DISEÑO DE UN MODELO CENTRALIZADO QUE PERMITA EL USO DE IDENTIDADES DENTRO DE UNA ORGANIZACIÓN

ALVARO WILSON ORTIZ ARIAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ.D.C.
2016

DISEÑO DE UN MODELO CENTRALIZADO QUE PERMITA EL USO DE IDENTIDADES DENTRO DE UNA ORGANIZACIÓN

ALVARO WILSON ORTIZ ARIAS

Monografía de grado para optar el título de
Especialista en Seguridad Informática

Esp. Ing. Freddy Enrique Acosta
Asesor de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA, D.C.
2016

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, D.C. 16 de diciembre de 2016

DEDICATORIA

A Dios, fuente de luz y sabiduría que me ilumina en mis intereses de formación integral como ser humano y en la búsqueda de la verdad.

A todos mis familiares por su apoyo incondicional en mis propósitos de superación personal y profesional

ALVARO WILSON ORTIZ ARIAS

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

La Universidad Nacional Abierta y a Distancia- UNAD, por la oportunidad que me brindó para cursar y culminar estudios en el área de mi interés

Al Ingeniero Freddy Enrique Acosta por su permanente asesoría en los procesos de desarrollo de esta monografía y por su paciencia en corregir oportunamente sus contenidos y metodología para que se ajustaran a la rigurosidad científica y técnica exigida por la Universidad.

Al licenciado Jorge Rojas por el interés mostrado por mi trabajo y las sugerencias recibidas, a doña Mary por su valiosa colaboración en la digitación de este documento.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Autenticación: Proceso por el cual el sistema constata, a través de algún mecanismo, que el usuario es quien dice ser. Existen muchos métodos diferentes de autenticación esencialmente basados en tres aspectos: lo que se conoce, lo que se tiene o lo que se es[1].

Autorización (Control de acceso): este proceso tiene como objetivo la protección de los recursos computacionales de accesos que no estén autorizados. En este proceso se lleva el control de acceso a los recursos y sistemas informáticos.

Capa de presentación: también denominada "capa de usuario", es la que el sistema le presenta al usuario, a través de ella se muestra y captura la información del usuario en un mínimo de proceso, previamente realizando un filtrado para comprobar que no hay errores de formato.

Control de acceso basado en roles (RBAC): se basa en la idea de que a los usuarios se les otorga el permiso de acceso a los recursos basado en los roles que posee dentro de la organización. En este escenario se identifican dos tipos de roles: (1) Roles de negocio, que determinan el lugar del usuario dentro de la jerarquía organizacional y (2) Roles de aplicación, definidos en el ámbito de las aplicaciones y sistemas empresariales y que permite la asociación de permisos sobre los recursos[2]

Decisión del control de acceso: la parte central de control de acceso a la información es determinar los recursos a los cuales una identidad tiene autorización de acceso[3]. La decisión es basada en una política de seguridad cuya elaboración debe ser previa a este proceso.

Gestión de identidades: La gestión de identidades y control de acceso por sus siglas en inglés IAM, es un término que se puede entender como el conjunto de procesos de negocio, tecnologías, infraestructura y políticas que permite realizar la gestión de las identidades de usuario y controlar el acceso de éstas a los diferentes recursos organizacionales[4]

---

[1] PALAZÓN R. Antoni, FELGUERA Jordi y CASTELLÀ Jordi. Single sign-on y federación de identidades. Cataluña UOC 2008,P.11

[2] MONTOYA S., José RESTREPO, Zuleima Gestión de identidades y control de acceso desde una perspectiva organizacional. USBMed, Vol. 3, No. 1, pp. 23-34. 2012

[3] IAM: Administración de identidades de acceso (Identify and Access Management)

[4] MONTOYA S., José RESTREPO, Zuleima Gestión de identidades y control de acceso desde una perspectiva organizacional. USBMed, Vol. 3, No. 1, pp. 23-34. 2012

Kerberos: arquitectura cliente-servidor que proporciona seguridad a las transacciones en las redes. El servicio ofrece una sólida autenticación de usuario y también integridad y privacidad. La autenticación garantiza que las identidades del remitente y del destinatario de las transacciones de la red sean verdaderas[5]

Realización del control de acceso: sistema centralizado para la gestión de control de acceso. Este modelo está relacionado con una solución que permite la distribución de permisos a todas las aplicaciones y sistemas.

Seguridad informática: Consiste en asegurar en que los recursos del sistema de información de una organización se utilizan de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización[6]

Sistema de información. Un Sistema de Información es el Conjunto total de procedimientos, operaciones, funciones y difusión de datos o información en una organización. Las tres partes fundamentales de un sistema de procesamiento electrónico de datos son el sistema de computación, el sistema de numeración y el sistema Operativo[7].

Servicio de directorios: un servicio de directorios es un componente de la red que permite que un directorio sea administrado de forma central y al mismo tiempo provee información para las aplicaciones organizacionales que interactúen con éste.

Sistema de gestión de identidades: es aquel sistema que busca unificar en un solo repositorio (centralizado o distribuido) todas las identidades de los usuarios de una organización[8].

---

[5] ORACLE. Guía de administración del sistema: servicios de seguridad. México. 2011. Disponible en Internet: https://docs.oracle.com/cd/E24842_01/html/E23286/intro-5.html

[6] https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

[7] http://fccea.unicauca.edu.co/old/siconceptosbasicos.htm

[8] JUMMP. Desarrollo de software. Sistema de gestión de identidades [En línea]. Mayo 2011. [Consultado sep. 21 de 2015]. Disponible en https://jummp.wordpress.com/2011/05/04/desarrollo-de-software-sistema-de-gestion-de-identidades/

RESUMEN

El avance en las tecnologías de información y la gran cantidad de aplicaciones a los que tienen acceso las personas, hace necesario que las organizaciones cuenten con un modelo que permita gestionar los usuarios que acceden a ellas.

Este trabajo está orientado a la presentación de un modelo que permita la gestión de usuarios de manera centralizada sobre los diferentes sistemas de información; y es aplicable a cualquier organización sin importar su tamaño. Cubre aspectos relevantes como un procedimiento, un manual de administración y políticas de administración de usuarios, la recomendación para adquirir una herramienta automatizada que permita la gestión de usuarios. Se detalla en cada uno de estos objetivos los pasos a seguir, las políticas, la operación, los deberes, los derechos, y en general todo aquello que esté vinculado con la gestión integral de usuarios.

Se hace énfasis a temas como manejo de contraseñas de usuario, el cuidado que se debe tener con ellas, y se cubre todos los tipos de usuarios existentes en los sistemas de información, desde el usuario final hasta el administrador del mismo.

Este documento se basó en experiencias vividas, así como en las metodologías propuestas en las normas, como son la ISO 27001, buenas prácticas sobre ITIL para la prestación de servicio de gestión de usuarios, extrayendo de cada una de ellas lo más relevante para armar el modelo propuesto.

Por último, se presenta el diseño de un modelo en un sistema centralizado de manejo de identidades que puede ser aplicado en cualquier tipo de empresa sin importar la cantidad de sistemas que posea, ni de usuarios, ya que lo propuesto puede ser adaptado a los requerimientos organizacionales y operativos de acuerdo con el perfil de los usuarios de la empresa

Palabras Clave: Autenticación, Identidades, control, Gestión, Sistema de gestión de identidades, Kerberos

ABSTRAC

Advances in information technology and the many applications that have access to people, makes it necessary for organizations to have a model to manage users accessing them.

This work is aimed at presenting a model that allows user management centrally on the various information systems; and it is applicable to any organization regardless of size. It covers relevant aspects such as a procedure, a manual management and user management policies, the recommendation to acquire an automated tool that allows user management. Detailed in each of these goals the steps, policies, operation, duties, rights, and in general everything that is linked to the comprehensive management of users.

Emphasis is given to issues such as managing user passwords, care must be taken with them, and all types of users in information systems is covered, from the end user to the administrator.

This document was based on experiences, as well as the methodologies proposed in the standards, such as ISO 27001, best practices ITIL for service delivery user management, drawing from each the most relevant to arm the proposed model.

Finally the design of a model of a centralized identity management that can be applied to any type of company is presented regardless of the number of systems you have, or users, as proposed can be adapted to organizational requirements and operating according to the profile of users of the company

Keywords: Authentication, Identities, control, management, Identity Management System, Kerberos

INTRODUCCIÓN

La dinámica de los avances tecnológicos, requiere que se dispongan de sistemas de informáticos permanentemente actualizados que a tiempo que facilitan la interconexión de las organizaciones y de sus usuarios, permiten el acceso a aquellos datos que sean de interés para la consolidación y permanencia de las empresas en el mercado con competitividad y eficiencia. Para ello, se demanda que posean estructuras informáticas de fácil y oportuno acceso para los usuarios que estén debidamente acreditados lo cual requiere que a la vez se tenga de ellos una permanente actualización y seguro mantenimiento de sus identidades.

Frente a estos retos, se hace necesario la creación u obtención de un sistema centralizado de identidades que permita mantener actualizada el ciclo de permanencia de las identidades adscrita a la organización. Esto facilitará mantener un control de acceso a la información de manera confiable y segura evitando riesgos que afecten sensiblemente no sólo la imagen y estabilidad empresarial sino también la seguridad que se tenga sobre el desarrollo de los procesos que atañen solamente a la organización.

Estas condiciones son las que constituyen las dimensiones que debe presentar el sistema de seguridad informática: “la disponibilidad, la integridad y la confidencialidad”[9]

En cuanto a la disponibilidad, se hace necesario que se pueda tener acceso a la información de manera fácil y oportuna evitando procesamientos complejos que muchas veces ocasionan tergiversación de la misma información.

La integridad, con que se administren los sistemas informáticos, ayudará a que se cometan fraudes perjudiciales para los usuarios y para la misma organización.

La confidencialidad ayudará a darle seguridad a las identidades de los usuarios cuyas direcciones estén debidamente autenticadas y autorizadas.

Uno de los aspectos más relevantes de este trabajo monográfico es el presentar un modelo de sistema centralizado para el manejo de identidades que no estará asociado a ninguna herramienta de administración de usuarios de una marca comercial específica; ya que la empresa puede inclinarse en el desarrollo de su propio aplicativo con software libre, siendo un software propietario que no generaría pago de licenciamientos, obligatorio en el software comercial.

[9] REFUGIO, J. y VILLALOBOS, B. Jefatura de Tecnología de Información en Consorcio Minero Benito Juárez Peña Colorada, México, 2004, p.13

1 DEFINICIÓN DEL PROBLEMA

1.1 PLANTEMAMIENTO DEL PROBLEMA

Un gran número de organizaciones, independientemente de su tamaño o sector, requieren de algún tipo de solución para gestionar las identidades. A pesar de ello, la gran mayoría no dispone ni de procedimientos, ni de sistemas que le ayuden a esta importante labor. Siendo los sistemas de gestión de identidad herramientas que existen desde hace muchos años, y habiendo un gran número de ellas en el mercado, nos podemos preguntar por qué se produce la falta de presencia de algo tan necesario[10].

Por otra parte, muchas entidades, públicas y privadas, en efecto, se enfrentan al problema de la proliferación de cuentas de usuario y sus correspondientes contraseñas, fenómeno que deriva de la necesidad, impuesta a veces de forma artificial por muchas aplicaciones y sistemas, de tener que disponer de una cuenta de usuario y una contraseña para cada aplicación y sistema con el que se trabaja. Esta situación resulta difícil de controlar, ya que cada proveedor de la Administración dispone de su propia tecnología, decidiendo si utiliza o no autenticación certificada. Por el contrario, el factor de decisión para la compra del producto ha de ser su funcionalidad y calidad, y no tanto el sistema de autenticación empleado[11].

Sin embargo, cada vez que un usuario requiere un nuevo acceso a un nuevo recurso, una aplicación o conjunto de datos, tiene que acudir a la mesa de servicio e informar a los administradores responsables de cada sistema para que resuelvan la solicitud. Puede darse el caso que los administradores no estén siempre disponibles, porque se han ausentado temporalmente, por ejemplo, por vacaciones, permisos, viajes o por motivos de salud, o porque se han ido de la empresa de manera definitiva, por retiro o por despido para que puedan desactivar el acceso. Esto podría tener consecuencias muy negativas para la empresa, o si el usuario se va a trabajar para la competencia[12].

---

[10] GILARD IGLESIAS, Ignacio. Por qué implantar un sistema de gestión de identidad open source: WBS Visión. En: White Bear Solutions genuinely open (WBSgo). [En línea]. Octubre 2015. [Consultado oct. 15 de 2015]. Disponible en http://www.whitebearsolutions.com/por-que-implantar-un-sistema-de-gestion-de-identidad-open-source-wbsvision/

[11] DOMINGO, Ignacio Alamillo; i Aparisi, Xavier Urios; En: la gestión de identidades y capacidades por las administraciones públicas. [Pág. 3]. Diciembre 2004. Consultado mayo. 30 de 2006]. Disponible en Internet: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Tecnimap/pae_TECNIMAP_2006/pae_TECNIMAP_2006_Comunicaciones_Presentadas_-_5/gestion_de_identidades.pdf

[12] REFUGIO, Javier y VILLALOBOS, Becerra. Jefatura de Tecnología de Información en Consorcio Minero Benito Juárez Peña Colorada, México. 2014.

Todas esas situaciones se traducen en la problemática que se evidencia en muchas empresas al crecer en su infraestructura y soluciones informáticas independientes, se evidencia en el aumento de complejidad de los procesos de administración y gestión de usuarios tanto internos como externos, en el robo de identidades debido a los malos hábitos de los usuarios y al continuo incremento de claves de acceso que una misma persona llega a manejar. Todas estas deficiencias, propician el éxito de quienes buscan realizar actividades ilícitas.

Ahora bien, si se dispone de algún tipo de aplicativo o sistema informático, este muchas veces está diseñado con una estructura que sólo quienes tienen algún nivel de capacitación o de entrenamiento, pueden acceder para obtener la información o suministrar datos que sean de su interés y que les permitan mantener una comunicación fluida y oportuna con las distintas instancias empresariales. Son muchas herramientas a la vez que hacen tal comunicación más dispendiosa y a la postre difícil de acceder o de operar.

1.2 FORMULACIÓN DEL PROBLEMA

¿Será qué un modelo de identidades centralizado, permitirá a una organización reducir la gestión en la administración de usuarios y mitigar los riesgos de accesos no autorizados?

1.3 OBJETIVOS

1.3.1 Objetivo General

Diseñar un modelo que permita el manejo de identidades de usuario dentro de una organización, facilitando el acceso a las diferentes aplicaciones disponibles, y aplicar controles de seguridad con base a la norma ISO 27001:2013 para la generación de las políticas de seguridad para el manejo de identidades.

1.3.2 Objetivos Específicos

- ✓ Describir el modelo actual de identidades utilizado por las organizaciones para la administración de usuarios, porque debemos partir de lo que existe dentro de las organizaciones.

