PROPUESTA DE UN MODELO PARA EL CONTROL DE ACCESO LÓGICO EN LA CAPA DE APLICACIÓN DE LOS SISTEMAS DE INFORMACIÓN, CON LA IMPLEMENTACIÓN DE UN CASO DE ESTUDIO EN UN MÓDULO DEL SISTEMA SAP

LUIS GABRIEL MARTÍNEZ UPEGUI

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN
MEDELLÍN
2018

PROPUESTA DE UN MODELO PARA EL CONTROL DE ACCESO LÓGICO EN LA CAPA DE APLICACIÓN DE LOS SISTEMAS DE INFORMACIÓN, CON LA IMPLEMENTACIÓN DE UN CASO DE ESTUDIO EN UN MÓDULO DEL SISTEMA SAP

LUIS GABRIEL MARTÍNEZ UPEGUI

Trabajo de grado para optar al título de Magíster en Tecnologías de la Información y la Comunicación

Director

M.Sc. CESAR AUGUSTO LÓPEZ GALLEGO

Magíster en Ingeniería de Sistemas
Especialista en Teleinformática
Ingeniero de Sistemas

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN
MEDELLÍN
2018

DECLARACIÓN ORIGINALIDAD

"Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad". Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

FIRMA AUTOR (ES) 

Medellín 5 de septiembre de 2018

Tabla de contenido

Lista de Tablas

Lista de Figuras

1 Título

PROPUESTA DE UN MODELO PARA EL CONTROL DE ACCESO LÓGICO EN LA CAPA DE APLICACIÓN DE LOS SISTEMAS DE INFORMACIÓN, CON LA IMPLEMENTACIÓN DE UN CASO DE ESTUDIO EN UN MÓDULO DEL SISTEMA SAP.

2 Resumen ejecutivo

Se realizó la aplicación de un modelo para el control de acceso lógico en el sistema SAP S/4 Hana basado en estándares internacionalmente aceptados.

La etapa inicial fue un entendimiento de las necesidades de la empresa, donde se validó la unificación de criterios de seguridad para controlar el acceso lógico al sistema en la capa de aplicación.

En conjunto con el área de auditoría de la empresa, se realizó la categorización del sistema de acuerdo con el estándar (FIPS PUB 199, 2004) publicado por el NIST..

El resultado de la categorización del sistema SAP S4 Hana fue Moderado, debido a que en este sistema se registra toda la información financiera y la evaluación de este, hace parte de la opinión de la revisoría fiscal, la cual es entregada cada año en la asamblea de accionistas.

Un compromiso de la seguridad del sistema tendría un efecto adverso serio, debido a que podrían presentarse pérdidas financieras, conllevando a una opinión negativa por parte de la revisoría fiscal, dando como resultado una devaluación en el precio de la acción en el mercado de valores.

De acuerdo con el resultado y con base en el modelo, se seleccionaron los controles para un sistema con categoría Moderado, se revisó con el área técnica y de seguridad informática los controles disponibles en el sistema, se analizó el impacto de activarlos y el esfuerzo en la definición de los lineamientos de operación de los mismos. Asimismo, se identificaron los controles que no posee el sistema y deben ser establecidos, para los cuales se estableció un plan de acción para su implementación.

Durante la fase de pruebas del proyecto, se realizaron pruebas sobre la implementación de los controles disponibles en el sistema.

Los responsables de la seguridad del sistema SAP, incorporaron en sus procesos los controles seleccionados, y el área de auditoría interna incluyó en su plan anual de auditoría la revisión del funcionamiento de los controles de acceso lógico definidos.

3 Identificación del sitio de práctica

Este trabajo se desarrolló en una empresa del sector energético con sede en Medellín y presencia en Colombia y Centroamérica con un total de 1557 colaboradores, la cual participa en actividades de generación, transmisión, distribución y comercialización de energía. El modelo fue implementado durante la ejecución del proyecto Sapiencia que consiste en la implementación del sistema SAP S4 Hana.

La empresa incursiona en nuevos negocios con un innovador portafolio de energía para diferentes segmentos: ciudades, empresas y hogares. En el negocio de generación tiene presencia en Colombia y Centroamérica con centrales hidroeléctricas, térmicas, fotovoltaicas y eólicas. En los negocios de transmisión y distribución cuenta con subestaciones y redes de alta, media y baja tensión. Por su parte, en el negocio de comercialización atiende a 600.000 clientes con una red

de oficinas comerciales, puntos de pago y atención telefónica.

El grupo de humano que participó en el proyecto de implementación fue:

- Equipo de seguridad SAP: Giovanni Ocampo y Juan Camilo Garibello
- Equipo técnico SAP Basis: Danilo Erick y Eli Ramones
- Equipo funcional módulo FI: Claudia Botero y Luceny Acevedo
- Auditoría interna: Luis Gabriel Martínez
- Líder del proyecto: Martha Lucia Loaiza

4 Justificación

Los controles de acceso lógico tienen como objetivo restringir y limitar el acceso a la información y para su adecuado funcionamiento se deben implementar procedimientos formales para controlar la asignación de usuarios y privilegios, y a su vez estos deben estar documentados, comunicados y controlados para verificar su cumplimiento.

Los accesos tienen un ciclo de vida, por lo cual estos procedimientos deben incorporar las diferentes etapas del mismo, desde el comienzo con el análisis y registro inicial de un nuevo usuario, hasta la inhabilitación del mismo y retiro de los privilegios cuando estos ya no son requeridos.

Los controles deben garantizar el cumplimiento de los componentes de la seguridad informática: confidencialidad, integridad, disponibilidad y auditabilidad.

Este modelo considera los siguientes elementos:

- Administración de usuarios
- Controles de sesión y contraseñas

- Administración de roles y perfiles
- Segregación de funciones
- Aseguramiento del proceso

5 Objetivos

5.1 Objetivo General

Elaborar un modelo de control de acceso lógico a nivel de aplicación para los sistemas de información, con la implementación de un caso de estudio en un módulo del sistema SAP.

5.2 Objetivos Específicos

- Realizar la categorización del sistema de información SAP S/4 Hana.
- Diseñar los controles de acuerdo con la categorización de sistema.
- Aplicar el modelo de control de acceso lógico a nivel de aplicación para los sistemas de información en el módulo financiero del sistema SAP S/4 Hana.

6 Estudio del contexto

A continuación, se establece el entorno donde se va a realizar el trabajo, haciendo una breve descripción de los aspectos regulatorios y legales que aplican junto con el estado del arte de la normativa de dos de los organismos internacionales líderes en la emisión de estándares.

6.1 Marco contextual

La tendencia de las organizaciones para desarrollar su estrategia es soportar sus procesos en sistemas de información y nuevas tecnologías, buscando integrar

todas sus operaciones y actividades manteniendo la capacidad de adaptarse rápidamente a los cambios de mercado y a nuevas necesidades.

El control de acceso es un proceso mediante el cual el uso de los recursos del sistema se regula con una política de seguridad y es permitido solamente a aquellos entes autorizados (usuarios, programas, procesos u otros sistemas) de acuerdo con dicha política. (Shirey, 2007)

El control de acceso lógico en las organizaciones es complejo, se requieren diversos tipos de usuarios, la información tiene diferentes niveles de confidencialidad y el entorno corporativo es dinámico y cambia continuamente.

Un proceso de control de acceso bien definido es esencial para garantizar accesos autorizados, lo cual permite tener seguridad sobre los activos y operatividad del negocio, lo cual se conoce en la literatura como balance entre seguridad y utilidad (R. Kainda, I. Flechais, & A. Roscoe, 2010) (Zapata, 2013).

