos y Gestión de Identidades.
- Entregable 4. Programa de capacitación y sensibilización de usuarios finales.

8.1 DIAGNÓSTICO DE LAS NECESIDADES ACTUALES DE LA ORGANIZACIÓN

Con el fin de conocer el diagnóstico del estado actual de la gestión de identidades en la compañía se hizo necesario llevar a cabo actividades que permitieran recopilar toda la información requerida, con el fin de entender su funcionamiento y determinar las necesidades, para posteriormente poder definir las políticas y procedimientos orientados a la administración de accesos a los diferentes aplicativos y recursos de la compañía, conforme a esas necesidades identificadas.

Para esto se hizo una consulta del contexto externo e interno de la compañía, estudiando el tipo de organización, su objeto social, partes interesadas, misión, visión, productos y servicios ofrecidos, organización interna e igualmente se efectuó una reunión con los colaboradores y se consultó el resultado de las auditorias que se efectuaron de manera previa.

Adicionalmente, se efectuó un acompañamiento a los colaboradores que manejan la información crítica y procesos relevantes, para conocer y entender sus actividades y la funcionalidad de los recursos que utilizan para desarrollarlas y en cierta medida, establecer el estado de concienciación al interior de la compañía respecto a la seguridad de la información.

Al tener entendimiento y conocimiento sobre la compañía, funcionamiento y su entorno, se establece el punto de partida para trazar los planes de mejoramiento y cambio, fortaleciendo su gestión y cumpliendo adicionalmente con los lineamientos de seguridad.

Se presentaron algunas dificultades en la construcción del diagnóstico, debido a que las personas con las que se llevo a cabo las reuniones no suministraron toda la información requerida, por falta de disposición o en algunas ocasiones porque la carga laboral impedía la realización de las mismas.

8.1.1 ANÁLISIS DE CONTEXTO

El análisis del contexto de la compañía constituye la base para identificar los riesgos críticos asociados con el problema identificado, relacionado con la gestión de identidades.

A partir del entendimiento de la compañía, sus objetivos estratégicos y de proceso, situaciones internas y externas que puedan afectar su desempeño, estructura de roles y responsabilidades, niveles de decisión, valores, cultura y estilo operativo, entre otros aspectos.

La empresa sobre la cual se desarrolla este proyecto es una compañía de seguros de economía mixta del orden nacional, sometida al régimen de las empresas industriales y comerciales del Estado, vinculada al Ministerio de Hacienda y Crédito Público y por el tipo de actividad que desempeña, también es vigilada por la Superintendencia Financiera de Colombia, por lo cual debe cumplir los lineamientos definidos en la Circular 029 del 2014 Parte I, Título II, Capítulo I “Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros”.

Es una de las principales entidades del sector asegurador colombiano, contando con un amplio portafolio de productos en ramos de seguros generales, patrimoniales, de personas y prestando sus servicios con una amplia presencia nacional.

8.1.2 CONTEXTO INTERNO

La compañía de seguros es una sociedad de economía mixta del orden nacional, sometida al régimen de las empresas industriales y comerciales del Estado. Cuenta con personería jurídica y autonomía administrativa, está vinculada al Ministerio de Hacienda y Crédito Público y es vigilada por la Superintendencia Financiera de Colombia.

- Misión y Visión

Misión: Generar tranquilidad, confianza y bienestar a los clientes, protegiendo sus bienes y patrimonio.

Visión: La compañía de seguros se destacará por un servicio ágil, amable y eficiente a través de su amplia cobertura y apoyada en la mejor gente. Entre 2013 y 2017 duplicará sus ingresos y se reconocerá su liderazgo en rentabilidad técnica y financiera en el sector asegurador. Será también reconocida como una de las 10 mejores empresas para trabajar en los mercados en que opere.