- ✓ Diseñar el nuevo un modelo que permita el manejo de identidades de usuario dentro de una organización, facilitando el acceso a las diferentes aplicaciones disponibles.

- ✓ Establecer controles de seguridad para el uso de identidades dentro de una organización, basado de la norma ISO 27001:2013.

- ✓ Plantear políticas de seguridad para la utilización de identidades de usuario dentro de una organización.

1.4 JUSTIFICACIÒN

Al contar con un sistema único de identificación el acceso a las plataformas y/o servicios empresariales por parte de los usuarios resultará menos dispendioso, más seguro y ágil a la hora de realizar cualquier operación para acceder a determinado tipo de información. En ese sentido, se tendrá a la vez un mayor control del uso que se haga de la misma. "*Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario*"[13].

Básicamente se trata de pasar de un modelo en que simplemente se gestionan las diferentes identidades de los ciudadanos y empresas, a un modelo en que se gestionan, además, sus diferentes capacidades de actuación.

Conseguir implantar estas tecnologías y métodos en los procedimientos administrativos supondrá una importante simplificación en la tramitación formal, así como una considerable reducción de los documentos que forman el expediente, sin ninguna reducción de las garantías jurídicas, lo que justifica este cambio de paradigma, que supone el paso de la gestión de la identidad a la gestión de las capacidades jurídicas personales[14].

En el mundo actual, de mercados globalizados, las organizaciones necesitan incrementar la agilidad del negocio para el desarrollo de estrategias que les permitan competir de forma eficiente, cumplir con regulaciones y ser flexibles ante el entorno cambiante de regulaciones, normas y leyes; para esto necesitan contar con mecanismos que garanticen la disponibilidad de la información y el acceso seguro a las aplicaciones y recursos a través de múltiples sistemas y permitan el uso de servicios en línea para empleados, clientes, proveedores y socios de negocio[15].

La gestión de identidades con un modelo centralizado, se presenta como una solución que contribuye a la administración de las mismas durante todo el ciclo de permanencia de las identidades y al mismo tiempo ejercer control del acceso a las

[13] Norma ISO 27002: http://iso27000.wik.is/

[14] DOMINGO, Ignacio Alamillo; i Aparisi, Xavier Urios; En: la gestión de identidades y capacidades por las administraciones públicas. Op. Cit. p.7

[15] Montoya S, José A, Restrepo R. Zuleima. Gestión de identidades y control de acceso desde una perspectiva organizacional, Ing. USBMed, Vol. 3, No. 1, Enero-Junio 2012 .Consultado 21-11-2016. Disponible en http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf

distintas áreas, a fin reducir riesgos y costos y de esta forma hacer posible que los negocios se desarrollen de manera ágil y sin mayor complejidad.
Así mismo el modelo centralizado de gestión de identidades permitirá brindarle protección a los usuarios que hagan uso de la información que requieren de la organización con seguridad y evitando que se produzca robo de identidad, propiedad intelectual, amenazas y alteraciones de la información por parte de individuos o grupos de crimen organizado.

1.5 ALCANCES Y LIMITACIONES

1.5.1 Alcance

Esta monografía se encuentra ubicado en la línea de investigación de seguridad de la información y pretende la elaboración de una propuesta para el diseño de un modelo que permita el manejo de identidades de usuario dentro de una organización, facilitando el acceso a las diferentes aplicaciones disponibles, y aplicar controles de seguridad con base a la norma ISO 27001:2013 para la generación de las políticas de seguridad para el manejo de identidades.

1.5.2 Limitaciones

- ✓ No se entregará un documento técnico detallado de configuración.
- ✓ No se tendrá en cuenta asignación de recursos económicos, humanos y de tiempos de ejecución.
- ✓ No abarca el uso de ningún lenguaje de programación, tanto este como la base de datos de repositorio son de libre elección, según las necesidades de la entidad que implemente.
- ✓ La propuesta no será implementada, pero servirá como base para el modelo de identidades.
- ✓ Por confidencialidad no se revelará la razón social donde se elaboró el estudio para el desarrollo de la propuesta.

1.6 DISEÑO METODOLÓGICO

1.6.1 Investigación Descriptiva

Consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la

predicción e identificación de las relaciones que existen entre dos o más variables[16].

En ese sentido, a través de la investigación descriptiva se logran establecer de manera correlacionada, las semejanzas y diferencias que existen entre las opiniones, percepciones, conocimientos y/o experiencias y agrupar la información recolectada. Al respecto, se precisa que "los estudios descriptivos que obtienen datos exactos sobre el estado de las situaciones o identifican las relaciones que existen entre estas últimas e interpretan el significado de la información obtenida; ofrecen al investigador una información de gran valor práctico que puede ser empleada para resolver los diferentes problemas que surgen de la labor cotidiana"[17].

1.6.2 Investigación Proyectiva

La investigación proyectiva se ocupa de cómo deberían ser las cosas, para alcanzar unos fines y funcionar adecuadamente. La investigación proyectiva involucra creación, diseño, elaboración de planes, o de proyectos; sin embargo, no todo proyecto es investigación proyectiva. Para que un proyecto se considere investigación proyectiva, la propuesta debe estar fundamentada en un proceso sistemático de búsqueda e indagación que requiere la descripción, el análisis, la comparación, la explicación y la predicción.

A partir del estadio descriptivo se identifican necesidades y se define el evento a modificar; en los estadios comparativo, analítico y explicativo se identifican los procesos causales que han originado las condiciones actuales del evento a modificar, de modo que una explicación plausible del evento permitirá predecir ciertas circunstancias o consecuencias en caso de que se produzcan determinados cambios; el estadio predictivo permitirá identificar tendencias futuras, probabilidades, posibilidades y limitaciones. En función de esta información, el investigador debe diseñar o crear una propuesta capaz de producir los cambios deseados[18].

Por otra parte, a través de la investigación proyectiva, "se hacen explícitos escenarios alternativos de futuros predecibles (estadio futuro), permite identificar riesgos y oportunidades de ciertas situaciones futuras, Proporciona orientaciones para la acción (estadio proyectivo), y establece criterios de decisión para alcanzar el mejor futuro posible"[19].

---

[16] WIKIPEDIA La Enciclopedia libra. Investigación descriptiva. 2013 Disponible en internet: https://es.wikipedia.org/wiki/Investigaci%C3%B3n_descriptiva.
[17] SABINO, C. (1992).Metodología de la investigación. Bogotá, ed. Panamericana, p. 62.
[18] HURTADO DE BECERRA, J. Metodología de la investigación holística. Caracas Venezuela: Sypal, 2000.
[19] Ibid.p.328

2 MARCO REFERENCIAL

2.1 MARCO TEÓRICO

Las empresas en general, actualmente manejan servicios tales como: administración de servidores, de bases de datos, de redes, de telefonía, de servicios en red. Dicha gestión y herramientas se realiza a través de variedad de aplicaciones en diferentes lenguajes de programación.

Dentro de este contexto, las organizaciones se ven abocadas a enfrentar diversos retos movidas por su interés de lograr competitividad y rentabilidad, lo cual implica el incremento de la agilidad en los procesos de desarrollo empresarial y al mismo tiempo el mejoramiento de la seguridad y la disponibilidad de la infraestructura que los soporta. De ahí que sea necesario tener en cuenta que "el uso de múltiples sistemas, aplicaciones y estándares facilita la proliferación de diversas identidades digitales para clientes, empleados y socios de negocio. La complejidad se hace evidente cuando coexisten diversos repositorios de identidades que operan de forma independiente y con diferentes estándares"[20] . Esto se traduce por consiguiente en mayores costos de administración, inconsistencias en los datos y en la presencia de riesgos que afecten la seguridad de los sistemas, lo cual podría ser subsanado mediante el diseño de un modelo centralizado que permita el uso de identidades dentro de una organización.

Con dicho modelo el centro de servicios, se constituye en punto único de contacto para los usuarios y piedra angular del servicio, es el soporte que permite la comunicación y atención de las solicitudes, incidentes y/o requerimientos. El usuario puede acceder a este centro de servicios mediante los siguientes medios: línea telefónica, o la dirección de correo corporativa. Por esta razón la empresa requería urgentemente el desarrollo de un Sistema Centralizado de Manejo de Identidades, cuyas características y elementos componentes se explican en los siguientes términos:

2.1.1 Sistema centralizado de gestión de identidades.

Consiste en un directorio central de control de inventarios y de usuarios, permitiendo trazar a los usuarios, las aplicaciones, los dispositivos y poder determinar todas las cuentas asociadas a este, ya sean gestionados de forma automática o manual. Este sistema, permite además suministrar y controlar todos los accesos a los sistemas de información requeridos por los usuarios acreditados ante la organización de manera segura; permite también "el aprovisionamiento

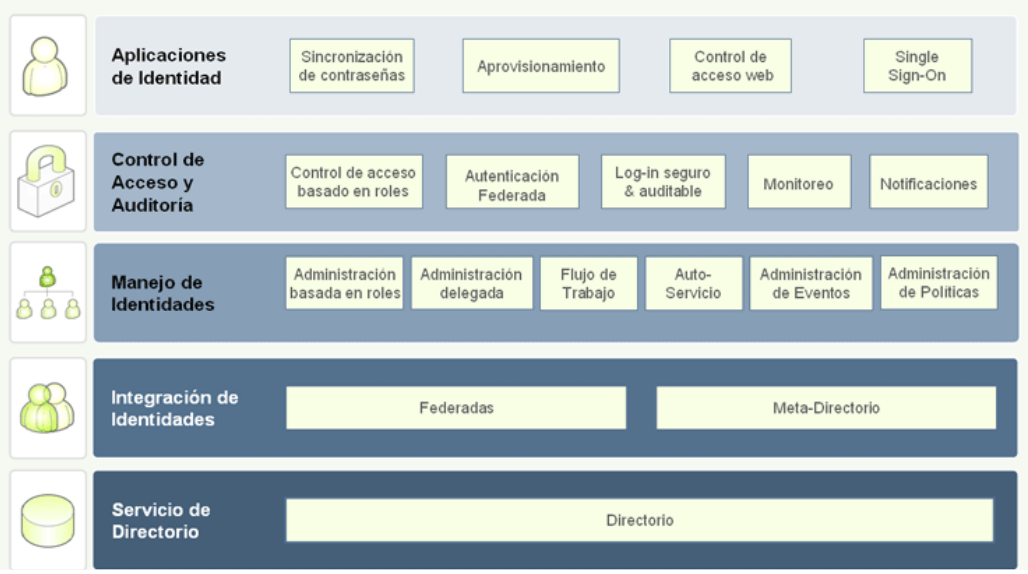
[20] Montoya S, José A, Restrepo R. Zuleima. Gestión de identidades y control de acceso desde una perspectiva organizacional, Ing. USBMed, Vol. 3, No. 1, Enero-Junio 2012 .Consultado 21-11-2016. Disponible en http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf

automático de las cuentas de acceso, ya sea a las aplicaciones, sistemas en general, o bases de datos; y el sincronizar información entre sistemas HRMS o CRMS con un repositorio central, que es manejado por el sistema de gestión de identidades"[21].

El sistema centralizado de gestión de identidades busca también unificar en un solo repositorio (centralizado o distribuido) todas las identidades de los usuarios de una organización[22]. Y está conformado por una parte procedimental y otra parte tecnológica, busca minimizar los errores que se pueden presentar al tener múltiples repositorios de usuarios, por ejemplo, error en la escritura de los nombres, duplicidad de cuentas, multiplicidad de contraseñas, etc.

2.1.2 Áreas funcionales del sistema de gestión de identidades.

Figura 1. Áreas Funcionales de un Sistema de Gestión de Identidades



Fuente Calderón A. 2009, Pág.22

La figura 1, representa las principales áreas comprometidas en un sistema de gestión de identidades relacionadas con aprovisionamiento, la sincronización de contraseñas, el manejo de identidades basado en la gestión de roles y la gestión del directorio.

---

[21] CALDERÓN B. GALO A. Estudio teórico de soluciones a la gestión centralizada de accesos a los sistemas mediante la aplicación de un sistema de gestión de identidades. Quito: Pontificia Universidad Católica del Ecuador. 2009

[22] JUMMP. Desarrollo de software. Sistema de gestión de identidades [En línea]. Mayo 2011. [Consultado sep. 21 de 2015]. Disponible en https://jummp.wordpress.com/2011/05/04/desarrollo-de-software-sistema-de-gestion-de-identidades/

A continuación, se explica brevemente cada una de estas áreas:
Aprovisionamiento y No Aprovisionamiento de Cuentas de Acceso. Esta área en la gestión de identidades, permite la administración actualizada de los usuarios vinculados a la empresa, lo mismo que las cuentas y procedimientos de acceso al sistema de tal suerte que se elimina el acceso a aquellos usuarios que han terminado cualquier tipo de relación con la organización. De ahí que sea necesario que se disponga de un sistema único permanentemente consolidado con los datos, cuentas, permisos de acceso debidamente depurados para evitar accesos que pongan en riesgo la confidencialidad de la empresa.

"La administración y el aprovisionamiento total de identidades permiten la administración centralizada de todas las identidades de usuario y la automatización de la creación, modificación, suspensión o exclusión de cuentas de usuario y derechos en todos los sistemas de TI.[23]

A través del aprovisionamiento se le suministra al usuario un conjunto de recursos dentro de la organización, que pueden ser "una cuenta de correo, un teléfono celular, la activación del acceso a una aplicación o un sistema, la tarjeta de acceso a un edificio, entre otros. En el caso de una aplicación o sistema se realiza la propagación de la identidad del gestor de identidades hacia la aplicación o sistema"[24].

Gestión de Contraseñas. La sincronización de las contraseñas además de permitir la autenticación de la validez de los usuarios acreditados sirve para que estos puedan acceder sin tener contratiempos que les causen demorar o alteraciones de la información deseada. Así, se evitará también la congestión que se puedan generar por el sinnúmero de llamadas telefónicas o de solicitudes de ayudas de apoyo.

Gestión de Roles. Esta gestión es importante ya que permite clasificar de manera selectiva los grupos de usuarios según privilegios específicos de acuerdo con el rol que cumplan o que se les haya asignado en la organización.