Según la Encuesta Global de Seguridad de Información “Adelántese a los delitos cibernéticos” realizada en 2014 por EY, los principales problemas identificados en el componente del acceso a los datos son:

- Los empleados son un potencial riesgo para la seguridad cibernética de una empresa, su programa de gestión de identidades y accesos es débil.
- Procesos manuales excesivos, revisiones irregulares o reportes inadecuados facilitan que los empleados puedan tener acceso a la información confidencial de manera inapropiada.
- La rotación de personal y empleados es un riesgo clave para la seguridad cibernética. (EY, 2014)

Informes formales basados en incidentes de seguridad emitidos por diversas

organizaciones que realizan investigación de violaciones de seguridad confirman el impacto causado por diferentes eventos de compromiso de datos. Uno de los informes de seguridad más relevante debido a su alta cobertura y gran cantidad de incidentes y brechas de seguridad confirmadas es el informe DBIR (Data Breach Investigation Report) de Verizon (Verizon Enterprise, 2015), el cual tiene una periodicidad anual y se construye con los reportes de incidentes de seguridad de 70 organizaciones globales de 61 países.

De los diferentes tipos de incidentes considerados en este reporte, se destaca el "uso indebido de privilegios e información", que corresponde a un uso malicioso y no aprobado de los recursos organizacionales, el cual puede ser originado por cualquiera de los actores (entes): internos, externos (por conspiración) o asociados empresariales. Este tipo de incidente puede ser causado por diferentes amenazas, pero de acuerdo con los informes 88% en el 2013 y 55% en el 2014 de los iniciadores de este tipo de incidente fueron "acciones de abuso de privilegios" que corresponde a usar algunos privilegios otorgados (debido a una relación laboral o de asociación) para cometer actos maliciosos.

En la Encuesta Global de Seguridad de Información “Crear confianza en el mundo digital” realizada en 2015 por EY, se catalogaron los riesgos y las amenazas de personas con información privilegiada como de prioridad media, a pesar de que el 56% considera que los empleados son una de las fuentes más probables de un ataque, y 36% señala a los contratistas externos como una fuente factible (EY, 2015).

En el mercado existen varios estándares de seguridad publicados como por ejemplo (ISO/IEC 27001:2013) y (NIST SP 800-53, Revision 4, 2015), sin embargo, la implementación de estos se ha tornado compleja debido a la adaptación que se debe hacer de acuerdo a las necesidades de cada organización.

6.2 Marco conceptual

A continuación, se presentan las definiciones y conceptos de acuerdo con cada uno de los organismos internaciones que realizan la emisión de estándares y que son necesarios para el entendimiento de la investigación:

NIST: Instituto Nacional de Normas y Tecnología con sus siglas en inglés, National Institute of Standards and Technology), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida. La FISMA (Federal Information Security Management Act) de Estados Unidos, otorgó al NIST, el desarrollo de un conjunto de documentos SP-800 con el objetivo de proveer un marco de referencia completo a la gestión de la seguridad de la Información, para que sea aplicado en forma obligatoria por las agencias norteamericanas.

ISO: es la organización Internacional de Estándares ISO con sus siglas en inglés, International Organization for Standardization, su finalidad principal es la de promover el desarrollo de estándares internacionales y actividades relacionadas incluyendo la conformidad de los estatutos para facilitar el intercambio de bienes y servicios en todo el mundo.

Control de acceso: propiedad de asegurar que el acceso a los activos es autorizado y restringido con base los requerimientos del negocio y de seguridad (ISO/IEC 27000:2016)

Seguridad de la Información: de acuerdo a ISO se define como la preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27000:2016) y para el NIST es la protección de la información y los sistemas de

información del acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción y con el fin de proporcionar confidencialidad, integridad y disponibilidad (NIST SP 800-53, Revision 4, 2015).

Confidencialidad: La preservación de las restricciones autorizadas al acceso de información y divulgación, que incluye medios para la protección de la intimidad personal y propiedad de la información (FIPS PUB 199, 2004) y para ISO es la propiedad de que la información no es disponible o divulgada a individuos, entidades, o procesos no autorizados (ISO/IEC 27000:2016)

Integridad: Protección contra la inadecuada modificación o destrucción de información, e incluye garantizar que el no repudio y la autenticidad de la (FIPS PUB 199, 2004). Una pérdida de la integridad es la modificación o destrucción de información no autorizada, mientras que para ISO es la propiedad de exactitud y completitud. (ISO/IEC 27000:2016)

Disponibilidad: Garantizar el acceso oportuno y confiable y uso de la información (FIPS PUB 199, 2004) y para ISO es la propiedad de ser accesible y utilizable a petición de una entidad autorizada (ISO/IEC 27000:2016).

SAP: es un sistema del tipo ERP (Enterprise Resource Planning), por lo que es un sistema integrado con aplicaciones de gestión empresarial y que tiene como objetivo cubrir los principales procesos funcionales de una organización (ventas, compras, contabilidad, nómina, entre otros) generando flujos de información y trabajo en el mismo sistema.

Transacción SAP: acceso a la ejecución de un programa en el sistema, cuya finalidad es realizar una operación o tarea definida.

Rol compuesto: rol de seguridad SAP encargado de agrupar roles, que permiten asignar a uno o varios usuarios un grupo de tareas específicas, usualmente asociadas a un cargo.

Rol maestro/padre: rol de seguridad SAP encargado de agrupar transacciones (no objetos de autorización de unidad organizacional) que poseen un sentido común orientado a desarrollar una tarea o función determinada. Rol considerado plantilla y no asignable al usuario final.

Rol derivado: rol de seguridad SAP derivado de un padre, encargado de alojar transacciones y objetos de autorización de carácter organizacional en unidades específicas, que permite segmentar las funciones de los roles simples sobre cada una de las unidades de negocio.

Actividad SAP: unidad mínima en funciones específicas de los usuarios en el sistema, asociado a una o varias transacciones.

Objeto de autorización: es el método técnico en unidades de agrupación dentro en un rol SAP, que permiten al usuario realizar actividades específicas en sectores definidos. El objeto de autorización se compone de campos que alojan los parámetros autorizados de la aplicación.

6.3 Marco legal

Como buenas prácticas en las organizaciones se han implementado requerimientos asociados a leyes y regulaciones que son propias de algunos países, a continuación, se menciona una de ellas.

SOX, abreviatura para Sarbanes Oxley Act es una ley americana que fue emitida en el 2002 en los Estados Unidos, como respuesta por parte del gobierno

estadounidense a los escándalos financieros ocurridos durante los años 2001 y principios del 2002 en su territorio. El nombre de la ley se deriva de los apellidos de sus dos principales patrocinadores, el diputado Michael G. Oxley y el senador Paul S. Sarbanes. El objetivo principal de la Ley es proteger a los inversionistas, a partir de la estructuración de un marco de requerimientos enfocados en aumentar el nivel de confiabilidad de la información financiera suministrada por los entes económicos y sancionar a los ejecutivos que cometan fraudes corporativos

Las entidades sometidas al cumplimiento de esta Ley, son aquellas empresas públicas registradas ante la Securities and Exchange Comission (SEC) en los Estados Unidos.

En el año 2008 en Colombia se expidió la (Ley 1266 de 2008) conocida como Ley de Hábeas Data Financiero, por la cual se dictan las disposiciones generales del Hábeas 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.

En Colombia mediante la (Ley 1273 de 2009) se incluyó la tipificación de los delitos informáticos al Código Penal Colombiano, en el Artículo 269A de esta Ley se determina el acceso abusivo a un sistema informático mencionando lo siguiente: “El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes”.

A nivel de protección de datos personales, en Colombia mediante la (Ley 1581 de 2012) y el (Decreto 1377 de 2013), se describen entre otras disposiciones:

derechos y condiciones de legalidad para el tratamiento de datos personales, deberes de los responsables y encargados del tratamiento, procedimientos para ejercer los derechos del ciudadano, la definición y responsabilidades de la Autoridad de Protección de Datos Personales, sanciones, el Registro Nacional de Bases de Datos (RNBD) y la transferencia de datos a terceros países.