- Promesa de valor

Gráfico 2. Promesa de Valor

- Mapa de Procesos

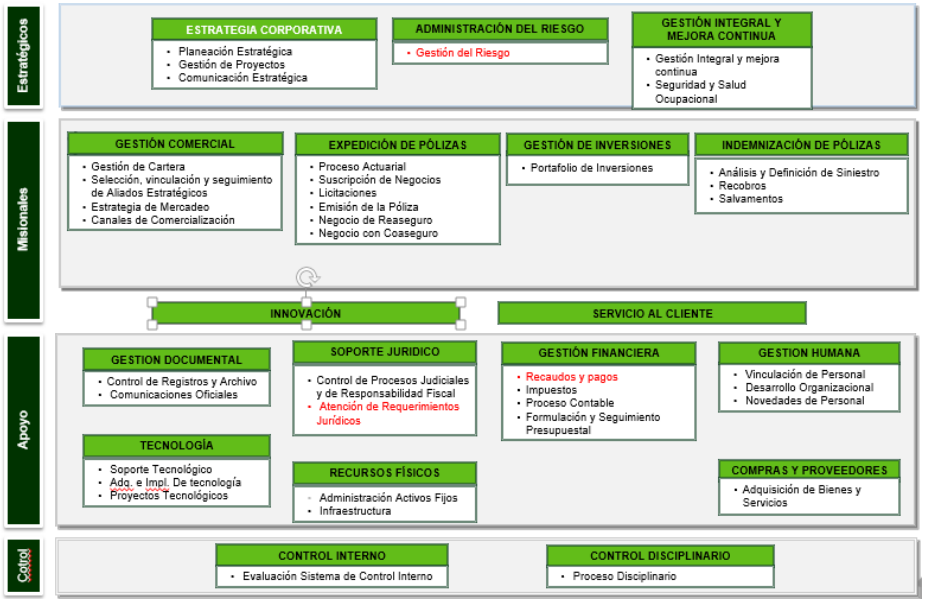

Gráfico 3. Mapa de Procesos

- Estructura organizacional

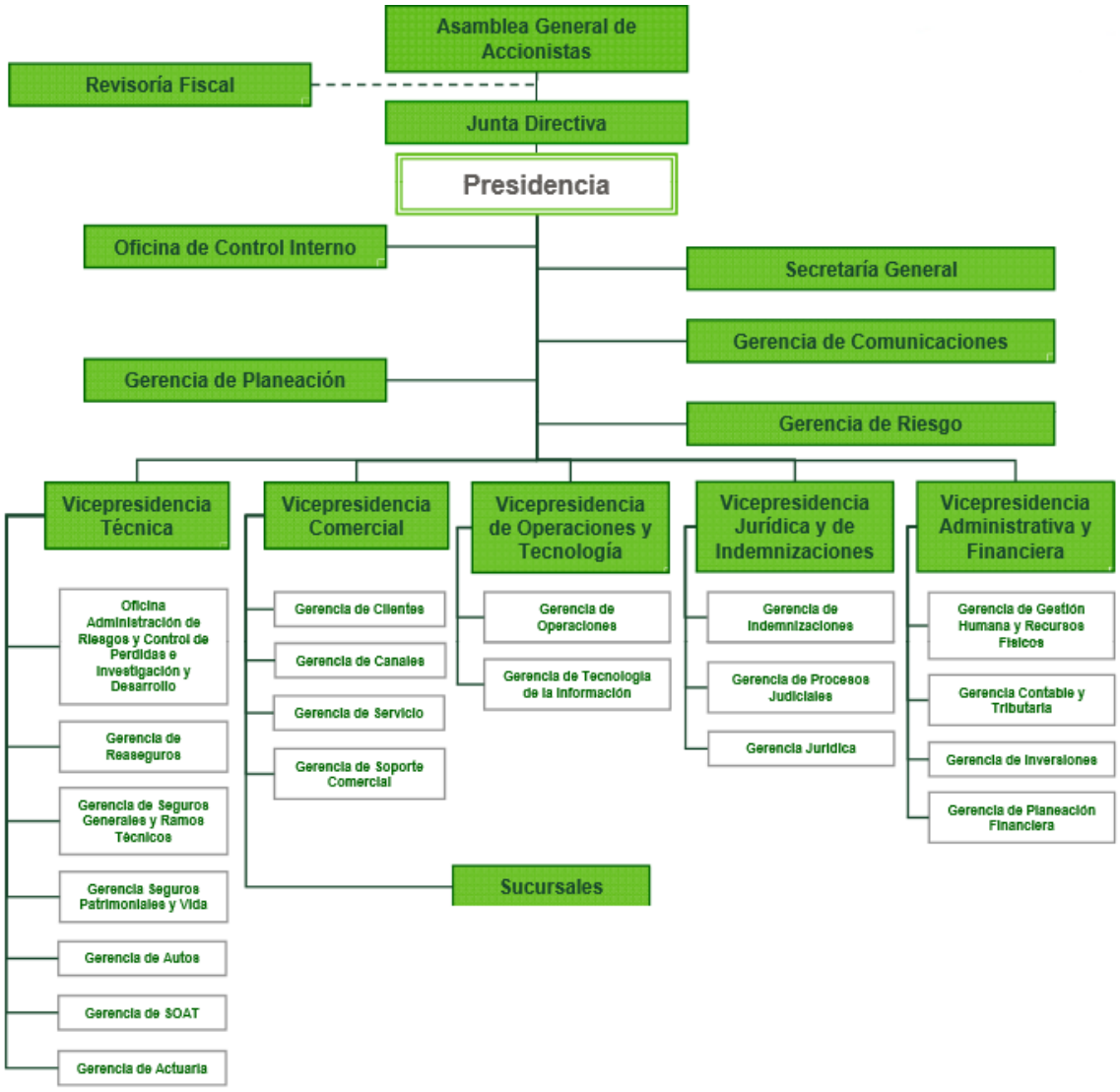

Gráfico 4. Organigrama

- Productos / Servicios

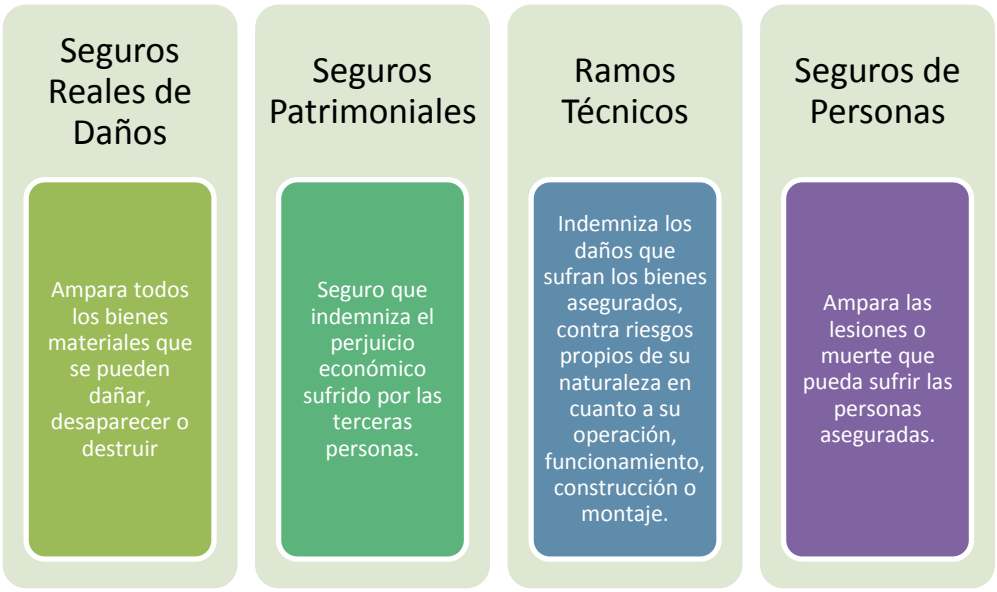

Gráfico 5. Productos y Servicios

8.1.3 BENEFICIOS DE LA GESTIÓN DE IDENTIDADES:

Teniendo en cuenta los objetivos del proyecto, se considera pertinente presentar los beneficios que tiene para las organizaciones, la implementación de una solución de gestión de identidades, dentro de los cuales se resaltan:

Protección de los datos de los usuarios asociados con los recursos de la organización, disminuyendo los riegos relacionados con robo de identidad y cualquier amenaza que afecte de forma directa o indirecta la información.

Si se implementa como una administración centralizada, aumenta la eficiencia disminuyendo riesgos y esfuerzo, ya que se definen procedimientos centralizados de administración, definición de roles, segregación de funciones, entre otros. Reducción de costos al tener unificados los usuarios para el acceso a las aplicaciones, disminuye la carga administrativa de las personas de soporte por cambios de contraseñas, desbloqueo, creación y eliminación de cuentas por aplicación. Esto se traduce en un incremento de la productividad.

Una solución de Gestión de Identidades puede implicar mejoras para el usuario final así como escalabilidad y flexibilidad para la organización.

De acuerdo al tipo de organización, implementar una solución de Gestión de Identidades aporta al cumplimiento regulatorio que le pueda ser aplicable.