"Las herramientas de administración de roles brindan un análisis potente para ayudar a las organizaciones a construir una base eficaz de roles que incluye roles, políticas, derechos de accesos, etc."[25]

---

[23] Transforming IT Management GUIA DE USUARIO: ADMINISTRACION DE IDENTIDADES Y ACCESOS 2007:6. Consultado 21-11-2016. Disponible en http://www.calatam.com/mails/docs/iam_buyers_guide_es.pdf

[24] Montoya S, José A, Restrepo R. Zuleima. Gestión de identidades y control de acceso desde una perspectiva organizacional, Ing. USBMed, Vol. 3, No. 1, Enero-Junio 2012 .Consultado 21-11-2016. Disponible en http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf

[25] Sumner Blount, Merritt Maxim CA Security Management. El rol de la administración de identidades y accesos para lograr un cumplimiento continuo 2012:9. Consultado 22-11-2016. Disponible en http://www.arcserve.com/ar/~/media/Files/whitepapers/latam/CS1933_ContinuanceCompliance_WP_0212_LAS.pdf

Gestión de Solicitudes, Administración Delegada y Autoservicio del directorio. La gestión de solicitudes facilita hacer una administración selectiva delegando responsabilidades según áreas o departamentos de la organización de acuerdo con los requerimientos de los usuarios. De esta forma se garantizará la atención a cada grupo de usuarios según sus necesidades e intereses, respetándoles los derechos que les hayan sido otorgados por parte de la organización. Así, la delegación administrativa facilita un control permanente de accesibilidad a quienes efectivamente tengan tales derechos o cumplan determinados deberes.

El autoservicio son funcionalidades incorporadas dentro de una solución de gestión de identidades y control de acceso, por medio de las cuales los usuarios pueden realizar la autogestión y recuperación de contraseñas y flujos de trabajo que automatizan la creación de solicitudes de recursos requeridos para el desarrollo de sus funciones" [26]

El diseño del modelo debe ser elaborado en una etapa y debe contar con facilidades para que se pueda documentar y explicar la funcionalidad de la solución integral que soporta el proceso de control de acceso.

2.1.3 Control de Acceso al Sistema de manejo de identidades

La gestión del sistema único de manejo de identidades demanda que se defina igualmente un sistema de control de accesibilidad según las delegaciones atribuidas, pudiéndose establecer las siguientes características:

Seguridad AAA. La seguridad triple AAA combina 3 funciones de seguridad, que permiten ejercer el control de los accesos ya sea a los sistemas o dispositivos de red. Este tipo de seguridad significa:

- **Autenticación:** Proceso por el cual, una entidad prueba su identidad ante otra. Normalmente, la entidad es un usuario o computador. Este proceso se obtiene mediante la presentación de una propuesta de identidad (nombre de usuario) y la demostración de estar en posesión de las credenciales de acceso, que permiten comprobarla. "La autenticación es la unión de una identidad a un sujeto"[27]

El proceso de Autenticación es quizás la pieza inicial y fundamental del control de la seguridad de la información. Es en esencia lo que permite indicar que una persona que dice que es. Tiene que ver con la comprobación de los datos o credenciales en los intentos de conexión. Y proceder al envío de una petición

[26] Montoya S, José A, Restrepo R. Zuleima. Op. Cit. p.25
[27] Bishop 2003. Citado por Villalobos B.. Refugio Propuesta de arquitectura de gestión de identidades digitales para el consorcio minero Benito Juárez. Colima 2012,p. 25

cliente-servidor de acceso remoto en forma de texto plano o cifrado. Un método de autenticación impone una barrera de acceso a la información. Un ejemplo común de este método de autenticación es la utilización de un nombre de usuario y una contraseña.

Lo difícil del sistema no es identificar al usuario en sí, sino comprobar que es quien realmente dice ser. Los métodos de autenticación se suelen dividir en tres grandes categorías[28]:

- ✓ Algo que el usuario sabe
- ✓ Algo que el usuario posee
- ✓ Características físicas del usuario (autenticación biométrica)

Para este proyecto se descarta el último método, ya que no procede para el desarrollo del mismo. Sin embargo, los dos primeros serán utilizados activamente por la asociación.

En cuanto al primero, será la autenticación básica y estándar de las aplicaciones ejemplo, una contraseña, una frase o un número de identificación personal. Tanto las webs, como las de escritorio o móvil, necesitan validar los datos del usuario antes de responder a sus peticiones y facilitar los datos.

"Algo que el usuario posee". Por ejemplo, tarjeta de la identificación, símbolo de la seguridad, símbolo del software o teléfono celular). De esta forma, se validan los datos y se da acceso.

Ahora que sabemos lo básico acerca de la autenticación, procedemos a la definición de lo que se busca en este proyecto.

EL Single sign-on (SSO)[29] es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación. Su traducción literal sería algo como «autenticación única» o «validación única».
Existen varios tipos de sistemas SSO, entre estos, Enterprise single sign-on (E-SSO)[30], Autenticación primaria. Intercepta los requerimientos de login que se le presentan por parte de otras aplicaciones para completarlos con las credenciales del usuario.

---

[28] WIKIPEDIA. Autenticación [En línea]. Oct. 2015. [Consultado oct. 21 de 2015]. Disponible en https://es.wikipedia.org/wiki/Autenticaci%C3%B3n

[29] ROUSE, Margareth. Single sign-on (SSO) definition [En línea]. En: TechTarget. 2015. [Consultado oct. 02 de 2015]. Disponible en http://searchsecurity.techtarget.com/definition/single-sign-on

[30] HITACHI ID SYSTEM. Definition of Enterprise Single Sign-On (E-SSO) [En línea]. 2015. [Consultado oct 10 de 2015]. Disponible en: http://hitachi-id.com/concepts/esso.html

Web single sign-on (Web-SSO)[31]: Solamente trabaja con aplicaciones y recursos en la web. A diferencia del E-SSO, los accesos no se interceptan directamente, sino a través de un proxy o un componente en el servidor destino. Utiliza cookies para su funcionamiento.

Kerberos: Uno de los métodos más populares para externalizar la autenticación. Utiliza un sistema de tickets donde el usuario ha de presentarlo a las aplicaciones clientes una vez que el servidor se los asigna[32].

Las principales ventajas de utilizar un sistema SSO son más que evidentes. Por un lado, se minimiza el malestar que puede provocarle al usuario tener diferentes nombres de usuarios y/o contraseñas. Así mismo también se reduce el tiempo que los usuarios pasan introduciendo credenciales en los formularios.

Por supuesto, también tiene desventajas. La principal, es que si el sistema central falla, o es atacado, todas las aplicaciones y datos de usuario de los distintos programas se verán comprometidos

- **Autorización (Control de acceso):** Son los privilegios de accesibilidad que se les otorga a los usuarios de acuerdo con la autenticación hecha de su identidad. Además de la autorización para acceder al sistema se establecen las restricciones que ayudan a mantener un control en cuanto a horarios, lugares u otros limitantes que puedan distorsionar o en algún momento bloquear el sistema como puede ser el caso de un usuario que realice o solicite múltiples ingresos a la vez.

La autorización tiene como objetivo la protección de los recursos computacionales de accesos que no estén autorizados. En este proceso se lleva el control de acceso a los recursos y sistemas informáticos según el flujo de trabajo que corresponda. Lo anterior se realiza en base a políticas de seguridad por lo cual solo se permite el acceso según las autorizaciones asignadas a cada usuario a través de una petición y una aprobación por parte del dueño del proceso. Tiene que ver con la comprobación de aceptación de la conexión. La autorización ocurre después de que el usuario se haya autenticado.

La aplicación para solicitud de autorización de cuentas y permisos de todos los sistemas donde se manejen usuarios y los requerimientos adicionales, debe permitir la ejecución directa sobre los repositorios de usuarios, de las diferentes aplicaciones que cuenten con una conexión, además permitir registrar lo que se haga manualmente en los sistemas no conectados.

---

[31] PAPERCUT SOFTWARE INTERNATIONAL PTY LTD. Web Browser Single Sign-on (SSO) [En línea]. 2015. [Consultado oct 15 de 2015]. Disponible en http://www.papercut.com/products/ng/manual/ch-sso.html

[32] MARRERO RODRÍGUEZ, Raúl. Sistema centralizado de gestión de usuarios para Innova 7. La Laguna, 2014, p. 4. Trabajo de Grado. (Ingeniería Informática). Universidad de La Laguna. Departamento de Ingeniería Informática.

La Bodega de Identidades BI debe ser el repositorio central de usuarios, donde deben converger todas las cuentas y permisos que tenga un usuario en los sistemas de la organización. Ya sea que la aplicación esté gestionada directamente desde la herramienta central, o aplicaciones y sistemas gestionados manualmente por los administradores. Se requiere que las solicitudes de cuentas y permisos se realicen vía web, mediante el formulario de solicitudes. Se debe tener en cuenta que los sistemas o aplicaciones son los más críticos para la organización y se les debe dar prioridad, para la conexión directa con la herramienta de gestión ya que, si es un producto comercial, probablemente tenga costo por sistema conectado. De igual manera se deben identificar cuáles aplicaciones o sistemas, seguirán siendo gestionadas de manera manual, directamente sobre el repositorio de usuarios de cada una de ellas

La autorización de acceso "es el área en donde se controla el acceso de los usuarios a los recursos empresariales, se administran las autorizaciones específicas y los derechos en torno a las aplicaciones empresariales, se previene anticipadamente toda actividad fraudulenta y se fortalecen la seguridad de autenticación y las identidades federadas y sesiones de usuarios en todas las empresas. Mientras la gestión de identidad administra el ciclo de vida de la información de identidad, la administración de acceso es el guardián que determina qué usuarios tienen acceso a qué tipo de información y en qué momento, sobre la base de un cambiante conjunto de políticas"[33].

Auditoría: A través de eta se realiza seguimiento o frecuencia con que se accede al sistema por parte de los usuarios que requieren los distintos recursos de la organización. Con la información de auditaje se podrá hacer una revisión permanente sobre los datos que tengan mayores volúmenes de solicitudes o inquietudes y en consecuencia hacer los ajustes que sean pertinentes con las mismas. De igual forma los tiempos de permanencia de cada usuario.

2.1.4 Seguridad informática

Es entendida como "la protección de ventajas de información de la revelación no autorizada, de la modificación, o de la destrucción, o accidental o intencional, o la incapacidad para procesar esa información. La seguridad de la red, se compone de esas medidas tomadas para proteger una red del acceso no autorizado, interferencia accidental o intencionada con operaciones normales, o con la destrucción, inclusive la protección de facilidades físicas, del software, y de la seguridad del personal".[34]

En ese sentido, la seguridad informática como en cualquier otro campo de actividad humana, es "un concepto asociado a la certeza, falta de riesgo o

[33] ORACLE Introducción a Oracle Identity Management. 2008, p.5
[34] www.scoop.it/doc/download/cvdXLLFB5B3H35NMF97_qdw. Recuperado 11-05-2016

contingencia"[35] No obstante, es necesario aclarar que no siempre se puede asegurar la presencia o situación de riesgo porque constantemente surgen amenazas de distinta procedencia que vulneran la seguridad de la información. De ahí que se prefiera hablar de niveles de seguridad según sea el grado de confidencialidad de la información que opere dentro de la organización.

Ahora bien, en cuanto a los elementos principales y de mayor uso para proteger la información de datos, se diferencian tres: el **software, el hardware y los datos**. El hardware constituye el "conjunto de todos los elementos físicos de un sistema informático como CPU, terminales, cableados, medios de almacenamiento secundarios, tarjeta de red, etc... Por software, se entiende el conjunto de programas lógicos que hacen funcionar el hardware tanto sistemas operativos como aplicaciones y por datos el conjunto de información lógica que maneja el software y el hardware como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos"[36].

2.2 MARCO CONCEPTUAL

2.2.1 Sistema de gestión de identidades

Es aquel sistema que busca unificar en un solo repositorio (centralizado o distribuido) todas las identidades de los usuarios de una organización[37]. Y está conformado por una parte procedimental y otra parte tecnológica, busca minimizar los errores que se pueden presentar al tener múltiples repositorios de usuarios como, por ejemplo, error en la escritura de los nombres, duplicidad de cuentas, multiplicidad de contraseñas, etc.

La gestión de identidades y control de acceso involucra diferentes procesos y áreas en la organización, desde la alta gerencia hasta las áreas de soporte y apoyo; cuya implementación y buenos resultados depende de la disposición y grado de compromiso que demuestre cada uno de los diferentes actores al interior de la compañía en el desarrollo de un proyecto de este tipo.

De este modo, la gestión de la identidad y del acceso, frecuentemente conocida por su acrónimo anglosajón IAM (por "Identity and Access Management") es un área de negocio que se dedica a las siguientes tareas:

- ✓ Aprovisionamiento de cuentas de usuario y contraseñas, mediante automatismos, de acuerdo con políticas bien definidas y aplicadas.

---

[35] https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA, Recuperado 11-05-2016

[36] Ibid, p. 2

[37] JUMMP. Desarrollo de software. Sistema de gestión de identidades [En línea]. Mayo 2011. [Consultado sep. 21 de 2015]. Disponible en https://jummp.wordpress.com/2011/05/04/desarrollo-de-software-sistema-de-gestion-de-identidades/

- ✓ Implantación de sistemas de identificación y autenticación única corporativa (también denominado “single sign-on”).
- ✓ Gestión centralizada de las atribuciones de los usuarios, basada en directorios de usuarios (habitualmente basados en LDAP).
- ✓ Modelo de autorizaciones, que concentra en un solo punto las autorizaciones de acceso[38].

Componentes de una solución de Gestión de identidades y Control de Acceso Una solución de gestión de identidades y control de acceso cuenta con los siguientes componentes. Servicio de directorios. “Un servicio de directorios es un componente de la red que permite que un directorio sea administrado de forma central y al mismo tiempo provee información para las aplicaciones organizacionales que interactúen con éste. Un servidor de directorios permite almacenar no solamente usuarios, sino también recursos según sea las necesidades del negocio”[39] En este se toma en consideración lo siguiente:

- Información estructurada y extensible Es entendida a través del esquema del servicio de directorios que se refiere “al conjunto de reglas que determinan que información puede ser almacenada dentro de un servidor de directorios y además determina la manera en que esta información será utilizada en operaciones tales como la búsqueda[40].

Bajo este esquema, cuando el Servidor de Directorios intenta almacenar o modificar una entrada, entendida como una unidad de información representativa de una entidad dentro del servicio de directorios; en ella, el servidor constata que dichas reglas se apliquen conforme a lo que está determinado.

Por otra parte, cuando un cliente u otro servidor de directorios confrontan dos valores de atributos, “consultan al servidor de directorios para determinar el algoritmo de comparación a usar[41]. Para el procesamiento del esquema es importante tener en cuenta la combinación de información que requieren los diferentes servicios y aplicaciones que son atendidos por el servidor de directorios, con el fin de unificar datos redundantes de manera que quede el menor número de entidades posibles”[42].