En España existe la Ley Orgánica de Protección de Datos (LOPD) la cual regula los aspectos relativos al tratamiento de datos personales y su libre circulación. Se resalta de ella la descripción de los derechos de acceso, rectificación, cancelación y oposición que tienen los individuos sobre los datos personales, comúnmente llamados derechos ARCO.

En Latinoamérica el primer país en expedir una ley contra los delitos informáticos fue Chile con la Ley 19.223 del 28 de Mayo de 1993, la cual consta de cuatro artículos en los que se castigó conductas ilícitas como: la inutilización o destrucción de un sistema de tratamiento de información o sus componentes afectando el correcto funcionamiento del sistema, al igual que la interferencia, intercepción o acceso a un sistema de información con el fin de apoderarse de datos almacenados en el mismo, también sancionó el daño o destrucción de datos, así como la revelación o difusión de datos contenidos en un sistema de una manera malintencionada.

6.4 Estado del arte

Dado el significante y creciente peligro de amenazas relacionadas con el acceso a los sistemas de información, es fundamental que las organizaciones sensibilicen la importancia de lograr una seguridad de la información adecuada y realizar una gestión de riesgos de seguridad de estos sistemas.

Con el fin de aplicar un proceso de control de acceso para regular privilegios sobre activos, existen hoy en día algunos modelos de control de acceso (NIST/NSA Privilege Access Management Workshop Collaboration Team, 2010), cada uno con diferente complejidad y características, por ejemplo: listas de control de acceso (ACL), control de acceso basado en roles (RBAC), control de acceso basado en atributos (ABAC), control de acceso basado en políticas (PBAC) y control de acceso adaptable al riesgo (RAdAC). Estos modelos de control de acceso se encargan de procesar solicitudes de control de acceso y generar decisiones de autorización. Los beneficios de cada modelo hacen de algunos de ellos los más apropiados para algunas situaciones por encima de otros.

Los sistemas de control de acceso son un tópico importante de investigación, sobre el cual la comunidad científica se encuentra trabajando y el cual fue específicamente apoyado en la octava edición del programa para la investigación y el desarrollo tecnológico "Horizon 2020" por parte de la Unión Europea (European Comission, 2014). El tópico de control de acceso ha sido considerado dentro del desafío "sociedades seguras", enfocado en la protección de ciudadanos, sociedad, economía, activos europeos, infraestructura y servicios (European Comission, 2017).

NIST publicó un marco para mejorar la ciberseguridad en infraestructuras críticas (NIST, 2014), el cual emergió a través de la orden ejecutiva 13636 en la política de los Estados Unidos para mejorar la seguridad y resistencia de las infraestructuras críticas nacionales. Este programa tiene como propósito la definición de estándares y mejores prácticas para ayudar a organizaciones americanas a manejar riesgos de seguridad. Dentro de este programa, el control de acceso y la gestión de riesgos tienen un lugar especial en el desarrollo de la protección como una función clave.

ISO ha desarrollado una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información (ISO/IEC 27002:2013), el dominio número 9 es de Control de Accesos, allí se plantean los objetivos de control y sus respectivos controles para gestionar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Se encontraron nuevos enfoques para la implementación de un modelo de control de acceso basado en roles, siguiendo las especificaciones de la norma IEC 62351 y utilizando XACML como lenguaje estándar para la descripción de las políticas de control de acceso.

En el artículo *Role-based access control for substation automation systems using XACML.* (Lee B., 2015) plantea la necesidad de acceder desde sistema externos a datos en los equipos internos y dispositivos en una subestación. Para ello implementaron este modelo en los sistemas de automatización de las subestaciones de una red eléctrica avanzada. Como resultado los autores concluyeron que el modelo planteado es flexible y permitiría futuras ampliaciones, asimismo gracias a la estabilidad de los elementos del modelo de control de acceso basado en roles en el sistema de subestación, se espera un impacto mínimo por futuros cambios en las políticas de acceso en el entorno de producción.

En el artículo *Extended access control and recommendation methods for enterprise knowledge management system,* (Wang H., Guo X., Fan Y., Bi J., 2014) proponen un método de control de acceso basado en roles extendido para superar las deficiencias al implementar un control de acceso basado en roles tradicional en un sistema de gestión de conocimiento en empresas de gran tamaño. Este caso de estudio se aplicó a una empresa con departamentos y organizaciones virtuales, e incluyeron el concepto de grupos en el modelo. Al establecer conexiones entre el

usuario y la función, así como entre el usuario y el grupo, el modelo extendido conserva las funciones principales del control de acceso basado en roles y facilita la administración. Con el objetivo de lograr restricciones a nivel de funciones del sistema y a la información que deben acceder, introducen una estructura de tres capas (usuarios, roles y grupos). En la capa de grupos se restringe el acceso a la información mientras que en los roles se restringen las funciones del sistema y los usuarios se clasifican en internos y externos.

6.5 Metodología y Alcance

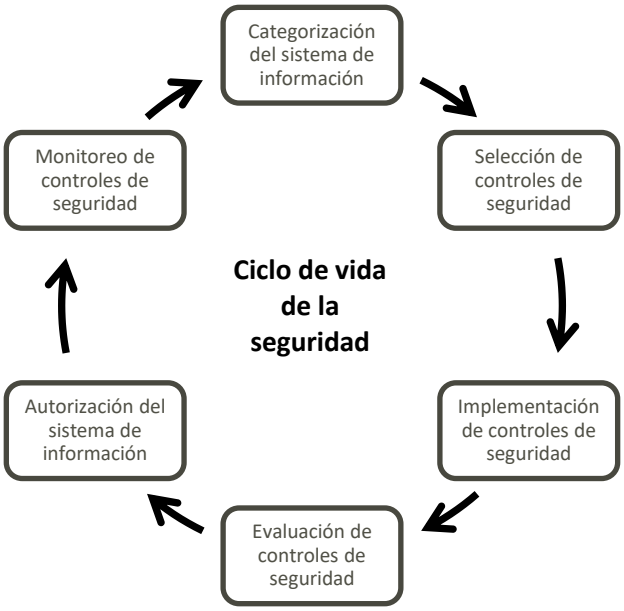
Para el desarrollo de este trabajo se tuvo en cuenta la metodología utilizada en el ciclo de vida de la seguridad (NIST SP 800-37, Revision 1, 2014) del NIST, cuyos estándares son ampliamente utilizados en las empresas y proveedores del gobierno de Estados Unidos.

Con base en esta metodología, se estableció la categoría de acuerdo con el nivel de riesgo establecido de cada sistema. Posteriormente se establecieron los controles y los procedimientos para la implementación y administración de los mismos, y finalmente se elaboró el programa de auditoría para la supervisión del modelo de control definido.

A continuación, se presenta una breve descripción de cada una de las etapas del ciclo de vida que se ilustra en la figura 1:

- Categorización de los sistemas de información de acuerdo con un análisis de impacto (FIPS PUB 199, 2004).
- Selección de los controles basados en la categorización y evaluación de riesgos (NIST SP 800-53, Revision 4, 2015).
- Implementación de los controles describiendo como deben ser empleados en el sistema y en las operaciones (NIST SP 800-160, 2016).
- Evaluación mediante procedimientos que permitan determinar su correcta implementación y el logro de los resultados esperados.
- Autorización de la operación del sistema con el nivel de riesgo aceptado (NIST SP 800-37, Revision 1, 2014).
- Monitoreo continúo evaluando la efectividad de los controles, los cambios del sistema y las operaciones, la realización de análisis de impactos y el reporte del estado de seguridad del sistema.

Figura 1 Ciclo de vida de la seguridad



Fuente: (NIST SP 800-37, Revision 1, 2014)

Como parte de este proyecto se planteó realizar la definición de controles de acceso lógico al módulo financiero del sistema SAP de una compañía del sector energético.