Casos de Éxito

Los casos de éxito constituyen un insumo fundamental en el desarrollo del presente proyecto, ya que contribuyen para la evaluación y contextualización de los datos que se tienen acerca de la definición y la importancia de la gestión de identidades.

En un reciente artículo publicado por Bancolombia[2] se presentan algunos casos de éxito de la gestión de identidades a nivel latinoamericano; varias empresas en su necesidad de mitigar algunas de sus necesidades tecnológicas han invertido tiempo y capital en soluciones de gestión de identidades y control de acceso obteniendo buenos resultados, mejorando la calidad y minimizando la administración de los procesos de recepción de control de acceso, lo que conlleva a una notable reducción de costos a nivel de administración de identidades.

→ Sector financiero: DAVIVIENDA

Esta entidad bancaria con el fin de sopesar varias de sus necesidades tecnológicas implementó una solución de Identity and Access Management y de esta manera logró cumplir con los siguientes aspectos:

- Integrar las aplicaciones en una sola y única plataforma, de esta manera los empleados de la entidad bancaria podrían acceder a los diferentes aplicativos de manera rápida y segura.
- Asegurar el cumplimiento de sus políticas de seguridad
- Mejorar la administración de la gestión de identidades, tanto de los empleados como de los clientes
- Reducción de la carga de trabajo en el área de gestión de identidades a un 60%.
- Autoservicio a los usuarios.

[2]Artículo publicado por Bancolombia Gestión de identidades y control de acceso desde una perspectiva organizacional. http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf

→ Sector pensiones y cesantías: ING

Con la implementación de una solución de Gestión de identidades ING mejoró el aprovisionamiento de usuarios facilitando la gestión de identidades de los usuarios, mejorando la operación de las autorizaciones de las personas para acceder a los activos de información, simplificando procedimientos de acceso y mejorando las actividades de gobierno de seguridad y cumplimiento regulatorio. [2]

→ Sector comunicaciones: CLARO

Con el fin de reducir la carga operativa que generaban los clientes Claro decidió contratar una solución de Identidades IAM, realizaron una prueba de concepto y evaluaron casos de implementación exitosa en el sector. El manejo de identidades está siendo automatizado por medio de la solución de IAM, de esta manera mejora la eficiencia de los procesos. (Bancolombia, 2012)

8.1.4 PROCEDIMIENTOS ACTUALES PARA LA GESTIÓN DE ACCESOS Y CONTROL DE IDENTIDADES

Luego de conocer la actividad económica y operacional de la organización de manera general, a continuación se describen los procesos a nivel de control de accesos a las herramientas de la compañía:

La empresa cuenta con varios aplicativos o herramientas tecnológicas para el desarrollo de las actividades tanto administrativas como propias del negocio. La administración de los accesos que se otorgan a los usuarios de las mismas, es bastante compleja dado que coexisten muchas aplicaciones o sistemas de información, cuya operación es independiente. La anterior situación conlleva a que se presenten brechas de seguridad asociadas a situaciones tales como que funcionarios que se encuentran en vacaciones, incapacitados o peor aún que ya no estén vinculados a la compañía o que terceros que ya no tengan relación con la misma, continúen con sus accesos a los diferentes sistemas de información habilitados, lo que puede ocasionar la materialización de riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información de la compañía.

A raíz de lo anterior, se evidenciaron algunas debilidades, en relación con las personas que intervienen directamente en este proceso:

- Directivos
  - No conocen sus responsabilidades frente a la autorización de accesos a los usuarios a los diferentes aplicativos tecnológicos.
  - No han establecido políticas claras respecto a la administración de usuarios de servicios tecnológicos.
  - No han destinado recursos que garanticen una eficiente gestión de usuarios de servicios tecnológicos.
  - No reportan las novedades de terceros (retiros, modificaciones de perfil, etc.), en su debida oportunidad

- Funcionarios y terceros
  - Prestan o piden prestadas las contraseñas de acceso a los aplicativos tecnológicos.
  - Podrían tener acumulación de permisos de acceso
  - No pueden acceder a los aplicativos tecnológicos en la oportunidad requerida

- Gerencia de Gestión Humana
  - No están definidos en los perfiles de cargo, los aplicativos, roles y perfiles a los que deben tener acceso los funcionarios, de acuerdo a su cargo.
  - No reportan en la debida oportunidad las novedades de nómina, debido a que consideran que es una carga adicional de trabajo
  - Desconocimiento de su responsabilidad frente al reporte de novedades de nómina a la mesa de servicio.