---

[38] DOMINGO, Ignacio Alamillo; i Aparisi, Xavier Urios; en: La gestión de identidades y capacidades por las administraciones públicas. [Pág. 3]. Diciembre 2004. Consultado. 22-11- 2016]. Disponible en Internet: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Tecnimap/pae_TECNIMAP_2006/pae_TECNIMAP_2006_Comunicaciones_Presentadas_-_5/gestion_de_identidades.pdf

[39] Montoya S, José A, Restrepo R. Zuleima. Gestión de identidades y control de acceso desde una perspectiva organizacional, Ing. USBMed, Vol. 3, No. 1, Enero-Junio 2012 .Consultado 21-11-2016. Disponible en http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf

[40] Ibid. p. 26

[41] Ibid, p. 27

[42] Ibid. p. 27

También el esquema del servicio de directorios se puede utilizar para aplicar limitaciones de tamaño, rango, y formato de los datos almacenados Así mismo, se considera que dentro del esquema de un servicio de directorios participan elementos tales como tipos de atributos que incluyen la siguiente información:

1. Un nombre que identifica de manera única el tipo de atributo,
2. Un OID (Object identifier), una cadena compuesta por una serie de dígitos decimales que tienen una jerarquía determinada y que son controlados por la IANA, ANSI e ISO, entre otros que también identifica de manera única el tipo de atributo.
3. Un indicador de sí el tipo de atributo permite o no múltiples valores,
4. Una sintaxis de atributo asociada y conjunto de reglas de comparación. Dentro de las sintaxis de atributos se especifica la manera exacta a través de la cual los atributos son representados y el algoritmo de comparación que será utilizado en el momento en el que se realice una comparación o búsqueda,
5. Un indicador de uso, de utilización interna por los servidores de directorios y
6. Restricciones respecto al tamaño, rango de valores que pueden ser aceptados por este tipo de atributo"[43].

Así, dentro de este esquema de atributos las organizaciones deben estar preparadas para procesar los respectivos datos mediante la disposición de aplicativos que le den confiabilidad a la información en el momento oportuno y/o cuando sean requeridos, pero también disponer de medidas de control para proteger dicha información, pero también para certificar la autorización de ingreso a las plataformas. "Sin embargo, esto es tan solo una parte del desafío que plantea la gestión de identidades y accesos (IAM). Los servicios deben estar disponibles única y exclusivamente para las personas con los privilegios adecuados, ya sean empleados, proveedores, socios o clientes. Pese a ser una capacidad cada vez más importante, es la que mayores dificultades plantea"[44].

Lo anterior significa que cada aplicación deba tener la información reservada por y para cada usuario lo que hace que el sistema deba disponer varias cuentas y contraseñas en cada caso y en sus diferentes aplicaciones según el número de usuarios. Igualmente, durante todo el ciclo de vida en que el usuario permanezca vinculado con la organización

- Diseño de la identidad digital: La gestión de la identidad digital engloba los procesos y las tecnologías necesarias para la gestión de la información almacenada sobre los individuos, el control de acceso basado en los roles y

[43] Montoya S, José A, Restrepo R. Zuleima. Gestión de identidades y control de acceso desde una perspectiva organizacional, Ing. USBMed, Vol. 3, No. 1, Enero-Junio 2012 .Consultado 21-11-2016. Disponible en http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf

[44] IBM Gestión de identidades y accesos para el cumplimiento continuado y la reducción del riesgo. Consultado 22-11-2016. Disponible en http://docs.media.bitpipe.com/io_10x/io_107393/item_607564/Q4_SWG%20Network%20Security_1162_ES_002_Gestion%20de%20Identidades.pdf

grupos y el proceso de autenticación y autorización en la infraestructura tecnológica de la organización, entre otros aspectos. El objetivo principal de la gestión de la identidad digital es el incremento de la seguridad y de la productividad de la organización[45].

De esta forma, la identidad digital suministra la información sobre las identidades adscritas a la organización, lo mismo que atributos definidos en cada uno de los usuarios. A partir de dicha información, se concretan los perfiles de las diferentes identidades, señalando el tipo de roles o grupos existentes y los privilegios que les asisten. En el diseño de la identidad digital es importante especificar quién, en qué momento y bajo qué condiciones los usuarios pueden ejercer su derecho de ingresar a la información que la organización tiene disponible para cada uno de ellos.

2.2.2 Control de acceso basado en roles (RBAC).

Las políticas de control de accesos basado en roles regulan el acceso de los usuarios a la información en términos de sus actividades y funciones de trabajo (roles), representándose así de forma natural la estructura de las organizaciones[46]. Los sistemas RBAC, son fundamentales para proteger la confidencialidad, integridad y disponibilidad de la información y establecer responsabilidades en los usuarios.

2.2.3 Servicios de directorios.

Son el componente clave de la mayoría de las plataformas de gestión de identidad. Este nivel fundamental está compuesto por el directorio LDAP, que guarda la información de identidad del usuario, incluyendo el nombre de usuarios y las contraseñas[47].

2.2.4 Capa de presentación.

También denominada "capa de usuario", es la que el sistema le presenta al usuario, a través de ella se muestra y captura la información del usuario en un mínimo de proceso, previamente realizando un filtrado para comprobar que no hay errores de formato. Es la interfaz gráfica, debe tener la característica de ser "amigable" (entendible y fácil de usar) para el usuario. Esta capa se comunica únicamente con la capa de negocio[48].

---

[45] PRISE Identidad digital. Consultado 23-11-2016.Disponible en https://www.prise.es/es/services/digid/cons/

[46] ECURED Sistemas de control Consultado 22-11-2016. Disponible en https://www.ecured.cu/Sistemas_de_control_de_acceso

[47] ORACLE Introducción a Oracle Identity Management. Consultado 22-11-2016.Disponible en : http://www.oracle.com/technetwork/es/documentation/317540-esa.pdf

[48] Montejo Juan C., Herrera Hair diseño de un modelo que permita el manejo de identidades de un usuario dentro de una organización. Disponible en http://repository.unad.edu.co/bitstream/10596/6168/1/79556048.pdf

2.2.5 Fundamentos de seguridad de la información.

La importancia de la seguridad de los sistemas informáticos de la empresa es crucial para su desempeño. Hoy en día el conocimiento resulta de suma importancia, ya que determina la esencia en la mayoría de las organizaciones contemporáneas. Por lo tanto, como en la actualidad la mayoría de la información de procesos de las empresas se encuentra digitalizada, se requiere que dicha información se encuentre dentro de un marco de seguridad.

Para generar un marco de seguridad en sus recursos y sistemas informáticos, la empresa cubre sus acciones en el manejo de riesgo, la continuidad del negocio y la seguridad de sistemas informáticos

La seguridad de la información es un conjunto de controles necesarios para la seguridad de los recursos de información (Sistemas de información, Activos, Base de datos y otros) permitiendo al usuario acceder a ellos de forma confiable y segura (Habeas Data)[49] y está dividido en los siguientes aspectos:

Autenticación. Proceso por el cual, una entidad prueba su identidad ante otra. Normalmente, la entidad es un usuario o computador. Este proceso se obtiene mediante la presentación de una propuesta de identidad (nombre de usuario) y la demostración de estar en posesión de las credenciales de acceso, que permiten comprobarla. “La autenticación es la unión de una identidad a un sujeto[50] Es decir es la certificación de la veracidad del nombre del usuario y del uso de la respectiva contraseña Los métodos de autenticación se suelen dividir en tres grandes categorías[51.]

- ✓ Algo que el usuario sabe.
- ✓ Algo que el usuario posee.
- ✓ Características físicas del usuario (autenticación biométrica).

Para el presente proyecto no se tiene en cuenta el último método, ya que no procede para el desarrollo del mismo. Sin embargo, los dos primeros serán utilizados activamente por la asociación.

En cuanto al primero, será la autenticación básica y estándar de las aplicaciones ejemplo, una contraseña, una frase o un número de identificación personal. Tanto las webs, como las de escritorio o móvil, necesitan validar los datos del usuario antes de responder a sus peticiones y facilitar los datos. “Algo que el usuario

[49] PRESIDENCIA DE LA REPÚBLICA. Manual de la política de seguridad para las tecnologías de la información y las comunicaciones – TICS. Versión 5. Bogotá D.C. 2014.

[50] [50] Bishop 2003. Citado por Villalobos B.. Refugio Propuesta de arquitectura de gestión de identidades digitales para el consorcio minero Benito Juárez. Colima 2012,p. 25

[51] PALAZON ROMERO, José María, FELGUERA, Antoni y CASTELLA-ROCA, Jordi. Single sign-on y federación de identidades. Universidad Oberta de Catalunya. España. 2011.

posee", por ejemplo, una tarjeta de la identificación, símbolo de la seguridad, símbolo del software o teléfono celular. De esta forma, se validan los datos y se da acceso.

A continuación, se especifican las siguientes a modo de ejemplo el Sistema centralizado.

Autorización (Control de acceso). Este proceso tiene como objetivo la protección de los recursos computacionales de accesos que no estén autorizados. En este proceso se lleva el control de acceso a los recursos y sistemas informáticos según el flujo de trabajo que corresponda. Lo anterior se realiza en base a políticas de seguridad por lo cual solo se permite el acceso según las autorizaciones asignadas a cada usuario[52] mediante una petición de este y la correspondiente aprobación por parte del deño del proceso.

Este trabajo se centra en autenticación. Ya que no existe autorización sin un previo mecanismo de comprobación, parece razonable pensar que el primer paso de todo sistema de login es la autenticación. Cualquier sistema de identificación ha de poseer unas determinadas características para ser viable:

Ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo de en los sistemas menos seguros).

Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto).

Soportar con éxito cierto tipo de ataques.

Ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen.

2.2.6 Sistema centralizado para la gestión de control de acceso.

Este modelo se relaciona con una medida que facilita la distribución de permisos a todas las aplicaciones y sistemas. “Una ventaja de este método es que la realización del control de acceso se encuentra centralizada, permitiendo con ello una sola interface para el manejo de la seguridad en todos los sistemas y el manejo de los recursos.
La principal desventaja es que se tiene un solo punto de fallo, por lo tanto, si queda fuera el sistema que controla la realización del acceso, el acceso a los sistemas y recursos no se podrá realizar. Una posible forma de mitigar el riesgo de

[52] Villalobos B. refugio. Propuesta de arquitectura de gestión de identidades digitales para el consorcio minero Benito Juárez. Consultado 23-11-2016.Disponible en http://digeset.ucol.mx/tesis_posgrado/Pdf/Refugio_Javier_Villalobos_Becerra.pdf

continuidad es contar con un solo sistema central que puede ser mediante Clustering del sistema de control de acceso[53].

2.2.7 La decisión del control de acceso.

La principal parte de control de acceso a la información es determinar los recursos a los cuales una identidad tiene autorización de acceso. La decisión se basa en una política de seguridad cuya elaboración debe ser previa a este proceso.
Para que una política de seguridad de acceso a los recursos sea efectiva, se debe tener un conocimiento pleno del flujo de trabajo de la empresa. Con este nivel de seguridad se logra mayor eficiencia al momento de gestionar el control de acceso.

2.2.8 Manejo de autorizaciones y garantizar el acceso a.

Garantizando el acceso al recurso que se necesite acceder y considerando las condiciones de seguridad que el sistema requiere, se mejora el tiempo de respuesta al usuario evitando demoras en la autorización

"Con lo anterior se facilita la tarea de mantenimiento de las autorizaciones, ya que por ejemplo en caso de que un usuario sea asignado a un área, solo se le tendría que asignar el rol correspondiente para que tome los permisos de acceso a los recursos, desafiliando solamente la aplicación o el rol si es necesario"[54].

Para lograr concretar el sistema centralizado de identidades al cual se refiere el presente proyecto, es necesario establecer las diferencias entre autorización y autenticación.

2.3 ESTADO DEL ARTE

2.3.1 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[55]:

- ✓ 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

[53] Montejo Juan C., Herrera Hair diseño de un modelo que permita el manejo de identidades de un usuario dentro de una organización. Disponible en http://repository.unad.edu.co/bitstream/10596/6168/1/79556048.pd
[54] Ibid. P. 30
[55] Ibid. p. 33.

- ✓ 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.

2.3.2 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. [56]

2.3.3 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.[57] El manejo de identidades está siendo automatizado por medio de la solución de IAM, de esta manera mejora la eficiencia de los procesos.

2.4 MARCO LEGAL

Constitución Política de Colombia En el artículo 15 hace referencia a la protección de la intimidad personal y el respeto a la privacidad.[58]
De manera específica la legislación y normatividad que en el país se ha dado con respecto a la protección de la información digital, existen las siguientes normas:

2.4.1 Ley 527 [59]

“Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”

---

[56] Ibid. p. 33.
[57] Ibid. p. 33.
[58] Asamblea Nacional Constituyente. Constitución Política de Colombia. Bogotá, 1991,art. 15
[59] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (Agosto 18 de 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones Diario Oficial 43.673 del 21 de agosto de 1999. p. 1-15.

2.4.2 Ley 594[60]

“Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.

2.4.3 Ley Estatutaria 1581[61]

“Por la cual se dictan disposiciones generales para la protección de datos personales”**.**

2.4.4 Ley estatutaria 1266[62]

“Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.

2.4.5 Ley 1273[63]

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones “.

---

[60] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 594 (4 de julio de 2000). por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Diario Oficial No. 44.093, de 20 de julio de 2000

[61]COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581. (Octubre 17 de 2012, art. 1). octubre 17 de 2000) Diario Oficial No. 48.587 de 18 de octubre de 2012

[62] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1266. (Diciembre 31 de 2008). por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial No. 47.219 de 31 de diciembre de 2008

[63] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (Enero 05 de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones Diario Oficial No. 47.223 de 5 de enero de 2009

2.4.6 Decreto 1377[64]

Reglamenta la Ley 1581 de 2012. Precisando que no se podrán recolectar datos personales sin autorización del Titular.

2.4.7 Resolución 2554[65]

Modificación al Régimen de Protección de los Derechos de los Usuarios de Servicios de Telecomunicaciones.

A nivel internacional existe una normatividad específica que opera en el ámbito europeo pero que es acogida por varios países latinoamericanos. Se pueden citar las siguientes normas:

2.4.8 Convenio (108) del Consejo de Europa[66]

Para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal.

2.4.9 Directiva 95/46/CE[67]

Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija

---

[64] Presidencia de la República Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581 con el fin de facilitar su implementación y cumplimiento en aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas. Diario Oficial 48834 de junio 27 de 2013

[65] Comisión de regulación de las comunicaciones.(19 de mayo de 2010) Por la cual se modifican los artículos 1o, 78, 79 y 86 de la Resolución CRT 1732 de 2007, y se deroga el artículo 85 de la Resolución CRT 1732 de 2007 y la Resolución CRT 1890 de 2008.Diario Oficial No. 47.715 de 20 de mayo de 2010

[66] Consejo Europeo Convenio 108 del Consejo de Europa, de 28-1-1981,para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.Ratificado por España el 27 de enero de 1984 (entró en vigor de forma general el 1 de octubre de 1985, de conformidad con lo establecido en el artículo 22.2 del mismo Boletín Oficial del Estado núm. 274, de 15 de septiembre de 1985

[67] Parlamento y Concejo Europeo Directiva La Directiva 95/46/CE. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales Diario Oficial de las Comunidades Europeas, DO L 281, 23/11/1995)

límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales.

2.4.10 Real Decreto 1332/1994[68]

Por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal.