7 Recursos utilizados.

A continuación se hace un breve descripción de los recursos utilizados

- Listado de preguntas para establecer el nivel de criticidad de los sistemas por cada objetivo de seguridad basado en el estándar de clasificación de la información NYS ITS (New York State Office of Information Technology Services, 2014)

- Documentos NIST para la categorización y clasificación de los sistemas de información y los catálogos de controles de acceso (NIST SP 800-53, Revision 4, 2015), (NIST SP 800-60, Revision 1, 2008).
- Política de seguridad de la información de la empresa
- Libro de SAP para la estructuración de los controles de accesos mediante el modelo de autorización y los parámetros del sistema (Lehnert, Bonitz, & Justice, 2010)
- Documento de PwC de segregación de funciones en SAP.

8 Resultados del proyecto.

A continuación, se presenta el modelo obtenido con sus respectivos productos luego de realizar las actividades propuestas para el logro de los objetivos del proyecto en el módulo financiero del sistema SAP S/4 Hana.

8.1 Categorización de seguridad del sistema

Se estableció la categoría de seguridad de acuerdo con el nivel de impacto asociado al compromiso de la confidencialidad, integridad y disponibilidad del sistema.

Se partió de las definiciones de objetivos de seguridad y niveles de impacto establecidos en (FIPS PUB 199, 2004).

A continuación, en la tabla 1 se presenta un breve resumen de los niveles de impacto, el efecto adverso en las operaciones y activos organizacionales y sus posibles consecuencias:

Tabla 1 Niveles de impacto

Nivel de impacto	Efecto adverso	Posibles consecuencias
Bajo	Limitado	• Causar degradación en la capacidad de operación, en una duración en la que la organización aún puede realizar sus funciones primarias, pero la efectividad de las funciones es reducida. • Resultar en daño menor a los activos de la organización • Resultar en una pérdida financiera menor. • Resultar en daño menor a los individuos
Medio	Serio	• Causar degradación significativa en la capacidad de operación, en una duración en la que la organización aún puede realizar sus funciones primarias, pero la efectividad de las funciones es significativamente reducida • Resultar en daño significativo a los activos de la organización • Resultar en una pérdida financiera significativa. • Resultar en daño significativo sin muerte o heridas de muerte a la vida de los individuos.
Alto	Severo o catastrófico	• Causar degradación severa en la capacidad de operación en una duración en la que la organización no puede realizar una o más de sus operaciones primarias • Resultar en daño mayor a los activos de la organización • Resultar en una pérdida financiera significativa. • Resulta en daño catastrófico o pérdida de vida o heridas de muerte a los individuos.

Fuente: (FIPS PUB 199, 2004)

La determinación de la categoría de seguridad de un sistema requiere de análisis y debe considerar las categorías de seguridad de todos los tipos de información residentes en el sistema de información. Para un sistema de información, los posibles valores de impacto asignados a los objetivos de seguridad respectivos (confidencialidad, integridad, disponibilidad) serán los valores más altos entre las categorías de seguridad que se han determinado para cada tipo de información residente en el sistema.

El formato generalizado para expresar la categoría de seguridad (SC) de un sistema de información es:

SC Sistema de información = {(confidencialidad, impacto), (integridad, impacto), (disponibilidad, impacto)}

Donde los valores aceptables para el impacto potencial son BAJO, MODERADO o ALTO.

El resultado de la categorización del sistema SAP S4 Hana es MODERADO, debido a que en este sistema se registra toda la información financiera y la evaluación de éste, hace parte de la opinión de la revisoría fiscal, la cual es entregada cada año en la asamblea de accionistas.

Un compromiso de la seguridad del sistema tendría un efecto adverso serio, debido a que podrían presentarse pérdidas financieras, conllevando a una opinión negativa por parte de la revisoría fiscal, dando como resultado una devaluación en el precio de la acción en el mercado de valores.

SC SAP S/4 Hana = {(confidencialidad, Moderado), (integridad, Moderado), (disponibilidad, Moderado)}

Para el caso en particular de SAP S/4 Hana los valores para cada uno de los tres objetivos de seguridad fue MODERADO, sin embargo, los posibles valores de impacto para la confidencialidad, la integridad y la disponibilidad pueden no ser siempre los mismos. Un sistema de impacto BAJO se define como un sistema de información en el que los tres objetivos de seguridad son bajos, un sistema de impacto MODERADO es un sistema en el que al menos uno de los objetivos de seguridad es moderado y ningún otro es mayor, y finalmente, un sistema de ALTO impacto es en el que al menos uno es alto.

8.2 Diseño de controles

A partir de la categorización del sistema, se dio inicio a la selección de controles de seguridad eligiendo la línea base correspondiente al nivel de impacto de la categorización del sistema. Estas líneas base son un punto de partida por lo tanto no son mandatorias, la empresa debe seleccionar, adicionar o complementar los controles que ella considere de acuerdo con las siguientes características:

- Los entornos en los que operan los sistemas
- La naturaleza de las operaciones realizadas por las empresas
- La funcionalidad empleada en los sistemas de información
- Los tipos de amenazas que enfrenta la empresa, los procesos y los sistemas
- El tipo de información procesada, almacenada o transmitida por los sistemas

A continuación, se presenta la tabla Líneas base de controles de acceso de acuerdo con la categoría del sistema, extractadas del apéndice D del estándar (NIST SP 800-53, Revision 4, 2015).

Tabla 2 Líneas base de controles de acceso

Numeral	**Control**	**Línea base**		
		Bajo	**Moderado**	**Alto**
AC-1	Política y procedimientos de control de acceso	X	X	X
AC-2	Administración de cuentas	X	X	X
AC-3	Acceso a la aplicación	X	X	X
AC-4	Aplicación de flujo de información	---	X	X
AC-5	Separación de tareas	---	X	X
AC-6	Privilegios mínimos	---	X	X
AC-7	Intentos fallidos de inicio de sesión	X	X	X
AC-8	Notificación de uso del sistema	X	X	X
AC-10	Control de sesión simultánea	---	---	X
AC-11	Bloqueo de sesión	---	X	X
AC-12	Terminación de la sesión	---	X	X
AC-14	Acciones permitidas sin identificación o	X	X	X

Numeral	Control	Línea base		
		Bajo	Moderado	Alto
	autenticación			
AC-17	Acceso remoto	X	X	X
AC-18	Acceso inalámbrico	X	X	X
AC-19	Control de acceso para dispositivos móviles	X	X	X
AC-20	Uso de sistemas de información externos	X	X	X
AC-21	El intercambio de información	---	X	X
AC-22	Contenido de acceso público	X	X	X

Fuente: (NIST SP 800-53, Revision 4, 2015)

En la tabla 3 se tiene un mapeo de los controles de acceso lógico entre el estándar (NIST SP 800-53, Revision 4, 2015) y (ISO/IEC 27001:2013).

Tabla 3 Mapeo de controles de acceso NIST vs ISO

Control	Numeral	
	NIST SP 800-53	ISO/IEC 27001
Política y procedimientos de control de acceso	AC-1	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2
Administración de cuentas	AC-2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
Acceso a la aplicación	AC-3	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
Aplicación de flujo de información	AC-4	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
Separación de tareas	AC-5	A.6.1.2
Privilegios mínimos	AC-6	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
Intentos fallidos de inicio de sesión	AC-7	A.9.4.2
Notificación de uso del sistema	AC-8	A.9.4.2
Notificación previa de inicio de sesión (acceso)	AC-9	A.9.4.2
Control de sesión simultánea	AC-10	Ninguno
Bloqueo de sesión	AC-11	A.11.2.8, A.11.2.9
Terminación de la sesión	AC-12	Ninguno
Acciones permitidas sin identificación o autenticación	AC-14	Ninguno

Control	Numeral	
	NIST SP 800-53	**ISO/IEC 27001**
Acceso remoto	AC-17	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
Acceso inalámbrico	AC-18	A.6.2.1, A.13.1.1, A.13.2.1
Control de acceso para dispositivos móviles	AC-19	A.6.2.1, A.11.2.6, A.13.2.1
Uso de sistemas de información externos	AC-20	A.11.2.6, A.13.1.1, A.13.2.1
El intercambio de información	AC-21	Ninguno
Contenido de acceso público	AC-22	Ninguno

Fuente: (NIST SP 800-53, Revision 4, 2015)

Al tener identificados los controles propuestos por los estándares ISO y NIST se procedió con la elaboración del modelo para el control de acceso lógico en la capa de aplicación.