- Gerencia de Canales
  - No reportan las novedades de los Aliados Estratégicos en su debida oportunidad
  - Aliados estratégicos
  - No son conscientes de sus responsabilidades frente al uso de los aplicativos tecnológicos a los que tienen acceso.

- Mesa de Servicio
  - Se demora mucho en el proceso de asignación o retiro de accesos a los aplicativos
  - Puede asignar erradamente a los usuarios, los accesos a los aplicativos tecnológicos.

Adicionalmente se encontró que no se cuenta con políticas y procedimientos formalizados, que regulen la gestión de accesos e identidades, dificultando la correcta administración de los mismos, exponiendo a la compañía a una gran variedad de riesgos de seguridad de la información.

De manera general se tienen definidos los siguientes lineamientos:

- Nivel de Permisos y Asignación de Usuarios.

Identificación de usuarios de servicios informáticos: Los usuarios se identifican a través de cuentas de usuario con las cuales también se autentican los mismos. Las cuentas de usuario se componen de nombre de usuario, contraseña e información de control de acceso.

- Nombre de usuario: El nombre de usuario es el mecanismo esencial para su identificación, por lo cual debe ser único y diferente al de los demás usuarios del sistema.

  En caso de presentarse una colisión de usuarios, es decir, que el convenio de nombre sea igual para dos usuarios, se complementará el nombre de usuario en colisión con números en secuencia (fperez, fperez1, perez2, etc.).

- Contraseñas: El uso de contraseñas se establece para que se demuestre que el usuario es quien dice ser, es decir sirve para probar la autenticidad de la persona que dice ser el usuario con ese nombre de usuario. La efectividad de un esquema basado en contraseñas recae en gran parte sobre varios aspectos de la contraseña como su confidencialidad, la resistencia de ser adivinada y la resistencia ante un ataque de fuerza bruta, por lo cual la política de contraseñas de la organización debe contemplar que las mismas sean robustas para garantizar que se cumpla con su objetivo. En la organización no se tienen definidos lineamientos específicos respecto al establecimiento de contraseñas.

- Información de control de acceso: Esta información toma formas diferentes dependiendo del aplicativo, las cuales pueden incluir identificación específica al usuario o al grupo global del sistema, lista de los grupos/capacidades adicionales a los cuales el usuario es miembro, información de acceso por defecto a aplicar para todos los archivos y recursos creados por el usuario.

- Autenticación de usuarios

La autenticación de usuarios es la validación de la identidad de un usuario. Para el ingreso al servicio de red la autenticación del usuario se efectúa frente al directorio activo, el cual contiene las credenciales del usuario y puede confirmar que el usuario las envió correctamente. Para el ingreso a los aplicativos, de acuerdo con el rol asignado, se accede con el usuario de red y una contraseña.

- Autorización de usuarios

Los privilegios y accesos para el uso de los recursos se efectúan conforme al rol de cada uno de los usuarios, determinado por los jefes inmediatos.

Es preciso aclarar que cada uno de los aplicativos o recursos, también tienen definidos diferentes accesos determinados por perfiles que debieran ser asignados de acuerdo a los roles segregando los niveles de operación, revisión y aprobación, no obstante, no se tiene especificada una matriz de roles y perfiles en la que se pueda validar esta información.

- Ingreso o salida de funcionarios por termino de labores.

Se tiene establecido, aunque de manera informal, un protocolo para el ingreso y baja de los funcionarios dentro de los sistemas así como para otorgar o eliminar los permisos sobre las aplicaciones según el cargo a desempeñar, no obstante al no ser un procedimiento formalizado, se evidencian grandes deficiencias y falta de control en la gestión.

8.2 POLÍTICA DE CONTROL DE ACCESOS Y GESTIÓN DE IDENTIDADES

Una política es una declaración de alto nivel que describe la posición de la compañía respecto a un tema específico, por lo cual con establecimiento la política de gestión de identidades se pretende dar los lineamientos de quién, qué, por qué, cuándo y cómo se deberán desarrollar las actividades necesarias para la implementación de un sistema de gestión de identidades.