2.4.11 Reglamento (UE) 2016/679 [69]

Establecido por el Parlamento Europeo y Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos.

2.5 MARCO CONTEXTUAL

Este estudio está dirigido a toda organización empresarial, tanto de bienes como de servicios que pretenda mejorar los procesos de identificación de los usuarios y/o clientes, lo mismo que ejercer un control más seguros de sus identidades que permita salvaguardar igualmente la información de la entidad como la identidad y manejo de los registros informativos de manera segura, y confiable, evitando así riesgos que alteren los datos o expongan la seguridad de la información registrada.

[68] Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. BOE núm. 147, de 21 de junio de 1994.

[69] Parlamento Europeo y Consejo Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos Diario Oficial de la Unión Europea L 119/1 de 27 de abril de 2016

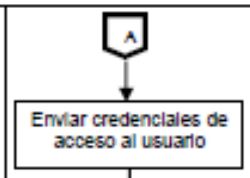
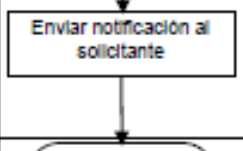
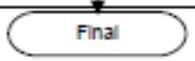
3 DESCRIPCIÓN DEL MODELO ACTUAL UTILIZADO POR LAS ORGANIZACIONES PARA EL MANEJO DE IDENTIDADES

3.1 INTRODUCCIÓN

Al interior de la entidad se hace evidente que no se tiene un procedimiento claramente definido para la gestión y administración de identidades, lo que puede derivar en duplicidad de usuarios, permisos que son mal asignados, usuarios a los que se les mantienen sus accesos y privilegios aún después de ser retirados de la entidad, no se definen políticas claras en la creación de contraseñas y nombres de usuario. Todo lo anterior puede en algunos casos hacer que se vea comprometida tanto la integralidad como la seguridad de la información de la entidad.

Figura 2. Formato De Solicitud De Creación De Cuentas De Usuario

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	Envio de correo solicitando creación de cuentas de usuario y/o asignación de privilegios	El jefe de área o persona responsable envía solicitud a través de correo electrónico, por cada aplicación a la cual el usuario necesite acceder.	Correo electrónico de solicitud creación de una cuenta de usuario.	Persona responsable del área a la cual pertenece el usuario para el cual se solicita la creación de una cuenta de usuario.
3	Recepción de solicitud	El administrador de cada aplicación recibe solicitud a través de correo electrónico.	Solicitud a través de correo electrónico para Creación de Cuentas de Usuario.	Persona responsable del área a la cual pertenece el usuario para el cual se solicita la creación de una cuenta de usuario o la asignación de un rol o privilegio.
4	Validación de las condiciones para la creación de cuentas de usuario y/o asignación de privilegios	Validar las condiciones: 1)Se valida los permisos solicitados para el usuario, correspondan con los del área a la cual pertenece.	Correo electrónico de solicitud.	Administrador de la aplicación.
5	Crear cuenta de acceso al usuario A	Si se cumplen las condiciones se procede a crear la cuenta de usuario o asignar los privilegios. Si no se cumplen las condiciones se debe informar al solicitante vía correo electrónico indicando las razones para no proceder a procesar el permiso.		Administrador de la aplicación.

6		Enviar las credenciales de acceso únicamente al correo electrónico corporativo del usuario para el cual se le solicitó la creación de una cuenta de usuario.	Correo electrónico	Administrador de la aplicación.
7		Notificar al solicitante del permiso y al usuario para el cual se solicitó el permiso del resultado de la solicitud		Administrador de la aplicación.
8				

Fuente: Propiedad del autor

En la figura 2 se puede observar el proceso que utilizan las organizaciones en el manejo de identidades, donde las solicitudes se pueden hacer a través de correo electrónico por parte del jefe de oficina, o de manera personal por parte del mismo usuario, sin tener un control de las solicitud a través de formatos, se puede llegar a que cada usuario dentro de la organización tenga un login para cada aplicación que tienen la organización.

3.2 Solicitud de cuentas de usuario

La solicitud de creación de cuentas de usuario se realiza a los diferentes administradores de las aplicaciones que de manera aislada procesan dicha solicitud, validando cada uno diferentes datos y en algunos casos sin previa verificación del área de talento humano, que permita por lo menos verificar si el funcionario está activo. Como no existen políticas claras que definan la administración y gestión de cuentas cada administrador lo realiza de acuerdo a su experticia, sin tener en cuenta las necesidades y políticas que deberían estar implementadas al interior de la entidad, cada aplicación maneja diferentes lineamientos tanto en la creación de nombres de usuario y contraseñas. No se tienen guías que indiquen como se realiza el procedimiento.

3.3 Sobrecarga de la mesa de ayuda

Existe una gran proliferación de usuarios y contraseñas como resultado de la gestión de cuentas de usuario para las distintas aplicaciones y sistemas, ocasionando que la mesa de ayuda a los usuarios termina destinando un alto porcentaje de operadores para gestionar los cambios de contraseña, así como llevando a cabo el desbloqueo de cuentas de usuario. Ocasionando pérdida de tiempo y recursos para atender estas solicitudes.

3.4 Gestión de usuarios de red

Actualmente no se cuenta con políticas definidas de manejo de identidades, con una tipología clara de creación de cuentas de red, la IP asignada a la cuenta de usuario no describe quien la tiene asignada si no al contrario muestra el nombre de la máquina, estas se crean indiscriminadamente sin ningún lineamiento si no con el criterio del administrador responsable.
También se genera múltiples usuarios con diferentes Id y con el mismo número de cédula.

3.5 Seguridad (Cuentas huérfanas)

Se evidencia que, debido al alto número de aplicaciones y la creación de cuentas para cada una de ellas, se hace más complicado establecer controles para garantizar que las cuentas se crean y eliminan de manera oportuna y apropiada. Así como que exista un único identificador para acceder a todas las aplicaciones.

3.6 Creación cuentas de correo corporativo.

Al igual que en los procesos anteriores se evidencia la falta de políticas para la creación de cuentas de correo institucional, resultando con esto que no hay estandarización en las cuentas, por ejemplo, en ocasiones se usa el nombre completo, en otros la inicial del nombre y el primer apellido, en otros primer nombre y primer apellido. No se tiene control sobre la cantidad de licencias disponibles.

Usuarios se eliminan de algunos aplicativos, como no se tiene el inventario completo de los que tiene asignado un usuario, esto dificulta el control y seguimiento.

4 DESCRIPCIÓN DEL MODELO PROPUESTO PARA EL MANEJO DE IDENTIDADES DENTRO DE UNA ORGANIZACIÓN

4.1 INTRODUCCIÓN

4.2 OBJETIVO

A continuación, se identifican los datos involucrados en la ejecución de las tareas de gestión de administración de identidades en el modelo de sistema propuesto.

Figura 3. Formato De Solicitud De Creación De Cuentas De Usuario

	FORMATO DE SOLICITUD DE CREACIÓN CUENTAS DE USUARIO	Código:
		Fecha de aprobación:
	GRUPO DE SOPORTE O SISTEMAS	Versión: 01

FECHA:	día/mes/año

I. Datos del Responsable de Área que hace la solicitud

Nombre	
Dependencia	
Cargo	
Correo electrónico	

II. Detalles de Creación de Cuenta de Usuario o asignación de privilegio/perfil

Nombre completo del usuario					
Número de Identificación					
Cargo					
Validez de la solicitud (Marcar con una X)	Indefinida	X	Temporal		
En caso de que sea temporal indicar la duración:		Marcar con una X:		Días	
				Meses	
Correo electrónico del usuario para la notificación de asignación de privilegio y/o envío de las credenciales de acceso:					

III. Sistemas de Información sobre los que se solicita la creación de cuenta o asignación de privilegio/perfil		
Nombre del sistema de información (Por ejemplo, Correo electrónico, App1, App2)	**Privilegio/Rol de usuario/Perfil de Usuario solicitado**	**Permiso adicional solicitado (si aplica)**

IV. Evaluación de la Solicitud por parte del Custodio del Sistema de Información				
Solicitud cumple con condiciones de seguridad (Marcar con una X)	SI		NO	
Razones por las cuales no es aprobada la solicitud (en caso que corresponda)				
1				
2				

4.2.1 Descripción Formato de solicitud creación de cuentas de usuario

✓ Fecha: Fecha en la que se realiza la solicitud.

✓ Datos del Responsable: Puede ser el Jefe de la Oficina, el Coordinador, el Director (o quien el delegue) o la persona responsable del área a la cual pertenece el usuario para el que se solicita la creación de una cuenta de usuario o la asignación de un rol o privilegio.

✓ Detalles de Creación de Cuenta de Usuario: Datos de la persona para la cual se solicita la creación de la cuenta de usuario o la asignación de un rol o privilegio.

✓ Sistemas de Información sobre los que se solicita la creación de cuenta: Se coloca el detalle del sistema(s) de información en los cuales se solicita la creación de una cuenta de usuario o la asignación de privilegios.

✓ Evaluación de la Solicitud por parte del Custodio: Lo diligencia el Responsable/custodio del Sistema de Información.

✓ Razones por las cuales no es aprobada la solicitud: No se cuenta con autorización del sistema de información, se solicita una cuenta de grupo sin justificación, se incumple la separación de funciones.

Figura 4. Formato De Solicitud De Cancelación Cuentas O Permisos De Usuario

	FORMATO DE SOLICITUD DE CANCELACIÓN CUENTAS O PERMISOS DE USUARIO	Código:
		Fecha de aprobación:
	GRUPO DE SOPORTE O SISTEMAS	Versión: 01
FECHA:	día/mes/año	

I. Datos del Responsable de Área que hace la solicitud

Nombre	
Dependencia	
Cargo	
Correo electrónico	

II. Detalles de Cancelación de Cuenta de Usuario o derogación de privilegio/perfil

Nombre completo del usuario					
Número de Identificación					
Cargo					
Validez de la solicitud (Marcar con una X)	Indefinida	X	Temporal		
En caso de que sea temporal indicar la duración:		Marcar con una X:		Días	
				Meses	
Correo electrónico del usuario para la notificación de asignación de privilegio y/o envío de las credenciales de acceso:					

III. Sistemas de Información sobre los que se solicita la cancelación de cuenta o derogación de privilegio/perfil

Nombre del sistema de información (Por ejemplo, Correo electrónico, App1, App2)	**Privilegio/Rol de usuario/Perfil de Usuario solicitado**	**Permiso adicional solicitado (si aplica)**

IV. Evaluación de la Solicitud por parte del Custodio del Sistema de Información				
Solicitud cumple con condiciones de seguridad (Marcar con una X)	SI		NO	
Razones por las cuales no es aprobada la solicitud (en caso que corresponda)				
1				
2				
3				

4.2.2 Descripción Formato de solicitud cancelación cuentas o permisos de usuario

✓ Fecha: Fecha en la que se realiza la solicitud.

✓ Datos del Responsable: Puede ser el Jefe de la Oficina, el Coordinador, el Director (o quien el delegue) o la persona responsable del área a la cual pertenece el usuario para el que se solicita la cancelación de una cuenta o permiso de usuario o la derogación de un rol o privilegio.

✓ Detalles de Cancelación de Cuenta de Usuario: Datos de la persona para la cual se solicita la cancelación de la cuenta de usuario o la derogación de un rol o privilegio.

✓ Sistemas de Información sobre los que se solicita la creación de cuenta: Se coloca el detalle del sistema(s) de información en los cuales se solicita la cancelación de una cuenta de usuario o la derogación de privilegios.

✓ Evaluación de la Solicitud por parte del Custodio: Lo diligencia el Responsable/custodio del Sistema de Información.

4.3 PROCEDIMIENTOS

4.3.1 PROCEDIMIENTO CREACIÓN Y CANCELACIÓN DE CUENTAS DE USUARIO

	PROCEDIMIENTO DE CREACIÓN Y CANCELACIÓN DE CUENTAS DE USUARIO	Código:
		Fecha de aprobación:
	GRUPO DE SOPORTE O SISTEMAS	Versión: 01

1. Objetivo
Asegurar que las solicitudes de creación y cancelación de cuentas de usuario, así como los cambios en los niveles de privilegios se realizan considerando los lineamientos indicados en la Política de Control de Acceso para garantizar la correcta gestión de accesos a los activos de información de la entidad.

2. Alcance

Todos los procesos, de la entidad se inician desde el momento en que un usuario envía una solicitud y termina cuando se da la respuesta respectiva.

3. Definiciones

3.1 Usuario solicitante: Quien hace la solicitud de creación de una nueva cuenta de usuario en un sistema de información o la asignación de un privilegio sobre una cuenta existente.

3.2 Sistema de información: Elementos de diferente tipo (humanos, tecnológicos, conocimiento, información) que componen una arquitectura de gestión y procesamiento de datos para suplir un objetivo o requerimiento de una organización.

3.3 Separación de Funciones: Principio que establece que las actividades críticas o de alta responsabilidad, (como algunas incluidas en un sistema de información) deberían ser segregadas para reducir para reducir oportunidades de acceso no autorizado, modificaciones no intencionales o mal uso.

4. Criterios Operativos

4.1. Sobre quienes solicitan la creación y cancelación de cuentas de usuario: Corresponde a la persona responsable del área a la cual pertenece el usuario para el que se solicita la creación de una cuenta de usuario o la asignación de un rol o privilegio.

4.2. Sobre la consulta al propietario del sistema de información para el cual se solicita acceso: Se debe validar con el propietario del sistema de información sobre el cual se solicita la creación de una cuenta de usuario o la asignación de un rol o privilegio, que efectivamente se cuenta con autorización para el permiso solicitado. En caso de que no se obtenga aprobación no se podrá realizar la configuración del permiso.

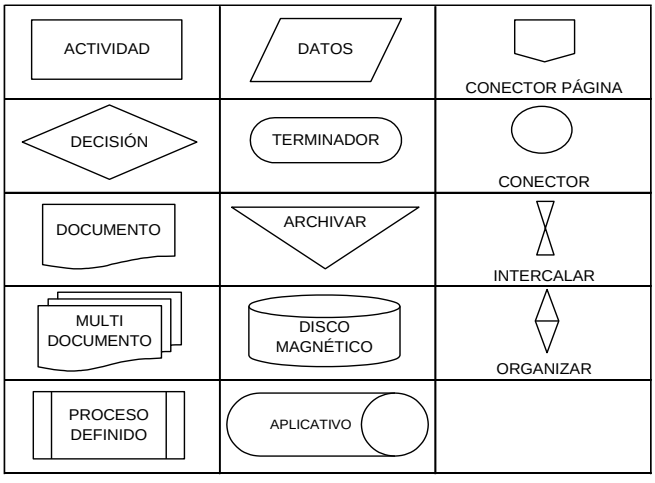
4.3 Sobre el envío de credenciales de acceso: Las credenciales de acceso se deben enviar únicamente a la cuenta de correo electrónico corporativa del usuario para el cual se solicita la creación de una cuenta en un sistema de información. Solo en el caso de creación de cuentas de correo electrónico corporativas se podrá enviar la información de credenciales de acceso a una cuenta de correo personal.