El modelo inicia con la selección de los controles de acceso, para los cual se debe realizar un análisis de la disponibilidad y los impactos de la incorporación de estos en el sistema, para luego establecer las estrategias para su implementación.

Para la aplicación de este modelo en el sistema SAP S/4 Hana se realizó la selección de los controles de acuerdo con el resultado de la categorización del sistema, en la tabla 4 se encuentra la selección realizada.

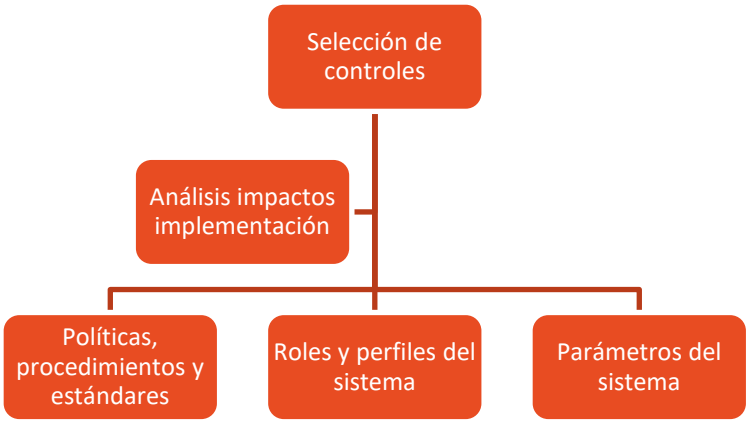
Los controles seleccionados fueron analizados en conjunto con los equipos de implementación del proyecto, identificando que en el sistema SAP S/4 Hana se puede establecer el control de acceso mediante roles RBAC y varios de los controles de acceso seleccionados se encuentran disponibles para su configuración mediante parámetros del sistema.

Como producto de este análisis también se establecieron las siguientes estrategias para su implementación.

- Políticas, procedimientos y estándares: esta estrategia está encaminada a verificar la existencia de estos lineamientos en las políticas de la empresa, particularmente en la política de seguridad de la información, en caso de que no hagan parte de ella, se deben incluir y desarrollar los procedimientos y estándares que permitan articular estos lineamientos.
- Roles y perfiles del sistema: matriz de control de acceso para regular privilegios a los usuarios sobre los activos.
- Parámetros del sistema: configuración de variables mediante las cuales se activan y se definen controles en actividades y procesos que realiza el sistema.

En la figura 2 se esquematiza el modelo de seguridad en la capa de aplicación para el sistema S/4 Hana

Figura 2 Modelo de control de acceso lógico en la capa de aplicación



Fuente: Elaboración propia

En la tabla 4 se presentan los controles con los que se estructuró el modelo de seguridad lógica para el sistema SAP S/4 Hana y la estrategia utilizada para su implementación:

Tabla 4 Controles de acceso SAP S/4 Hana

Numeral	Control	Estrategia de implementación
AC-1	Política y procedimientos de control de acceso	Política de seguridad
AC-2	Administración de cuentas	Política de seguridad, matriz de roles y parámetros del sistema
AC-3	Acceso a la aplicación	Política de seguridad, matriz de roles y parámetros del sistema
AC-4	Aplicación de flujo de información	Parámetros del sistema
AC-5	Separación de tareas	Política de seguridad y matriz de roles
AC-6	Privilegios mínimos	Política de seguridad y matriz de roles
AC-7	Intentos fallidos de inicio de sesión	Parámetros del sistema
AC-8	Notificación de uso del sistema	Parámetros del sistema
AC-10	Control de sesión simultánea	Parámetros del sistema
AC-11	Bloqueo de sesión	Parámetros del sistema
AC-12	Terminación de la sesión	Parámetros del sistema
AC-14	Acciones permitidas sin identificación o autenticación	Política de seguridad
AC-17	Acceso remoto	Política de seguridad
AC-18	Acceso inalámbrico	Política de seguridad
AC-19	Control de acceso para dispositivos móviles	Política de seguridad
AC-20	Uso de sistemas de información externos	Política de seguridad
AC-21	El intercambio de información	Política de seguridad
AC-22	Contenido de acceso público	Política de seguridad

Fuente: Elaboración propia

En el presente informe trataremos solamente los siguientes controles:

- AC-1 Política y procedimientos de control de acceso
- AC-2 Administración de cuentas
- AC-5 Separación de tareas
- AC-6 Privilegios mínimos
- AC-7 Intentos fallidos de inicio de sesión
- AC-10 Control de sesión simultánea

- AC-12 Terminación de la sesión

8.3 Implementación de controles

Durante la implementación del sistema S/4 Hana se entregaron las siguientes recomendaciones al Comité del proyecto teniendo en cuenta los controles identificados previamente

En la tabla 5 se muestra la interrelación de los elementos en la estructura de seguridad lógica:

Tabla 5 Estructura seguridad lógica

POLÍTICAS DE SEGURIDAD			
CONCEPTUALIZACIÓN DE LA ESTRUCTURA DEL MODELO			
Revisión de procesos a partir de la segregación de funciones	Diseño del Modelo de Seguridad Lógica	Implementación del Modelo de Seguridad Lógica	
IDENTIFICACIÓN DE RECURSOS TECNOLÓGICOS			
Redes y Conexión	Aplicaciones	Base de Datos	Sistemas Operativos
ARTICULACIÓN DEL DISEÑO Y LOS RECURSOS TECNOLÓGICOS			
Procedimientos		Estándares	
ADMINISTRACIÓN DEL MODELO DE SEGURIDAD LÓGICA			

Fuente: Elaboración propia

A partir de la definición de las políticas de seguridad se inicia la revisión de los procesos organizacionales, luego se diseña el Modelo de Seguridad Lógica, es decir la forma en que se articulan las funciones, se implementan los controles y se siguen los procedimientos y estándares para la administración del Modelo.

8.3.1 AC-1 Política y procedimientos de control de acceso

Se planteó la necesidad de la unificación de las políticas de seguridad (ver anexo Política de seguridad unificada) y se inició la revisión de los procesos

organizacionales, considerando el control *AC-5 Separación de tareas* que deben existir en cada área.

La separación de tareas o segregación de funciones tiene como objetivo minimizar el riesgo de error por concentración de funciones.

Luego de entender cómo opera el control de acceso lógico en SAP, se determinó que este opera con el modelo RBAC y se identificó que para la estructuración de los accesos y privilegios sobre el sistema SAP se pueden utilizar varios tipos de esquemas. Debido a la complejidad que se tiene y a la necesidad de escalabilidad de la seguridad, se optó por utilizar el esquema de rol maestro- rol derivado.

La implementación del Modelo de Seguridad Lógica implica la identificación de los recursos tecnológicos sobre los cuales se asignarán los accesos y transacciones y deben estar soportados en documentos que contengan los procedimientos y estándares que respaldan el diseño del Modelo.