Es así como, teniendo en cuenta el diagnóstico efectuado y las necesidades evidenciadas en torno al tema de gestión de identidades, se debe diseñar y establecer una política que esté alineada con la forma en que funciona la compañía, sus objetivos institucionales y los del proceso, para que sea aprobada por la alta dirección. Esta política enmarca los principios y lineamientos que guiarán las

actividades para desarrollar un proceso efectivo y eficiente de gestión de identidades.

La política, detallada en el Anexo1, fue diseñada con base en las mejores prácticas del mercado y en los requisitos establecidos en la norma ISO:27001 y su anexo A, con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de la información cuando ello se requiera.

Ahora bien, para implementar y operativizar la política se establecen algunos procedimientos, los cuales hacen parte del presente proyecto y se encuentran descritos en el Anexo 2.

8.3 ESQUEMA PARA LA GESTION Y CICLO DE VIDA DE LAS IDENTIDADES.

Este entregable consiste en un modelo para gestionar de forma óptima el ciclo de vida de las identidades de los usuarios en la compañía, desde la creación hasta su baja, pasando por bloqueo, desbloqueo, activación, inactivación, asignación y derogación de roles, teniendo en cuenta el mantenimiento de la información general como: cargo, ubicación y la identificación respectiva dentro de la organización.

Para la construcción del esquema se hizo necesario establecer un análisis gap enfatizando en los controles A.9.2 y A.9.4 del anexo A de la norma ISO 27001 para evaluar, verificar y diseñar el plan de mejora, así como la identificación de los riesgos a los que está expuesta la organización. Esto se realizó mediante auditoria dentro de las instalaciones, con participación del personal involucrado con el proceso, verificación de logs y muestreo de casos, entre otros.

Partiendo del resultado de este análisis y del diagnóstico de la organización se definieron los lineamientos sobre los permisos, asignación, autenticación, autorización de usuarios, ingreso o salida de funcionarios por término o cambio de labores.

En desarrollo de la auditoria se evidenció la existencia de algunos procedimientos documentados que no se cumplen, dado que no son aplicables o a que están obsoletos, así como controles que no se usan, lo que puede conllevar a situaciones de fuga o pérdida de información, por ejemplo.

Como resultado de lo mencionado, es de vital importancia gestionar el ciclo de vida de las identidades para la compañía de seguros, una vez se han definido las

políticas y procedimientos que incluyen desde la creación de la identidad hasta su dada de baja, pasando por bloqueo, desbloqueo, activación, inactivación, asignación y derogación de roles, teniendo en cuenta el mantenimiento de la información general como: cargo, ubicación y la identificación respectiva dentro de la compañía.

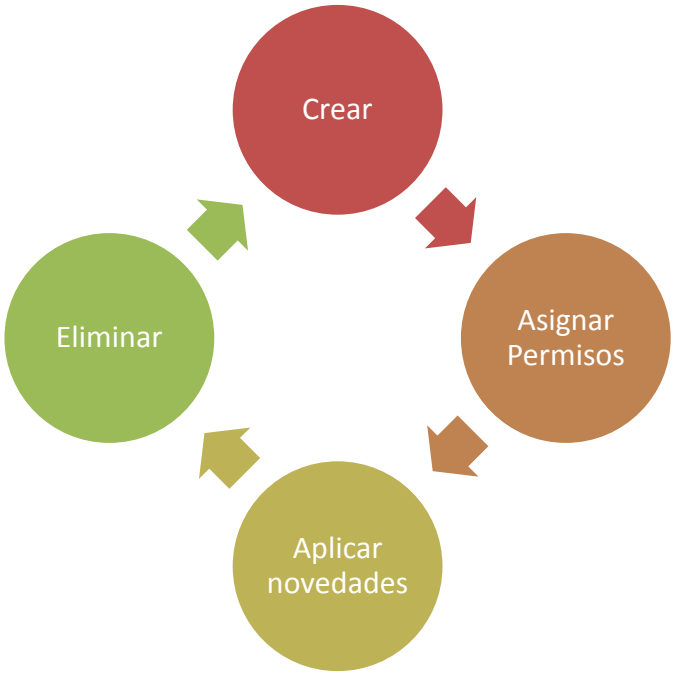

Gráfico 6. Ciclo de Vida de la Identidad

- Creación

Cuando una nueva persona ingresa a la entidad, normalmente se le da acceso a varios recursos (dependiendo de sus responsabilidades). La gestión se realiza de la siguiente manera:

La Gerencia de Gestión Humana debe notificar a la Mesa de Servicio el ingreso del nuevo funcionario para la creación del usuario de red.