5. Normatividad

5.1. Norma ISO 27001:2013

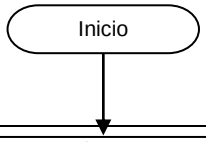
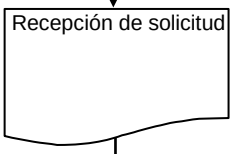
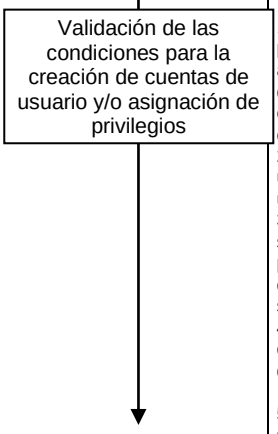
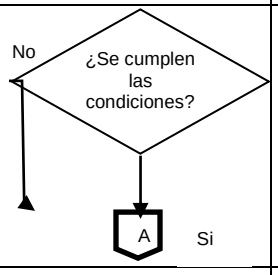
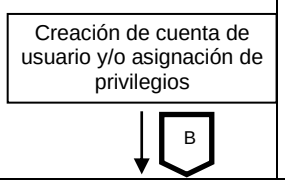
5.2. Control de seguridad A.9.2.1, A.9.2.2, A.9.2.3 Norma ISO 27001:2013

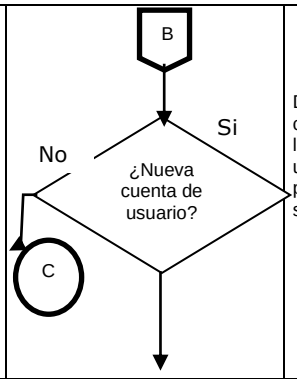
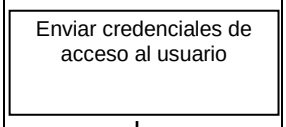
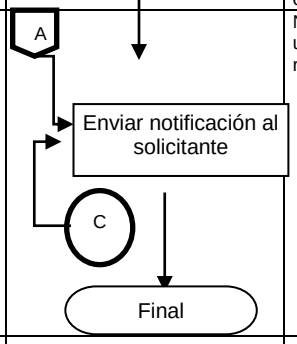
6. Símbolos
diagramas de flujo



4.3.2 PROCEDIMIENTO CREACIÓN DE CUENTAS DE USUARIO

	PROCEDIMIENTO DE CREACIÓN DE CUENTAS DE USUARIO	Código:
		Fecha de aprobación:
	AREA DE SISTEMAS E INFORMATICA	Versión:01

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1				
2		El proceso de tecnología recibe solicitud a través de la mesa de ayuda, correo electrónico o memorando.	Solicitud en la mesa de ayuda, memorando o correo electrónico que incluye el Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario.	Persona responsable del área a la cual pertenece el usuario para el cual se solicita la creación de una cuenta de usuario o la asignación de un rol o privilegio. Puede ser el Jefe de la Oficina, Coordinador, Director, o quien ellos deleguen.
3		Validar las condiciones de seguridad: 1) El usuario debe poseer un único ID que permita mantener la responsabilidad de las acciones realizadas por cada usuario (No se deben configurar IDs de grupo, salvo que exista una justificación institucional). Sino cuenta con uno se debe crearlo. 2)No se deben asignar o habilitar IDs de usuario redundantes o genéricos (Admin, user, guest). 3)En el caso de solicitudes de acceso a sistemas de información que sean de propiedad de otro proceso se debe contar con autorización del propietario de ese sistema de información 4)Los permisos solicitados deben corresponder a los mínimos requeridos para desarrollar la función. 5)Se debe cumplir la condición de segregación de funciones (una actividad crítica no puede quedar a cargo de un único usuario).	Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Custodio del sistema de información
4		Si se cumplen las condiciones se procede a crear la cuenta de usuario o asignar los privilegios. Si no se cumplen las condiciones se debe informar al solicitante indicando las razones para no proceder a procesar el permiso.	Formato de Solicitud de Creación y Eliminación de Cuentas de Usuario.	Custodio del sistema de información
5		Configurar la cuenta de usuario solicitada o asignar el privilegio	Registro de actividad en el sistema de información	Custodio del sistema de información

6		Dependiendo de si se trata de una nueva cuenta de usuario, se procede al envío de las credenciales únicamente al usuario que utilizará el acceso. En caso contrario se procede a la notificación al usuario y al solicitante de los cambios realizados.	Correo electrónico	Custodio del sistema de información
7		Enviar las credenciales de acceso únicamente al correo electrónico corporativo del usuario para el cual se le solicitó la creación de una cuenta de usuario. Solo en el caso de creación de cuentas de correo electrónico corporativas se podrá enviar la información de credenciales de acceso a una cuenta de correo personal.	Correo electrónico	Personal de Soporte
8		Notificar al solicitante del permiso y al usuario para el cual se solicitó el permiso del resultado de la solicitud	Actualización en la mesa de ayuda, memorando o correo electrónico incluyendo el Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Personal de Soporte

DURACIÓN DEL PROCEDIMIENTO	OBSERVACIONES
La duración varía en función del tiempo requerido por el custodio para la actividad 3 (Validación de condiciones para la creación de cuentas de usuario y asignación de privilegios) y la actividad 5 (Creación de cuenta de usuario y/o asignación de privilegios), puesto que depende del sistema de información. sin embargo, un estimado puede estar entre 1 y 3 horas.	

4.3.3 PROCEDIMIENTO CANCELACIÓN DE CUENTAS O PERMISOS DE USUARIO

	PROCEDIMIENTO DE CANCELACIÓN DE CUENTAS DE USUARIO	Código:
		Fecha de aprobación:
	AREA DE SISTEMAS E INFORMATICA	Versión:01

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	Recepción de solicitud	El proceso de tecnología recibe solicitud a través de la mesa de ayuda, correo electrónico o memorando.	Solicitud en la mesa de ayuda, memorando o correo electrónico que incluye el Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Corresponde a la persona responsable del área a la cual pertenece el usuario para el cual se solicita la cancelación de una cuenta de usuario o la derogación de un rol o privilegio.
3	Validación de las condiciones para la cancelación de cuentas de usuario y/o derogación de privilegios	Validar las condiciones de seguridad: -Se debe cumplir la condición de segregación de funciones (una actividad crítica no puede quedar a cargo de un único usuario). Si no se cumple esta condición se debe indicar al solicitante que antes de solicitar la cancelación de una cuenta o la derogación de un privilegio para un usuario X, primero se debe indicar a un usuario Y al cual se le otorgarán los privilegios que se revoquen al usuario X.	Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Custodio del sistema de información
4	No ¿Se cumplen las condiciones ? Si	Si se cumplen las condiciones se procede a cancelar la cuenta de usuario o a derogar los privilegios. Si no se cumplen las condiciones se debe informar al solicitante indicando las razones para no proceder a procesar el permiso.	Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Custodio del sistema de información
5	Cancelación de cuenta de usuario y/o derogación de privilegios	Cancelar la cuenta de usuario o derogar el privilegio indicado en la solicitud	Registro de actividad en el gestor de autenticación y autorización propio del sistema de información	Custodio del sistema de información
6	Enviar notificación al solicitante	Notificar al solicitante y al usuario del resultado de la solicitud. En caso de que la solicitud no haya sido posible, se debe informar al solicitante la razón por medio del Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario.	Actualización en la mesa de ayuda, correo electrónico o memorando incluyendo el Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Personal de Soporte
	Final			

DURACIÓN DEL PROCEDIMIENTO	OBSERVACIONES
La duración vería en función del tiempo requerido por el custodio para la actividad 3 (Validación de condiciones para la cancelación de cuentas de usuario y/o derogación de privilegios) y la actividad 5 (Cancelación de cuenta de usuario y/o derogación de privilegios), puesto que depende del tiempo de configuración del sistema de información. Sin embargo, un estimado de tiempo puede estar entre 1 y 3 horas.	

5 DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD

5.1 OBJETIVO DE CONTROL Y CONTROLES DE SEGURIDAD CONFORMES AL ESTANDAR ISO 27001:2013

Figura 5. Anexo A Norma ISO/IEC 27001:2013[70]. Políticas de la Seguridad de la Información

<table>
<tr><td>A.5</td><td colspan="3">POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.5.1</td><td colspan="3">Orientación de la dirección para la gestión de la seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: Brindar orientación y soporte por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</td></tr>
<tr><td rowspan="3">A.5.1.1</td><td rowspan="3">Políticas para la seguridad de la información</td><td rowspan="3">Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.</td><td>APLICA</td></tr>
<tr><td>SI / NO</td></tr>
<tr><td>Las políticas de la seguridad de la información proveen un direccionamiento estratégico acorde a los requerimientos de la organización y cumplimiento con leyes y regulaciones. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
<tr><td rowspan="3">A.5.1.2</td><td rowspan="3">Revisión de las políticas para la seguridad de la información</td><td rowspan="3">Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.</td><td>APLICA</td></tr>
<tr><td>SI / NO</td></tr>
<tr><td>Las políticas de la seguridad de la información deberían ser evaluadas con el fin de responder a los cambios de la organización.</td></tr>
<tr><td>A.6</td><td colspan="3">ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.6.1</td><td colspan="3">Organización Interna</td></tr>
</table>

[70] Instituto Colombia no de normas técnicas y certificación, ICONTEC. Norma Técnica NTC-ISO.IEC 27001.Bogotá. 2013

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.			
A.6.1.1	Roles y responsabilidades para la seguridad de la información	**Control:** Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	**APLICA** **SI** / **NO** Los roles y responsabilidades son vitales para la protección de los activos informáticos individuales, así como los procesos específicos para la seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.
A.6.1.2	Separación de deberes	**Control:** Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	**APLICA** **SI** / **NO** Ningún empleado debería tener acceso a modificar los activos informáticos sin autorización previa.
A.6.1.5	Seguridad de la información en la gestión de proyectos	**Control:** La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyectos.	**APLICA** **SI** / **NO** Una metodología de análisis de riesgos debería ser parte del proceso de implementación de un proyecto de TI con el fin de direccionarlos y controlarlos.
A.6.2	Dispositivos móviles y teletrabajo		
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.			
A.6.2.1	Políticas para dispositivos móviles	**Control:** Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	**APLICA** **SI** / **NO** Los dispositivos móviles son un riesgo potencial para la seguridad de la información.
A.6.2.2	Teletrabajo	**Control:** Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	**APLICA** **SI** / **NO** El teletrabajo debería tener una política de seguridad sobre las condiciones y restricciones.
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS		
A.7.1	Antes de asumir el empleo		

<table>
<tr><td colspan="4">Objetivo: Asegurar que los empleados y contratistas comprenden las responsabilidades y son idóneos en los roles para que los consideran.</td></tr>
<tr><td rowspan="2">A.7.1.1</td><td rowspan="2">Selección</td><td rowspan="2">Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.</td><td>APLICA</td></tr>
<tr><td>SI / NO
Aparte de las competencias técnicas, el personal contratado debería ser éticamente correcto y confiable especialmente si accede a información sensitiva de la organización.</td></tr>
<tr><td rowspan="2">A.7.1.2</td><td rowspan="2">Términos y condiciones del empleo</td><td rowspan="2">Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.</td><td>APLICA</td></tr>
<tr><td>SI / NO
Los acuerdos contractuales de los empleados deberían tener cláusulas relativas a la confidencialidad de la información y respecto a las leyes y derechos de propiedad intelectual.</td></tr>
<tr><td>A.7.2</td><td colspan="3">Durante la ejecución del empleo</td></tr>
<tr><td colspan="4">Objetivo: Asegurarse de los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.</td></tr>
<tr><td rowspan="2">A.7.2.1</td><td rowspan="2">Responsabilidades de la dirección</td><td rowspan="2">Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.</td><td>APLICA</td></tr>
<tr><td>SI / NO
La dirección asegura que los roles y responsabilidades están claramente definidos antes de brindar acceso confidencial, así como los empleados están comprometidos con las políticas de seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
</table>

A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	**Control:** Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes a su cargo.	**APLICA** **SI** / **NO** Mediante un programa de entrenamiento relativo a la seguridad de la información, los empleados son conscientes de su importancia y cómo pueden cumplir con las políticas del SGSI.
A.7.2.3	Proceso disciplinario	**Control:** Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	**APLICA** **SI** / **NO** Los procesos disciplinarios son analizados en base al grado de responsabilidad del empleado y el impacto que tiene en la organización.
A.9	CONTROL DE ACCESO		
A.9.1	Requisitos del negocio para control de acceso		
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			
A.9.1.1	Política de control de acceso	**Control:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	**APLICA** **SI** / **NO** El control de acceso físico y lógico con principios del menor privilegio permite tener un control sobre los riesgos de diseminación de información o acceso físico a los activos a personas no autorizadas.
A.9.1.2	Acceso a redes y a servicios en red	**Control:** Sólo se debe permitir acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	**APLICA** **SI** / **NO** Las redes y servicios de red proveen acceso a diferentes servicios dentro de la organización al personal autorizado.
A.9.2	Gestión de acceso de usuarios		
Objetivo: Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			
A.9.2.1	Registro y cancelación de registro de usuarios	**Control:** Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	**APLICA** **SI** / **NO** Los identificadores únicos de los empleados mantienen un registro de las acciones realizadas.

A.9.2.2	Suministro de acceso de usuarios	**Control:** Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	**APLICA** **SI** / **NO** Los permisos y privilegios de los usuarios son asignados o revocados de forma automática mediante un proceso formal.
A.9.2.3	Gestión de derechos de acceso privilegiado	**Control:** Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	**APLICA** **SI** / **NO** Los privilegios de acceso a cualquier sistema o información deberían ser otorgados de acuerdo a las políticas de acceso.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	**Control:** Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	**APLICA** **SI** / **NO** La autenticación de los empleados en los sistemas debería mantenerse confidencial y secreta para evitar alteración y/o modificación de la información por parte de personas no autorizadas.
A.9.2.5	Revisión de los derechos de acceso de usuarios	**Control:** Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	**APLICA** **SI** / **NO** Los derechos de acceso verifican qué puede hacer un usuario sobre la información o sistemas.
A.9.2.6	Retiro o ajuste de los derechos de acceso	**Control:** Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	**APLICA** **SI** / **NO** La remoción de los derechos de acceso permite que los empleados no sigan teniendo acceso a información o a los sistemas una vez terminado el contrato o cambio en el cargo.
A.10	CIFRADO		
A.10.1	Controles criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o integridad de la información.			