- Diseño del control de acceso lógico en SAP

A continuación, se indican actividades y productos recomendados para el diseño del control de acceso lógico en SAP:

1. Revisión y ajuste de procesos: mapa de procesos

2. Identificación de actividades por proceso: mapa de actividades para cada proceso de la empresa.

3. Agrupación de actividades en roles y asignación de transacciones: mapa de procesos con roles asignados a las actividades, planilla de roles, transacciones y objetos de autorización a completar, variantes de rol

construidas y listas para las pruebas

- Revisión y ajuste de procesos

Como parte de la implementación de SAP, se inició en la etapa de *Business Blueprint* la revisión de los procesos organizacionales considerando las diferentes actividades de control de cada proceso para garantizar la confiabilidad de las operaciones de la empresa.

Las actividades de control son procedimientos que ayudan a asegurar que las políticas de la administración se llevan a cabo, estas se ejecutan en todos los niveles de la empresa y en cada una de las etapas de la gestión, partiendo del conocimiento de los riesgos y los controles destinados a evitarlos o minimizarlos.

Como resultado de esta actividad se obtiene el Mapa de procesos

- Identificación de actividades por proceso

Se construyó una matriz de funciones que permitió la identificación de todas las actividades que se desarrollan en cada proceso considerando los controles *AC-5 Separación de tareas* y *AC-6 Privilegios mínimos* (ver anexo Actividades).

- Agrupación de actividades en roles y asignación de transacciones

A continuación, se presenta en la figura 3 el proceso para la agrupación de actividades en roles y asignación de transacciones:

Figura 3 Agrupación de actividades en roles y asignación de transacciones

Fuente: Elaboración propia

- Identificación de roles

A partir del mapa de procesos se identificaron las actividades indivisibles que podían ser agrupadas en roles. A su vez sobre estos roles, se realizó un primer análisis de segregación de funciones para detectar incompatibilidades.

Un problema común es la identificación de roles con puesto organizativo. Esto es un error que puede llevar al fracaso cualquier modelo de seguridad, ya que los roles organizativos evolucionan y cambian en el tiempo, obligando a continuas modificaciones del rol SAP. Lo correcto es identificar aquellos grupos de tareas indivisibles que en general siempre se utilizan para efectuar una actividad y serán necesarias para un mismo usuario.

El resultado de esta actividad es un mapa de procesos con roles asignados a las actividades. (Ver anexo roles por proceso)

- Selección de transacciones

A partir de mapa de procesos con roles asignados a las actividades, se efectuó la definición de transacciones necesarias para ejecutar las actividades, construyendo los roles y analizando la segregación por código de transacción. A continuación, se muestra un ejemplo.

Rol	Actividad	Transacción
Aprobador de solicitud	Generar solicitud de pedido	ME51N
	Modificar solicitud de pedido	ME52N
	Liberar solicitud de pedido	ME54N

El resultado de esta actividad es la planilla de roles, transacciones y objetos de autorización a completar. (Ver anexo roles transacciones)

- Definición de variantes

A partir de la planilla de roles, transacciones y objetos de autorización a completar, se elabora una planilla de criterios de apertura por niveles organizativos u otras necesidades específicas, en la cual se incluyeron las necesidades de apertura basándose en la confidencialidad, requerimientos del negocio, distribución geográfica, y control interno.

El resultado de esta actividad es la planilla de variantes de rol construidas y listas para las pruebas.

- Asignación a usuarios

A partir de planilla de roles, transacciones, objetos de autorización a completar y variantes, se efectúa el relevamiento de asignación de usuarios a roles. Puede hacerse un relevamiento previo para validar el criterio de roles con el negocio, y luego abrirlo en las variantes respectivas. A continuación, se muestra un ejemplo.

	Aprobador solicitud	Solicitante de material	Gestor de proveedor	Gestor de catálogos	Gestor compras	Gestor contratos
Pérez, Juan	X	X				
Ríos, Carlos			X	X		
Gómez, Pedro					X	X

En el ejemplo anterior se determina que el usuario Pérez, Juan tendrá asignados los roles Aprobador solicitud y Solicitante de material; el usuario Ríos, Carlos tendrá asignados los roles Gestor de proveedor y Gestor de catálogos y el usuario Gómez, Pedro tendrá asignados los roles Gestor de compras y Gestor contratos.

- Administración de los roles en SAP

En la figura 3 se plantean los responsables y las actividades en el diseño, implementación y administración de los controles de acceso lógico en SAP:

Figura 4 Administración roles en SAP

Fuente: Elaboración propia

El proceso comienza con la recepción del requerimiento por parte de la mesa de servicios y la clasificación de este como una solicitud/modificación de permisos, el cual se remite al responsable del proceso y al líder funcional para que realicen la aprobación y análisis del mismo, si se determina la necesidad de crear un nuevo rol, el líder funcional del proceso realiza la definición teniendo en cuenta la segregación de funciones y el principio del mínimo privilegio, con esta definición el

líder funcional de seguridad crea el rol para que luego el líder funcional del proceso realice las pruebas.

8.3.2 AC-2 Administración de cuentas

A continuación, se presentan las recomendaciones entregadas al proyecto para la administración de usuarios:

- Gestión automática de cuentas de usuario

Este control consiste en utilizar mecanismos que permitan notificar a los administradores de usuarios las novedades de empleados como, por ejemplo: retiros, ascensos, vacaciones, entre otros. El desarrollo de este control de forma automática no es posible con las herramientas actuales con las que cuenta la empresa, sin embargo, se analizará la implementación de un sistema de gestión de identidades. Actualmente se realiza este control de forma manual.

- Tipificación de usuarios

De acuerdo con el tipo de usuario en algunos sistemas puede otorgarse privilegios adicionales a los otorgados por el Modelo de control de acceso lógico.

En el sistema SAP existen 5 tipos diferentes de usuarios:

Tabla 6 Tipos de usuario SAP

Tipo	Características
Dialogo	Tipo de usuario con el que deben acceder normalmente los usuarios finales que necesitan interactuar con el sistema a través de la interfaz gráfica de usuario SAP GUI. Todos los parámetros definidos son verificados al iniciar sesión, como así también las restricciones de inicio de sesión múltiples.
Sistema	No interactivos, no pueden iniciar sesión por la interfaz gráfica de usuario SAP

Tipo	Características
	GUI. Comúnmente utilizados para procesamiento por lotes, *workflow*, procesos ALE, etc. La contraseña solo puede ser cambiada por el administrador del sistema, permite inicio de sesión múltiples. Uso interno del sistema.
Comunicación	Utilizados para llamadas de funciones remotas (RFC) entre sistemas, comúnmente utilizados para las interfaces con otros sistemas. No es posible establecer inicio de sesión a través de la interfaz gráfica de usuario SAP GUI.
Servicio	La contraseña nunca expira, la misma solo puede ser cambiada por el administrador del sistema. Las autorizaciones deben ser mínimas y restringidas específicamente a la necesidad por la que se creó el usuario. Su uso no es recomendable salvo necesidad específica, ya que pueden iniciar sesión en el sistema a través de la interfaz gráfica de usuario SAP GUI
Referencia	No admite inicio de sesión. Utilizado para traspasar sus autorizaciones al usuario que lo tiene como referente.

Fuente: Elaboración propia

Conforme con esta información, se recomendó el tipo Dialogo para los usuarios que requieren utilizar el sistema como una herramienta para desarrollar sus funciones.

Para los procesos del sistema como la ejecución de trabajos en lotes, flujos de trabajo (workflow), actualizaciones, entre otros, se recomendó la utilización de usuarios tipo Sistema.

Para los usuarios de interfaces con los sistemas legados y las transferencias de órdenes de transporte entre mandantes se recomendó el tipo de usuario Comunicaciones.

Se recomendó restringir el tipo de usuario Servicio, debido a que, por sus características, no sigue las políticas definidas para el control de contraseñas.

- Perfiles críticos de autorización por defecto en el sistema

Para utilizar los perfiles de autorización por defecto de los sistemas, estos deben ser analizados previamente para verificar que estos no tienen una concentración de funciones y cumplir el principio de mínimo privilegio.