- Asignación de Permisos

Cuando ingresa un funcionario nuevo a la compañía, el área de gestión humana notifica al supervisor de la nueva persona acerca de sus funciones y a su vez éste se encarga de radicar el requerimiento con la mesa de servicio para que se otorguen los permisos y accesos de acuerdo al cargo que desempeñará y las políticas de la compañía en cuanto al cumplimiento por parte del usuario sobre las directrices de seguridad de la información que se tienen establecidas.

- Aplicación de novedades

Es normal que dentro de la compañía se presenten cambios ya sea por terminación de contrato, modificación de funciones, incapacidades, licencias, entre otros. Por lo anterior, el área de gestión humana debe notificar dichos cambios a la mesa de ayuda y al jefe de área, con el fin de revocar o modificar los permisos asignados sobre los servicios y/o aplicaciones y que de manera oportuna se gestionen estas solicitudes. También se pueden presentar otro tipo de modificaciones que deben darse a tiempo tales como copias de respaldo en caso de terminación de labores repentina, accesos temporales a usuarios que no pertenecen a la compañía y los cuales se encuentran como prestación de servicios a un término definido, o solicitudes directas de los usuarios por temas de contraseña o inhabilitación de usuarios por un uso no regular.

- Eliminación

Cuando un funcionario termine sus labores dentro de la empresa se deben revocar los permisos de manera inmediata. Para cumplir con este punto a cabalidad, es importante que el jefe de área reporte al área de gestión humana antes de la terminación del contrato con el fin de tener el tiempo suficiente de solicitar a la mesa de ayuda la aplicación de los cambios.

- Responsables

Se realiza la descripción de los responsables por cada etapa del ciclo de vida de gestión de identidad, descrita anteriormente:

Ítem	Responsable	Actividad
Creación	Gerencia de Gestión Humana	Notifica el ingreso del nuevo funcionario para la creación de usuario de red
	Mesa de Ayuda	Creación de la cuenta de red.
	Gerencia de Gestión Humana	Notificación de funciones del nuevo funcionario
Asignación de Permisos	Jefe de Área	Realiza solicitud de asignación de permisos (roles) para el acceso a los recursos que se requiere para el cumplimiento de las funciones a realizar.
	Mesa de ayuda	Asignación de permisos
	Gerencia de Gestión Humana	Notifica novedades de licencias, permisos, vacaciones, retiros, etc.
Aplicar Novedades	Mesa de ayuda	Aplica las novedades según solicitud de la Gerencia de Recursos Humanos con el formato requerido y aprobación del jefe de área

Tabla 3. Responsables del Ciclo de Vida de la Identidad

8.4 PROGRAMA DE CAPACITACIÓN Y SENSIBILIZACIÓN A LOS USUARIOS FINALES

Este programa de capacitación y sensibilización consiste en documentar a los usuarios finales respecto a las responsabilidades frente a la autogestión y a la auto-administración de accesos, acorde con las políticas y procedimientos diseñados, con el fin de fomentar las competencias de los usuarios sobre este particular. Es entonces de vital importancia capacitarlos y acogerlos para hacerlos parte del proceso de implementación de la gestión de identidades, así como del cumplimiento de las políticas y procedimientos descritos y definidos en la organización, considerando que todos los usuarios deben conocer las responsabilidades que tienen frente a la adecuada utilización de las aplicaciones, accesos y herramientas que les brinda la compañía para su labor diaria.

Los lineamientos que se definieron para que hagan parte del programa de sensibilización y entrenamiento básicamente consisten en:

- Comunicación y publicación a los empleados de las políticas establecidas al interior de la organización por medio de la intranet para conocimiento general.

- Envío de boletines mensuales vía correo electrónico institucional, con la información requerida para conocer cómo se debe cuidar y garantizar la seguridad de la información desde la labor ejecutada en cada uno de los cargos.

  Estos boletines se elaboraron con un lenguaje de fácil comprensión y con las recomendaciones más importantes, sobre los temas que se identificaron eran los que se presentaban de manera recurrente entre los funcionarios. Para esto se generó un estudio sobre las prácticas y tendencias que se presentaban en la operación diaria y se aplicaron encuestas para determinar el nivel de conocimiento que tiene cada funcionario frente a los compromisos en términos de seguridad de la información.