A.10.1.1	Política sobre el uso de controles criptográficos	**Control:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	**APLICA** **SI** / **NO** La criptografía cifra mediante algoritmos de encriptación los mensajes transmitidos garantizando la confidencialidad, integridad y autenticidad de los mensajes, impidiendo así que sea legible por personas no autorizadas.
A.10.1.2	Gestión de llaves	**Control:** Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	**APLICA** **SI** / **NO** La gestión de llaves criptográficas vela por su seguridad, mantenimiento, renovación, distribución y destrucción.
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1	Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			
A.11.1.1	Perímetro de seguridad física	**Control:** Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	**APLICA** **SI** / **NO** El perímetro de seguridad física impide el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización.
A.11.1.2	Controles de acceso físicos	**Control:** Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	**APLICA** **SI** / **NO** Los controles de accesos físicos impiden el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	**Control:** Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	**APLICA** **SI** / **NO** Las oficinas y lugares de trabajo claves deberían estar protegidas impidiendo el acceso físico a personas no autorizadas, así como no ser públicamente visibles.
A.11.1.4	Protección contra amenazas externas y ambientales	**Control:** Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	**APLICA** **SI** / **NO** Protección física contra los desastres naturales y/o humanos.

6 POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

6.1 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo

Brindar orientación y soporte por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
Las Políticas de Seguridad de la Información, deben surgir como un compromiso de la alta dirección, donde se busque sensibilizar e involucrar tanto a directivos, funcionarios, contratistas y terceros que de una u otra forma tengan relación con la entidad; acerca de la importancia de la información y por ende de las medidas que permitan su protección, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional. De igual forma se debe realizar una revisión periódica de las políticas y hacer los correspondientes ajustes que se requieran.

Aplicabilidad

Estas son políticas que aplican a la Alta Gerencia, Directores, Secretarios, Jefes de Oficina, Jefes de Área, funcionarios, contratistas, en general a todos los usuarios de la información que cumplan con los propósitos generales de la entidad.

6.2 POLÍTICA DE ORGANIZACIÓN INTERNA

Objetivo

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

6.2.1 Roles y responsabilidades

Los roles y responsabilidades son vitales para la protección de los activos informáticos individuales, así como los procesos específicos para la seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013

Directrices

1. Todos los Colaboradores, proveedores o contratistas, así como los terceros autorizados para acceder a la infraestructura de procesamiento de

información, serán responsables del cumplimiento de las políticas, procedimientos y estándares definidos por la Entidad.

2. La información almacenada en los equipos de cómputo de la Entidad es propiedad de la misma y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.

3. Todos los Colaboradores deberán mantener especial cuidado de no divulgar información CONFIDENCIAL o RESERVADA en lugares públicos o privados, mediante conversaciones o situaciones que puedan comprometer la seguridad o el buen nombre de la organización. Esta restricción se extiende inclusive con posterioridad a terminación del vínculo laboral o terminación de los contratos y debe estar incluida en los Acuerdos de Confidencialidad.

4. Todos los activos de información de la entidad deben tener claramente identificado su propietario y su custodio.

5. Únicamente los dueños de procesos estratégicos, misionales o de apoyo, de acuerdo al mapa de procesos de la entidad, pueden ejercer el rol de propietarios de activos de información. En este caso el propietario es el encargado de tomar las decisiones claves sobre dicho activo y se apoya en el custodio para su protección en términos de seguridad.

6. Los Colaboradores que ejercen el rol de custodios de algún activo de información, actúan como responsables de proteger el activo en términos de confidencialidad, integridad y disponibilidad, por lo tanto, debe informarse acerca de las medidas necesarias para proteger el activo.

6.2.2 Seguridad de la información en gestión de proyectos

Directrices

1. La metodología de gestión de proyectos empleada por la entidad debe considerar la seguridad de la información como un componente transversal y por lo tanto debe incluirla desde el inicio del proyecto y durante su ejecución. Esto aplica a cualquier tipo de proyecto.

2. Como parte de los objetivos definidos para los proyectos desarrollados, se deben incluir objetivos de seguridad de la información acordes con la información que va a ser manejada a lo largo del proyecto.

3. En las etapas iníciales de un proyecto como parte de los riesgos asociados al proyecto, se debe incluir una identificación y evaluación de riesgos de

seguridad de la información, para los cuales se deben definir controles de seguridad que aporten a su mitigación.

La responsabilidad sobre la implementación y la efectividad de los controles de seguridad aplica sobre el gerente de proyectos o supervisor del contrato de implementación.

6.2.3 Política de Dispositivos Móviles

Objetivo

Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

Directrices

1. El uso de los equipos portátiles de propiedad de la entidad fuera de las instalaciones, únicamente se permitirá a usuarios autorizados mediante una orden de salida, la cual debe tener el visto bueno del delegado de los procesos con firma autorizada para este fin.

2. Los equipos que estén autorizados para salir y que contengan información sensible, se deben proteger mediante el uso de uno o varios de los siguientes controles tecnológicos:

   - ✓ Antivirus.
   - ✓ Cifrado de datos.
   - ✓ Restricción en la ejecución de aplicaciones.
   - ✓ Restricción de conexión de dispositivos USB.
   - ✓ Protección física mediante la guaya de seguridad.
   - ✓ Desactivar accesos inalámbricos cuando se encuentren conectadas a la red LAN

3. Cualquier dispositivo móvil que albergue información de la entidad debe poseer un sistema de autenticación, basado al menos en un patrón de movimiento, un código de desbloqueo o una contraseña.

4. Cualquier dispositivo móvil que albergue información de la entidad debe tener instalado un software de antivirus.

5. Los dispositivos móviles que son propiedad de la entidad pueden estar sometidos a un control sobre el tipo y la versión de aplicaciones instaladas, al igual que pueden estar sometidos a restricciones de conexión hacia ciertos servicios de información que sean considerados maliciosos.

6. Los dispositivos móviles que son propiedad de los funcionarios, pueden tener almacenada información de la entidad, como el correo electrónico, siempre y cuando dichos equipos se encuentren registrados e identificados y se implementen las medidas de aseguramiento para garantizar la preservación de la confidencialidad e integridad de la información de la entidad.

7. En caso de pérdida o robo de un dispositivo móvil que contenga información de la entidad, el funcionario a cargo del dispositivo móvil, debe avisar inmediatamente al grupo de trabajo de Soporte o sistemas, quien está en libertad para iniciar un proceso de borrado remoto de información.

6.2.4 Política de Teletrabajo

Objetivo

Proteger la información de la entidad accedida desde lugares donde se realiza teletrabajo.

Directrices

1. Las solicitudes de acceso remoto a equipos de cómputo o servicios de procesamiento de información de la red interna de la entidad, deben contar con el aval del propietario del proceso al cual pertenece el funcionario solicitante del acceso.

2. Las solicitudes de acceso remoto serán configuradas principalmente para acceder por escritorio remoto únicamente al equipo de escritorio que ha sido designado al funcionario en las instalaciones de la entidad, evitando de esta forma el procesamiento y almacenamiento de información de la entidad en equipos de terceros. En la situación, en la que el funcionario no cuente con un equipo de escritorio en las instalaciones de la entidad, se habilitarán accesos a servicios de procesamiento de información individuales, basados siempre en una justificación de la necesidad de acceso.

3. Las solicitudes de acceso remoto a equipos de cómputo diferentes del equipo de escritorio que ha sido designado al funcionario en las instalaciones de la entidad, deben contar con la aprobación del propietario del activo de tipo información primario almacenado en el equipo de cómputo al cual se desea tener acceso, por ejemplo para el acceso remoto a un servidor de inteligencia de negocios, se debe contar con la aprobación del funcionario que hace las veces de propietario de la información almacenada en dicho servidor.

4. Las solicitudes de acceso remoto a equipos de cómputo o servicios de procesamiento de información deben indicar siempre un tiempo de duración del acceso remoto, siendo tres (3) meses el tiempo máximo para una solicitud. En caso de que este tiempo no se especifique, se asumirá un tiempo de duración del acceso remoto de una (1) semana.

5. Posterior al tiempo de duración del acceso remoto, el acceso remoto será revocado hasta que se haga una nueva solicitud de acceso. La revocación exige la creación de unas nuevas credenciales de acceso para el usuario solicitante.

6. Los accesos remotos se deben configurar considerando siempre: conexiones cifradas, tiempos de sesión y autenticación a nivel de usuario. Para este propósito, el mecanismo autorizado son conexiones de tipo VPN (Virtual Private Network).

7. El funcionario solicitante del acceso remoto es responsable del uso indebido o no autorizado que se haga con el acceso remoto que le ha sido designado, incluyendo el que realicen otros usuarios con acceso al equipo de cómputo desde el cual se hace el acceso remoto.

8. La entidad tiene potestad para verificar las características operativas y de seguridad de equipos de cómputo de terceros desde los cuales se hace el acceso remoto. En caso de encontrarse condiciones no óptimas, el acceso remoto puede ser negado o revocado, indicándose la justificación que condujo a dicha decisión.

9. Los accesos remotos están sujetos a monitoreo, el cual incluye hora y duración de la conexión, datos transmitidos o recibidos hacia o desde la infraestructura de la entidad, direcciones IP de origen de la conexión, etc.

10. El usuario solicitante deberá recibir las indicaciones adecuadas para hacer la correcta instalación del software requerido para el acceso de tipo VPN.

6.3 SEGURIDAD DE LOS RECURSOS HUMANOS

Política de Seguridad de los recursos humanos

Objetivo

Asegurar que los empleados y contratistas comprenden las responsabilidades y son idóneos en los roles para que los consideran.

Directrices

1. Dentro de los procesos de contratación de personal o de prestación de servicios, deberá realizarse la verificación de antecedentes cuando así lo amerite y en los casos que se considere necesario se debe contemplar la realización del estudio de seguridad. Esto aplica especialmente cuando el Colaborador vaya a tener acceso a información de la entidad que haya sido clasificada como CONFIDENCIAL o RESERVADA.

2. El grupo de Talento Humano es el responsable de realizar la verificación de antecedentes, para lo cual puede llevar a cabo cualquiera de las siguientes actividades: verificación de referencias personales y laborales, validación de la hoja de vida del aplicante, confirmación de calificaciones académicas y profesionales, revisión de documentación de identidad alterna (pasaporte, tarjeta de conducción, etc.), revisión de antecedentes criminales, etc.

3. Todos los Colaboradores de la entidad debe cumplir con los requerimientos de seguridad de la información y estos debe hacer parte integral de los contratos o documentos de vinculación a que haya lugar, para ello se firmará el documento Acuerdo Individual de Confidencialidad (Ver Formato Acuerdo Individual de Confidencialidad) donde se evidencie el conocimiento y aceptación del documento “Documento de Políticas y Lineamientos de seguridad de la información”.

4. Todos los Colaboradores, durante el proceso de vinculación a la entidad, deberán recibir una inducción sobre las Políticas de Seguridad de la Información.

5. Los Colaboradores de la entidad deben ser entrenados y capacitados para las funciones/actividades y cargos a desempeñar con el fin de proteger adecuadamente los recursos y la información de la institución; y garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente. En los casos en que así se establezca, este entrenamiento deberá extenderse al personal de contratistas o terceros, cuando sus responsabilidades así lo exijan.

6. A todos los incidentes de seguridad de la información ocurridos en la entidad se le debe dar el tratamiento respectivo con el fin de determinar sus causas y responsables. De los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta la gravedad y responsabilidades identificadas, se tomarán acciones y se realizará el respectivo trámite ante las instancias correspondientes.

6.4 CONTROL DE ACCESO

Política de Control de Acceso

Objetivo

Limitar el acceso a información y a instalaciones de procesamiento de información.

Directrices

1. La entidad suministra a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

2. Solo personal designado por el Grupo de Trabajo de Soporte o sistemas está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la entidad.

3. Todo trabajo que requiera acceder a los servidores, equipos o a las redes de la entidad, se debe realizar en las instalaciones. No se podrá realizar ninguna actividad de tipo remoto sin la debida autorización del Grupo de Soporte o sistemas.

4. La conexión remota a la red de área local de la entidad debe ser hecha a través de una conexión VPN segura suministrada por la entidad, la cual debe ser autorizada por el Grupo de Trabajo de Soporte o sistemas.

5. Gestión de altas/bajas en el registro de usuarios: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

6. Gestión de los derechos de acceso asignados a usuarios: Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

7. Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

8. Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.

9. Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.

10. Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

6.5 POLÍTICA DE SEGURIDAD GESTIÓN DE CONTRASEÑAS PARA USUARIOS

Objetivo

Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

Directrices

1. Los usuarios deben acatar las políticas para el uso y selección de las contraseñas de acceso y por lo tanto son responsables de cualquier acción que se realice utilizando el usuario y contraseña de usuario que le sean asignados.

2. Las contraseñas son de uso personal y por ningún motivo se deberán prestar o compartir a otros usuarios.
3. Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

4. Las contraseñas no se deben escribir en ningún medio.

5. Reportar al correo autorizado para tal fin sobre cualquier sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

6. Reportar al correo autorizado para tal fin sobre cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.

7. Las contraseñas se deberán cambiar según los requerimientos establecidos por el Grupo de Trabajo de Soporte o sistemas.

8. El nombre del usuario debe estar compuesto por nombre. apellido, si hay más de un usuario con el mismo nombre y apellido se tomará la letra subsiguiente del segundo apellido.

9. Las contraseñas estarán compuestas al menos por: una letra mayúscula, números o caracteres especiales y su longitud debe ser de mínimo ocho (8) caracteres.

10. Los usuarios deberán cambiar las contraseñas la primera vez que usen las cuentas asignadas.

6.5.1 Revisión de los derechos de acceso de los Usuarios

Los derechos de acceso de los usuarios a la información y a la infraestructura de procesamiento de información de la entidad, deberán ser revisados periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

6.5.2 Retiro de los derechos de acceso

Directrices

1. Cada uno de los procesos de la Entidad serán los encargados de comunicar al grupo de Talento Humano, el cambio de cargo, funciones/actividades o la terminación contractual de los Colaboradores pertenecientes al proceso. El grupo de Talento Humano será el encargado de comunicar al Grupo de Trabajo de soporte o sistemas sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

6.6 POLÍTICA DE SEGURIDAD USO DE CONTROLES CRIPTOGRAFICOS

Objetivo

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o integridad de la información.

Directrices

1. Se contemplará la evaluación e implementación de controles criptográficos en la medida que un determinado servicio de procesamiento de información o acceso lo requiera. Se verificarán los medios y herramientas criptográficas que mejor se acoplen a las necesidades de la entidad.

2. Antes de la implementación del tipo de control criptográfico seleccionado, se debe definir y comunicar el procedimiento para la gestión de las llaves públicas o privadas, según el caso, entre las partes interesadas.

3. Las características de los controles criptográficos, incluyendo el tipo, fortaleza y calidad, al igual que las herramientas y mecanismos a emplear para implementar los controles, serán definidos por el Grupo de Trabajo de Soporte o sistemas en función de la clasificación de la información.

4. Se debe garantizar que el uso de controles criptográficos no entorpezca aquellos controles de seguridad basados en inspección de contenido, tales como filtrado web, antimalware, antispyware, etc. El Grupo de Trabajo de Soporte o sistemas deberá validar dicha condición y determinar las mejores condiciones de aplicabilidad de los controles criptográficos.