El sistema SAP trae por defecto los perfiles de autorización SAP_ALL y SAP_NEW, los cuales comprenden las autorizaciones globales sobre todos los procesos, transacciones y reportes definidos en el sistema, permitiendo ejecutar todas las funciones de procesamiento del sistema SAP sin restricción alguna. Considerando lo anterior, se recomendó no asignar a ningún usuario dichos perfiles críticos.

- Usuarios por defecto del sistema

Los sistemas traen creados usuarios por defecto con el objetivo de realizar la configuración inicial de los mismos, estos usuarios son genéricos y por lo general tienen altos privilegios, por lo que se recomienda no hacer uso de ellos cuando el sistema se encuentre en Producción.

Los siguientes usuarios se encuentran por defecto en el sistema SAP y poseen perfiles de autorización amplios y/o globales; por lo tanto, se recomendó que el acceso a los mismos debe ser limitado solo para las funciones propias del sistema, su activación debe ser temporal y por periodos de tiempo definidos en el momento en que sean requeridos:

Tabla 7 Estado usuarios propios del sistema

Usuario	Recomendación	Mandante
SAP*	Debe de existir, tener el estado bloqueado y su contraseña no debe ser la que posee por defecto ni debe ser trivial.	Todos los mandantes en los ambientes de producción, calidad y desarrollo.

Usuario	Recomendación	Mandante
DDIC	Debe de existir, puede estar desbloqueado y debe estar acompañado de una política para cambiar su contraseña periódicamente.	Todos los mandantes en los ambientes de producción, calidad y desarrollo.
EARLYWATCH	Debe de existir, la contraseña no debe ser la que posee por defecto, no debe ser trivial. Este usuario debe permanecer bloqueado.	Servicio de EARLYWATCH.
SAPCPIC	Debe de existir, la contraseña no debe ser la que posee por defecto, no debe ser trivial. Este usuario debe permanecer bloqueado.	Todos los mandantes en los ambientes de producción, calidad y desarrollo.

Fuente: Elaboración propia

- Cuenta de usuario temporales/emergencia

El sistema de información debe automáticamente deshabilitar las cuentas de uso temporal/emergencia después del período de tiempo definido por la empresa.
En el módulo de administración de usuarios del sistema SAP, se puede establecer el inicio y el fin mediante fechas de la vigencia de las cuentas de usuarios como de los roles, por lo cual se recomendó que todo usuario temporal debe tener definido en el sistema el inicio y fin de la vigencia de la cuenta y sus roles, y su necesidad y aprobación debe estar documentada.

- Deshabilitar cuentas inactivas

Transcurrido un periodo de tiempo definido por la empresa y el usuario no haya sido utilizado, la cuenta debe ser deshabilitada automáticamente.

El sistema SAP no cuenta con este control tal y como lo recomienda NIST, sin embargo, el sistema tiene el parámetro *login/password_max_idle_initial* que define el número máximo de días que la contraseña inicial definida por el administrador de usuarios permanece habilitada para que el usuario ingrese y defina una

contraseña personal. Adicionalmente el sistema también tiene el parámetro *login/password_expiration_time* mediante el cual la cantidad de días que transcurren antes de que expiré la contraseña del usuario y el sistema solicite un cambio de la misma.

Con base en lo anterior, se recomendó definir los valores para los parámetros: *login/password_max_idle_initial*=10 y *login/password_expiration_time*=30.
Además, se recomendó al administrador de seguridad realizar revisiones periódicas sobre el uso de los usuarios con el objetivo de optimizar el licenciamiento.

- Cuentas de usuario privilegiados

La empresa debe establecer que la administración de accesos en usuarios privilegiados debe ser de acuerdo con el esquema de acceso basado en roles con el objetivo conservar el control del acceso al sistema.

Entre los usuarios privilegiados más conocidos se encuentran, por ejemplo: administrador de contraseñas, administración de usuarios, administración de redes y sistemas, administración de bases de datos y administración web.
En el sistema SAP se crearon roles para cada una de las funciones de administración del sistema (gestión de usuarios, gestión de roles, gestión de transportes, respaldos, contraseñas, entre otros).

8.3.3 AC-5 Segregación de funciones

La separación de tareas o segregación de funciones implica asignar tareas incompatibles a diferentes personas con el objetivo minimizar el riesgo de error o fraude.

A continuación, se indican los lineamientos de segregación de funciones, los cuales fueron concertados con el área de control interno y auditoría de la empresa:

- Ambientes de desarrollo y prueba, separados de producción.
- Ninguna persona puede comprometer los activos de la organización unilateralmente.
- Iniciación, aprobación, procesamiento y registro de transacciones segregadas entre sí.
- Procesos segregados entre sí.
- Administración de datos maestros segregada de funciones transaccionales.

En la definición del modelo de seguridad lógica del sistema SAP, se establecieron reglas que permitieran identificar problemas de segregación de funciones (ver adjunto Matriz de segregación de funciones del módulo FI)

8.3.4 AC-6 Privilegios mínimos

La organización debe emplear el principio de privilegio mínimo, permitiendo solo accesos autorizados para los usuarios (o procesos que actúan en nombre de los usuarios) que son necesarios para llevar a cabo las tareas asignadas de acuerdo con las misiones de la organización y las funciones del negocio.

Este principio se encuentra incluido en la Política de seguridad de la empresa, y es utilizado para la administración del modelo de seguridad lógica del sistema SAP.

8.3.5 AC-7 Intentos fallidos de inicio de sesión

El sistema debe Imponer un límite de intentos de inicio de sesión no válidos consecutivos por un usuario durante un periodo determinado y bloquear automáticamente la cuenta hasta que sea liberada por un administrador.

El sistema SAP tiene el parámetro login/fails_to_user_lock, y mediante este se determina la cantidad de errores consecutivos en el ingreso de la contraseña a partir del cual se bloquea el usuario, el cual debe ser desbloqueado por el administrador. Conforme a lo anterior se recomendó definir el parámetro con valor de 3.

8.3.6 AC-10 Control de sesión simultánea

El sistema de información debe limitar el número de sesiones simultaneas por usuario.

El sistema SAP tiene el parámetro rdisp/max_alt_modes que permite controlar el número máximo de sesiones que puede abrir un usuario simultáneamente, asi mismo también tiene parámetro *login/disable_multi_gui_login* que permite controlar los inicios de sesión de forma simultánea con el mismo usuario.
Se recomendó definir el parámetro rdisp/max_alt_modes= 6 y deshabilitar el inicio de sesión simultanea debido a que tiene implicaciones en términos de licenciamiento.

8.3.7 AC-12 Terminación de la sesión

Cuando se presente inactividad por un periodo de tiempo definido por la empresa, la sesión debe ser cerrada o si el usuario finaliza la sesión esta debe ser terminada

El sistema SAP cuenta con el parámetro *rdisp/gui_auto_logout* mediante el cual se determina en segundos la cantidad de tiempo de inactividad antes que se terminé la sesión del usuario. Se recomendó definir este parámetro en 900 segundos (15 minutos). El sistema SAP al desconectarse se finaliza la sesión.

9 Limitaciones o dificultades.

Las dificultades estuvieron relacionadas con la resistencia al cambio por parte de los usuarios en cuanto a la limitación de privilegios sobre el nuevo sistema y adoptar los flujos de autorización para la asignación de nuevos accesos. Adicionalmente la estructuración de un modelo de control de acceso basado en roles es una actividad dispendiosa, pero permite detallar con más exactitud las funciones y acceso a la información de los usuarios.