  Ejemplos: Articulo Escritorios limpios, responsabilidad de todos; Articulo Prestamos de usuarios y claves; Articulo Uso seguro del correo institucional. Ver Anexo 3, Anexo 4 y Anexo 5 respectivamente.

- Con el ideal de crear conciencia entre todas las personas que interactúan con la organización se colocaron home screen (papel tapiz) del computador con recomendaciones e impulso de la campaña de seguridad, de esta manera se aporta al proceso de capacitación y divulgación de tips sobre las buenas prácticas. Estos solo pueden ser actualizados por el administrador de la mesa de ayuda según autorización previa. Ver Anexo 6.

- Implementación de la semana se la seguridad donde se realizarán eventos que permitan a las personas conocer, entender y motivarlos a hacer parte de la seguridad y cuidados de la información. Esta semana se desarrolla programando diferentes actividades y en diversos horarios para que todos los funcionarios puedan involucrarse y conocer los temas tratados. Las actividades promueven la participación, son llamativas y su contenido es explícito para facilitar su entendimiento.

  El cronograma de actividades así como su horario se indican específicamente. Ver Anexo 7.

9. CONCLUSIONES

El diagnóstico de las necesidades de la organización en torno a la gestión de identidades y su contexto, fue de vital importancia como insumo para obtener el panorama actual de la compañía, establecer los procedimientos y controles a implementar.

Se evidenciaron las falencias en el manejo de la gestión de identidades dentro de la compañía.

La definición del ciclo de vida de la identidad ajustado a la organización, permitió evidenciar los mecanismos para reducir los accesos no autorizados que puedan comprometer la información relevante del negocio.

Se definieron políticas, procedimientos y controles para la gestión y control de usuarios y accesos con base en el diagnóstico realizado, con el fin de lograr la gestión exitosa de accesos e identidades así la administración de los mismos, mitigando los riesgos de seguridad de la información.

Se establecieron los lineamientos y recomendaciones para generar el plan de sensibilización y entrenamiento, dirigido a los usuarios finales buscando hacerlos parte del proceso de implementación de la gestión de identidades y de la seguridad de la información.

En el desarrollo del proyecto se apropiaron los conceptos y conocimientos de gestión de identidad y seguridad de la información, adquiridos en el proceso de formación, en un ámbito práctico aplicado a una compañía de seguros.

10. BIBLIOGRAFIA

Alonso, E. Á. (07 de 2012). *INTECO.* España: Creative Commons. Recuperado el 04 de 05 de 2017

Bancolombia. (2012). GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESO DESDE UNA. *USMMed, 3*(1).

BSI Group. (15 de 05 de 2017). *BSI Group*. Obtenido de https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/

Harris, S. (2011). CISSP All-in-One Exam Guide,. Fifth Edition. En *CISSP All-in-One Exam Guide,. Fifth Edition* (pág. Chapter 4: Access Control). New York: McGraw Hill Professional.

ISO. (s.f.). *ISO*. Recuperado el 09 de 05 de 2017, de https://www.iso.org/isoiec-27001-information-security.html

Jose Quintero. (06 de 10 de 2011). *ISACA.* Recuperado el 08 de 05 de 2017, de web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf

Karla Evita Castro Velarde, J. d. (2010). *Universidad San Martin de Porres.* Recuperado el 10 de 05 de 2017, de www.repositorioacademico.usmp.edu.pe/bitstream/usmp/331/1/castro_ke.pdf

Microsoft. (s.f.). Recuperado el 04 de 05 de 2017, de https://www.microsoft.com/es-es/cloud-platform/identity-management

Oracle. (2008). *Introducción a Oracle Identity Management.* Recuperado el 14 de 05 de 2017, de http://www.oracle.com/corporate/analyst/reports/infrastructure/index.html.

Security, H. (07 de 2013). *CSRC.* Recuperado el 12 de 05 de 2017, de http://csrc.nist.gov/projects/abac/july2013_workshop/july2013_abac_workshop_ksmith.pdf

SOCIAL, C. N. (2016). *POLITICA NACIONAL DE SEGURIDAD DIGITAL.* Bogota.

techtarget. (06 de 2016). Recuperado el 02 de 05 de 2017, de http://searchdatacenter.techtarget.com/es/definicion/IAM-o-Sistema-de-gestion-de-accesos-e-identidades