5. Los sistemas de información misionales que involucren accesos desde internet y que gestionen información de criticidad media o alta de acuerdo al inventario de activos de información, deben estar protegidos por un control de cifrado que garantice la confidencialidad, el no repudio y la integridad de los datos, por ejemplo, certificados digitales con claves públicas RSA.

6.7 SEGURIDAD FÍSICA Y DEL ENTORNO

6.7.1 Política de Seguridad Física y del Entorno

Objetivo

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

6.7.2 Perímetro de Seguridad Física

Directrices

1. Todos los ingresos que utilizan sistemas de control de acceso deben permanecer cerrados y es responsabilidad de todos los Colaboradores autorizados evitar que las puertas se dejen abiertas.

2. Se deberá exigir a todos los visitantes, sin excepción, el porte de la tarjeta de identificación de visitante o escarapela en un lugar visible. Así mismo, todos los Colaboradores deberán portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones de la entidad.

3. Los visitantes deberán permanecer acompañados de un Colaborador de la entidad, cuando se encuentren en las oficinas o áreas donde se maneje información.

4. Es responsabilidad de todos los Colaboradores de la entidad borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se deberán dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.
5. Los visitantes que requieran permanecer en las oficinas de la entidad por periodos superiores a dos (2) días deberán ser presentados al personal de oficina donde permanecerán.

6. El horario autorizado para recibir visitantes en las instalaciones de la entidad es de 8:15 AM a 5:15 PM. En horarios distintos se requerirá de la autorización del Director, Jefe de Oficina, Subdirector o Coordinador del Grupo correspondiente.

7. Los equipos portátiles, así como toda información CONFIDENCIAL de la entidad, independientemente del medio en que se encuentre, deberán permanecer guardados bajo llave durante la noche o en horarios en los cuales el Colaborador responsable no se encuentre en su sitio de trabajo.

6.7.3 Controles de Acceso Físico.

Directrices

1. Las áreas seguras, dentro de las cuales se encuentran el Centro de Cómputo, centros de cableado, áreas de archivo y áreas de recepción y entrega de correspondencia, deberán contar con mecanismos de protección física y ambiental, y controles de acceso que pueden ser mediante tarjeta de proximidad o puertas con cerradura.

2. En las áreas seguras, bajo ninguna circunstancia se podrá fumar, comer o beber.

3. Las actividades de limpieza en las áreas seguras deberán ser controladas y supervisadas por un Colaborador del proceso. El personal de limpieza deberá ser instruido acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohibirá el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

6.7.4 Ubicación y Protección de los equipos

Directrices

1. La infraestructura tecnológica (Hardware, software y comunicaciones) deberá contar con medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.
2. Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

7 CONCLUSIONES

A través del desarrollo de este documento se ha logrado concretar las principales características referentes a la gestión de identidades y el control de acceso; también se ha visto cómo una solución de este tipo puede ayudar a las organizaciones en el desarrollo de nuevas estrategias, el cumplimiento de normas y regulaciones. Así mismo se han abordado las acciones pertinentes para el mejoramiento del acceso seguro a la información y los recursos.

Es evidente que el desarrollo e implementación de un sistema de gestión de identidades y control de acceso implica de parte de las entidades una gran inversión de tiempo, dinero y recursos; pero a la postre puede evidenciarse la mejora en los procesos y disminución en algunos casos de carga laboral, así como un adecuado modelo que permite minimizar ciertos riesgos.

Se logró la identificación de algunos factores críticos que sugieren la necesidad de utilizar sistemas de gestión de identidades. La criticidad de esos factores dentro de la entidad es lo que realmente crea la necesidad de su implementación y uso, máxime cuando estos factores representan el éxito para la entidad.

El proceso de control de acceso, es de gran importancia para el logro los pilares de la seguridad de la información, como son integridad, disponibilidad, confidencialidad.

Se logró cumplir con los objetivos trazados tanto a nivel general como específicos, presentados de forma clara y en un lenguaje que permite a las personas que trabajan en tecnología el entendimiento de todo el documento.

La implementación de un sistema centralizado en el manejo de identidades y la aplicación de las políticas recomendadas en la norma ISO 27001 para desarrollar un sistema de gestión de seguridad de la información, permite a la entidad mostrarse a sus clientes y proveedores como garante de que su información está protegida a través de los diferentes procesos que evitan o disminuyen considerablemente los riesgos de fraude, filtración o pérdida de información, ya que permite formalizar las responsabilidades operativas y legales de los usuarios internos y externos de la Información y ayuda al cumplimiento de las disposiciones legales nacionales e internacionales.

Las entidades deberían implementar y poner en práctica como mínimo los controles y lineamientos presentados en este documento, para tener una buena gestión de usuarios, ya que solo una parte dejaría muchos vacíos que se puede reflejar en vulnerabilidades.

El sistema centralizado de gestión de identidades es un modelo de fácil aplicación y que cubre lo más relevante para la gestión de usuarios.

8 RECOMENDACIONES

Para que se pueda implementar un sistema centralizado de gestión de identidades que incluya las políticas y lineamientos contenidos en la norma ISO 27001 expuestos en el desarrollo de este documento es necesario tener en cuenta los siguientes aspectos:

- ✓ La Alta Gerencia de la entidad es quién debe liderar el proceso de implantación y mejora continua del SGSI en cada entidad.
- ✓ No es posible llevar a cabo la implementación exitosa de un Sistema de gestión de seguridad de la información sin el apoyo decidido de la alta gerencia.

La alta gerencia debe:

- ✓ Establecer y apoyar la política de seguridad de la información.
- ✓ Asegurarse de que se establecen objetivos y planes del SGSI en su entidad.
- ✓ Establecer roles y responsabilidades de seguridad de la información.
- ✓ Dar a conocer a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales, contractuales y la necesidad de mejora continua.

Una vez dadas a conocer las políticas a los usuarios; empleados, contratistas proveedores etc. Es obligación de estos:

- ✓ Recordar que las cuentas de acceso asignadas son de carácter personal e intransferible. Cada usuario es responsable por la actividad que se genere a partir de las cuentas que solicite y le sean asignadas.
- ✓ Solicitar el bloqueo de sus cuentas cuando vaya a suspender sus actividades por periodos largos de tiempo.
- ✓ Siempre bloquear su sesión de trabajo al dejar desatendido su computador. Evite que otro usuario realice cualquier actividad sobre su sesión de trabajo.

- ✓ Mantener la privacidad de sus contraseñas de acceso a la red y aplicaciones, evitando comunicarlas a terceros o escribiéndolas en lugares visibles o de fácil acceso. Si cree que sus contraseñas están en conocimiento de un tercero proceda a cambiarlas a la mayor brevedad posible.

- ✓ Use contraseñas que sean fáciles de recordar, pero difíciles de adivinar, tenga en cuenta las recomendaciones al momento de solicitar la creación de su cuenta de usuario.

- ✓ No mantenga contraseñas que le fueron suministradas como predeterminadas.

9 BIBLIOGRAFIA

ASAMBLEA NACIONAL Constituyente. Constitución Política de Colombia. Bogotá, 1991, art. 15

BISHOP 2003. Citado por Villalobos B. Refugio Propuesta de arquitectura de gestión de identidades digitales para el consorcio minero Benito Juárez. Colima 2012, p. 25

CALDERÓN B. GALO A. Estudio teórico de soluciones a la gestión centralizada de accesos a los sistemas mediante la aplicación de un sistema de gestión de identidades. Quito: Pontificia Universidad Católica del Ecuador. 2009

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (Agosto 18 de 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones Diario Oficial 43.673 del 21 de agosto de 1999. p. 1-15.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 594 (4 de julio de 2000). Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Diario Oficial No. 44.093, de 20 de julio de 2000

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581. (Octubre 17 de 2012, art. 1). Octubre 17 de 2000) Diario Oficial No. 48.587 de 18 de octubre de 2012

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1266. (Diciembre 31 de 2008). Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial No. 47.219 de 31 de diciembre de 2008

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (Enero 05 de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones Diario Oficial No. 47.223 de 5 de enero de 2009

Comisión de regulación de las comunicaciones.(19 de mayo de 2010) Por la cual se modifican los artículos 1o, 78, 79 y 86 de la Resolución CRT 1732 de 2007, y se deroga el artículo 85 de la Resolución CRT 1732 de 2007 y la Resolución CRT 1890 de 2008.Diario Oficial No. 47.715 de 20 de mayo de 2010

CONSEJO EUROPEO Convenio 108 del Consejo de Europa, de 28-1-1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.Ratificado por España el 27 de enero de 1984 (entró en vigor de forma general el 1 de octubre de 1985, de conformidad con lo establecido en el artículo 22.2 del mismo Boletín Oficial del Estado núm. 274, de 15 de septiembre de 1985

HURTADO DE BECERRA, J. Metodología de la investigación holística. Caracas Venezuela: Sypal, 2000.

IAM: Administración de identidades de acceso (Identify and Access Management)

Instituto Colombiano de normas técnicas y certificación, ICONTEC. Norma Técnica NTC-ISO.IEC 27001.Bogotá. 2013

MONTOYA S., José RESTREPO, Zuleima Gestión de identidades y control de acceso desde una perspectiva organizacional. USBMed, Vol. 3, No. 1, pp. 23-34. 2012

PALAZÓN R. Antoni, FELGUERA Jordi y CASTELLÀ Jordi. Single sign-on y federación de identidades. Cataluña UOC 2008.

PARLAMENTO Y CONCEJO EUROPEO Directiva La Directiva 95/46/CE. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales Diario Oficial de las Comunidades Europeas, DO L 281, 23/11/1995)

PARLAMENTO EUROPEO Y CONSEJO REGLAMENTO (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos Diario Oficial de la Unión Europea L 119/1 de 27 de abril de 2016

PRESIDENCIA DE LA REPÚBLICA. Manual de la política de seguridad para las tecnologías de la información y las comunicaciones – TICS. Versión 5. Bogotá D.C. 2014.

PRESIDENCIA DE LA REPÚBLICA Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581 con el fin de facilitar su implementación y cumplimiento en aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas. Diario Oficial 48834 de junio 27 de 2013

Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. BOE núm. 147, de 21 de junio de 1994

10 WEBGRAFIA

DOMINGO, Ignacio Alamillo; i Aparisi, Xavier Urios; En: la gestión de identidades y capacidades por las administraciones públicas. [Pág. 3]. Diciembre 2004. Consultado mayo. 30 de 2006]. Disponible en Internet: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Tecnimap/pae_TECNIMAP_2006/pae_TECNIMAP_2006_Comunicaciones_Presentadas_-_5/gestion_de_identidades.pdf

ECURED Sistemas de control Consultado 22-11-2016. Disponible en https://www.ecured.cu/Sistemas_de_control_de_acceso

GILARD IGLESIAS, Ignacio. Por qué implantar un sistema de gestión de identidad open source: WBS Visión. En: White Bear Solutions genuinely open (WBSgo). [En línea]. Octubre 2015. [Consultado oct. 15 de 2015]. Disponible en http://www.whitebearsolutions.com/por-que-implantar-un-sistema-de-gestion-de-identidad-open-source-wbsvision/

HITACHI ID SYSTEM. Definition of Enterprise Single Sign-On (E-SSO) [En línea]. 2015. [Consultado oct 10 de 2015]. Disponible en: http://hitachi-id.com/concepts/esso.html

IBM Gestión de identidades y accesos para el cumplimiento continuado y la reducción del riesgo. Consultado 22-11-2016. Disponible en http://docs.media.bitpipe.com/io_10x/io_107393/item_607564/Q4_SWG%20Network%20Security_1162_ES_002_Gestion%20de%20Identidades.pdf

JUMMP. Desarrollo de software. Sistema de gestión de identidades [En línea]. Mayo 2011. [Consultado sep. 21 de 2015]. Disponible en https://jummp.wordpress.com/2011/05/04/desarrollo-de-software-sistema-de-gestion-de-identidades/

MARRERO RODRÍGUEZ, Raúl. Sistema centralizado de gestión de usuarios para Innova 7. La Laguna, 2014, p. 4. Trabajo de Grado. (Ingeniería Informática). Universidad de La Laguna. Departamento de Ingeniería Informática.

MONTEJO Juan C., HERRERA Hair diseño de un modelo que permita el manejo de identidades de un usuario dentro de una organización. Disponible en http://repository.unad.edu.co/bitstream/10596/6168/1/79556048.pdf

ORACLE. Guía de administración del sistema: servicios de seguridad. México. 2011. Disponible en Internet: https://docs.oracle.com/cd/E24842_01/html/E23286/intro-5.html
https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

ORACLE Introducción a Oracle Identity Management. Consultado 22-11-2016.Disponible en: http://www.oracle.com/technetwork/es/documentation/317540-esa.pdf

PAPERCUT SOFTWARE INTERNATIONAL PTY LTD. Web Browser Single Sign-on (SSO) [En línea]. 2015. [Consultado oct 15 de 2015]. Disponible en http://www.papercut.com/products/ng/manual/ch-sso.html

PRISE Identidad digital. Consultado 23-11-2016.Disponible en https://www.prise.es/es/services/digid/cons/

REFUGIO, J. y VILLALOBOS, B. Jefatura de Tecnología de Información en Consorcio Minero Benito Juárez Peña Colorada, México, 2004, p.13
Transforming IT Management Guía de usuario: administración de identidades y accesos 2007:6. Consultado 21-11-2016. Disponible en http://www.calatam.com/mails/docs/iam_buyers_guide_es.pdf

ROUSE, Margareth. Single sign-on (SSO) definition [En línea]. En: TechTarget. 2015. [Consultado oct. 02 de 2015]. Disponible en http://searchsecurity.techtarget.com/definition/single-sign-on

Sumner Blount, Merritt Maxim CA Security Management. El rol de la administración de identidades y accesos para lograr un cumplimiento continuo 2012:9. Consultado 22-11-2016. Disponible en http://www.arcserve.com/ar/~/media/Files/whitepapers/latam/CS1933_Continuance Compliance_WP_0212_LAS.pdf

VILLALOBOS B. refugio. Propuesta de arquitectura de gestión de identidades digitales para
el consorcio minero Benito Juárez. Consultado 23-11-2016.Disponible en http://digeset.ucol.mx/tesis_posgrado/Pdf/Refugio_Javier_Villalobos_Becerra.pdf

WIKIPEDIA. Autenticación [En línea]. Oct. 2015. [Consultado oct. 21 de 2015]. Disponible en https://es.wikipedia.org/wiki/Autenticaci%C3%B3n
www.scoop.it/doc/download/cvdXLLFB5B3H35NMF97_qdw. Recuperado 11-05-2016

https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA, Recuperado 11-05-2016

http://fccea.unicauca.edu.co/old/siconceptosbasicos.htm