10 Conclusiones.

La implementación de modelos y esquemas de seguridad debe tener el patrocinio y apoyo de la Dirección. Gracias a este respaldo el equipo tuvo participación activa en las reuniones del comité del proyecto, las cuales se realizaban cada semana, permitiendo conocer las particularidades y avance del proyecto de primera mano. Durante las pruebas integrales fue fundamental la intervención de la Dirección cuando por premura en los tiempos de implementación del proyecto se consideró la propuesta de realizar esta fase sin la seguridad de roles y perfiles, por lo cual se explicó al proyecto y a la Dirección los riesgos y problemas futuros de realizar las pruebas de esa manera, debido a esto, la Dirección le pidió al proyecto descartar esa propuesta e implementar la seguridad de roles y perfiles y reprogramar sesiones de pruebas todos los días de la semana con horario extendido.

La implementación de modelos de seguridad debe tener en paralelo un fuerte proceso de comunicaciones y de gestión de cambios soportado por las áreas de Gestión Humana y Arquitectura y Procesos para dirigir a los usuarios frente a los cambios en los accesos otorgados e identificar zonas grises en las cuales la responsabilidad frente a una función no esté claramente definida.

El proyecto definió una estrategia de comunicaciones y de gestión del cambio que tuvo como objetivo generar un compromiso con las partes interesadas para conducir una transición sin problemas a la nueva forma de trabajar. Este proceso contó con el apoyo de las diferentes gerencias del negocio, la estrategia utilizada consistió en enviar mensajes clave al comienzo de cada una de las fases a las diferentes audiencias con los objetivos esperados y resaltando la importancia de la participación y compromiso de cada uno de ellos. La gestión de cambios estuvo apoyada por videos en los que se indicaban los beneficios de los nuevos procesos y el paso a paso de cada uno de los procesos y como los diferentes roles organizacionales participaban en cada actividad,

Debido a la complejidad del modelo de autorización en el sistema SAP dada por la alta cantidad de objetos de autorización y transacciones y los cambios inesperados en el perfil de acceso de usuarios por modificaciones en el contenido y la asignación de roles, se recomienda utilizar herramientas sistematizadas que permitan definir reglas para identificar los conflictos de segregación de funciones de forma previa a la asignación de los accesos.

Existen varias soluciones en el mercado para verificar la segregación de funciones en SAP, sin embargo, la más completa y que se integra de forma natural con SAP es el módulo de control de acceso que hace parte de la solución de GRC de SAP, el cual permite realizar la revisión detallada de la seguridad a nivel de objetos de autorización y asignación de perfiles de forma dinámica.

Es fundamental concientizar al área de Gestión Humana sobre la importancia de la comunicación de novedades en ingresos, retiros, ascensos y cambios de cargos y funciones para alcanzar un adecuado ciclo de vida de usuarios y accesos. Para el cumplimiento de este objetivo se realizaron sesiones en las que se explicaron los riesgos al tener la información de cargos y empleados desactualizada, se acordaron acuerdos de niveles de servicio y se planteó como trabajo futuro, la

implementación de un sistema de gestión de identidades que esté integrado con los sistemas de personal, se recomendó el sistema IdM de SAP debido a que se integra naturalmente al módulo de seguridad del sistema S/4 Hana y al Employee Central del sistema Success Factor, el cual es el módulo de administración de personal de la empresa.

11 Bibliografía

Decreto 1377 de 2013. (s.f.). *Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.* Obtenido de https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

European Comission. (2014). *Digital Security: Cybersecurity, Privacy*. Obtenido de Call H2020-DS-2014-1, DS-02-2014: http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/ds-02-2014.html

European Comission. (2017). *HORIZON 2020 Work Programme 2016-2017 - Secure Societies - Protecting freedom and security of Europe and its citizens*. Obtenido de http://http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf

EY. (2014). *Adelántese a los delitos cibernéticos.* Obtenido de Encuesta Global de Seguridad de Información 2014: http://www.ey.com/Publication/vwLUAssets/Encuesta_global_de_seguridad_de_informaci%C3%B3n_2014/$FILE/EY-encuesta-global-de-seguridad-de-informacion-2014.pdf

EY. (2015). *Crear confianza en el mundo digital.* Obtenido de Encuesta Global sobre Seguridad de la Información de EY de 2015: http://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015/$FILE/ey-encuesta-global-seguridad-informacion-2015.pdf

FIPS PUB 199. (Febrero de 2004). *Standards for Security Categorization of Federal Information and Information Systems.* Obtenido de FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

FIPS PUB 200. (9 de Marzo de 2006). *Minimum Security Requirements for Federal Information and Information Systems.* Obtenido de FEDERAL

INFORMATION PROCESSING STANDARDS PUBLICATION: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

ISO. (2017). *International Organization for Standardization*. Obtenido de https://www.iso.org/about-us.html

ISO/IEC 13335-1:2004. (s.f.). *Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management.*

ISO/IEC 27000:2016. (s.f.). *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary.*

ISO/IEC 27001:2013. (s.f.). *Information technology -- Security techniques -- Information security management systems -- Requirements.*

ISO/IEC 27002:2013. (s.f.). *Information technology -- Security techniques -- Code of practice for information security controls.*

Lee B., K. D. (2015). Role-based access control for substation automation systems using XACML. *Information Systems, 53*, 237 – 249. doi:https://doi.org/10.1016/j.is.2015.01.007

Lehnert, V., Bonitz, K., & Justice, L. (2010). *Authorizations in SAP Software: Design and Configuration.* SAP PRESS.

Ley 1266 de 2008. (s.f.). Obtenido de UIAF Unidad de Información y Análisis Financiero de Colombia: https://www.uiaf.gov.co/?idcategoria=20630

Ley 1273 de 2009. (s.f.). Obtenido de Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

Ley 1581 de 2012. (s.f.). *Congreso de Colombia.* Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

New York State Office of Information Technology Services. (2014). *Information Technology Standard Information Classification.* Obtenido de NYS-S14-002: https://its.ny.gov/sites/default/files/documents/Enterprise_Information_Classification_v3_1.pdf

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Obtenido de https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NIST SP 800-137. (Septiembre de 2011). *Information Security Continuous Monitoring for Federal Information Systems and Organizations.* Obtenido de http://dx.doi.org/10.6028/NIST.SP.800-137

NIST SP 800-160. (Mayo de 2016). *Systems Security Engineering.* Obtenido de http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf

NIST SP 800-37, Revision 1. (10 de junio de 2014). *Guide for Applying the Risk Management Framework to Federal Information Systems.* Obtenido de https://dx.doi.org/10.6028/NIST.SP.800-37r1

NIST SP 800-53, Revision 4. (22 de Enero de 2015). *Security and Privacy Controls for Federal Information Systems and Organizations [including updates as of 1/22/2015].* Obtenido de http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST SP 800-53A, Revision 4. (Junio de 2010). *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.* Obtenido de http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

NIST SP 800-60, Revision 1. (Agosto de 2008). *Guide for Mapping Types of Information and Information Systems to Security Categories.* Obtenido de http://dx.doi.org/10.6028/NIST.SP.800-60v1r1

NIST/NSA Privilege Access Management Workshop Collaboration Team. (2010). *Nist IR 7657 - A Report on the Privilege (Access) Management Workshop.* Obtenido de http://dx.doi.org/10.6028/NIST.IR.7657

R. Kainda, I. Flechais, & A. Roscoe. (2010). Security and usability: Analysis and evaluation. *ARES 2010, Fifth International Conference on Availability, Reliability and Security.*

Shirey, R. (2007). RFC4949 - Internet Security Glossary, Version 2. IETF - Informational Memo. doi:10.17487/RFC4949

Verizon Enterprise. (2015). *2015 DATA BREACH INVESTIGATIONS REPORT.* Obtenido de http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

Wang H., Guo X., Fan Y., Bi J. (2014). Extended access control and recommendation methods for enterprise knowledge management system. *IERI Procedia, 10*, 224-230.

Zapata, L. (julio de 2013). *Development of a Model for Security and Usability.* Universidad Politécnica de Madrid.