ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO E IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 – 2013 PARA EL SERVICIO DE DIRECTORIO DE UNA EMPRESA DE VENTA AL DETALLE"

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por

ANGEL FABRICIO ELIZALDE TAPIA

Guayaquil – Ecuador

2018

AGRADECIMIENTO

A Dios por entregarme paciencia e inspiración. A Laura por su ayuda y su guía. A Gad, Victor y Priscilla por su apoyo. A la vida por las oportunidades presentadas.

DEDICATORIA

Dedicado a Alfonso y Gloria por el amor y ser el ejemplo a seguir todos estos años. A Mirtha, Tatiana, Carlos Cesar, Daniel Emilio y Gianna por ser el incentivo de mejorar cada día. A Alain, Yanitza, Roberto y todos mis amigos por ser y estar.

TRIBUNAL DE SUSTENTACIÓN

_____

Mgs. Lenin Freire

DIRECTOR MSIG / MSIA

_____

Mgs. Laura Ureta

DIRECTOR DEL PROYECTO DE GRADUACIÓN

_____

Mgs. Juan Carlos García

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Trabajo de Titulación, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Reglamento de exámenes y títulos profesionales de la ESPOL)

RESUMEN

En el capítulo 1 se indica los antecedentes y generalidades respecto de la situación de un grupo empresarial dedicado a la venta al detalle. Durante el mismo el autor ofrece una descripción del problema dentro de la empresa acerca del control interno en un servicio de apoyo. Basándose en esta descripción se propone como solución el diseño e implantación de un marco operacional diseñado a medida que permita solventar el problema indicado.

En el capítulo 2 se muestra el marco teórico que engloba conceptos básicos acerca de seguridad de la información tales como las vulnerabilidades, los riesgos y la forma en que se puede gestionar los mismos. Además, se describe las características de los sistemas de seguridad de la información y los beneficios de su uso.

En el capítulo 3 se realiza un levantamiento de información que detalla al grupo Corporativo sujeto de este estudio y su organización interna. Las características acerca de su entorno externo e interno en las que el grupo corporativo se desenvuelve durante sus operaciones. Adicionalmente se describe el área de Tecnología y su organización interna. Se recopila y define el requerimiento y las personas que intervienen como parte interesada en la mejora del servicio, también se detallan características del proceso analizado y el ámbito operacional del proceso dentro del área.

En el capítulo 4 se realiza el análisis de la información obtenida durante el levantamiento de información. Por medio del análisis se obtienen los riesgos potenciales que afectarían al servicio de directorio Corporativo. Durante reuniones con los interesados es posible obtener una ponderación basada en la frecuencia y el impacto, con esta ponderación y el apetito del riesgo se determinan los riesgos críticos que serán necesarios mitigar. Además, se realiza una revisión de las políticas existentes para reutilizar controles ya aprobados y facilitar el proceso de implementación. También se construye el plan de auditorías internas y el procedimiento para ejecutarlas como el procedimiento de medición de diseñado. Los indicadores son diseñados como métrica para dar un porcentaje de mitigación del riesgo. La declaración de

aplicabilidad que es el documento en que se acepta la mitigación de los riesgos encontrados por medio de los controles indicados en el documento. Como última actividad se realiza el proceso de aprobación del esquema y también se Declaración de Aplicabilidad.

En el capítulo 5, se ejecutan los planes para el afinamiento de los controles y se realizan las pruebas por parte del administrador del servicio. Se comienza por la difusión de las políticas a través del canal corporativo de comunicaciones, así como del esquema y los controles. A continuación, el plan de puesta en marcha de los controles y su validación a cargo del administrador. En el final del capítulo se realiza la actividad de medición por medio de una Auditoria Interna para obtener una imagen real del servicio y la efectividad de los controles implementados y en funcionamiento.

En el capítulo 6 se analizan los resultados de la auditoria interna para confirmar lo evidenciado, definiendo las no conformidades y remarcando las oportunidades de mejora. El análisis culmina con la elaboración del Informe de Auditoria Interna en que se detallan de manera más explícita las no

conformidades, oportunidades de mejora y los indicadores para dar una visión consolidada de mitigación de los riesgos críticos para la operación. Finalmente se presenta a la Gerencia de Tecnología el esquema diseñado e implementado y se comprueba a través de las métricas que la mejora continua es un componente necesario en el ciclo de vida de los servicios y procesos.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CIA	**:**	Confidentiality, Integrity, Availability
ILM	**:**	Life Cycle Management
ISO	**:**	International Organization for Standardization
MAGERIT	**:**	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
PDCA	**:**	Plan, Do, Check, Act
SGSI	**:**	Sistema de Gestión de Seguridad de la Información
SGSI	**:**	Sistema de Gestión de la Seguridad de la Información
SOA		Declaración de Aplicabilidad (SOA por las siglas en inglés de Statement of Applicability)
Stakeholder	**:**	Persona interesada o interesado

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La necesidad de las empresas de obtener una diferenciación de su competencia hace que los activos de información adquieran una mayor criticidad dentro de la operación. Los activos constituyen la información relevante a las operaciones de la empresa, su entorno y las oportunidades de mejora. Por medio del procesamiento de la información es que la empresa puede analizar, planear y controlar sus operaciones de manera que se pueda gestionar mejor sus recursos obteniendo eficiencia y seguridad. La criticidad de los activos de información hace necesario que se opere en un marco seguro para las operaciones para que las decisiones generadas sobre el procesamiento de esa información sea de calidad y aporte valor a la empresa. Es importante que la empresa enfoque su atención a normas y estándares propuestos por organismos dedicados a mejorar la eficiencia de la empresa.

Sin embargo, las empresas deben seleccionar las normas que faciliten sus procesos y tengan flexibilidad, además que incorporen procesos de mejora continua y garanticen que los procesos obtengan eficiencia. Las

normas ISO son las más ampliamente difundidas y mayor aceptación por las empresas para mejorar sus procesos. Las normas ISO se han diversificado para atender muchas áreas de operación de las empresas sin importar su tamaño o la actividad que estas realicen. El presente trabajo establecerá un esquema de seguridad para la operación de un servicio de apoyo para una empresa que le permita evaluar el desempeño de las normas para detectar riesgos y gestionar los mismos. La implementación de este esquema sentará las bases para la futura adopción de normas ISO dentro de la compañía.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedente

El mundo de las empresas es altamente competitivo, todas se ven forzadas a realizar a conciencia un análisis exhaustivo de su entorno, en busca de nuevas oportunidades de mercado que permitan su expansión y lograr ventajas competitivas sobre su competencia, cautivar a sus clientes e incursionar en nuevos mercados. El análisis del entorno y los datos obtenidos a través de fuentes internas o externas se logra a través del uso canales de información globalizados como la Internet y el uso de tecnologías como es el caso de conexiones o enlaces a redes de terceros. Los datos son procesados obteniendo información que

dependiendo de su importancia constituyen activos de información que genera valor para la empresa y el desarrollo de sus operaciones.

Considerando que la información posee confiabilidad, integridad y disponibilidad la empresa debe realizar su esfuerzo en proveer un mecanismo, marco o procedimiento que garantice que sus activos se salvaguarden acorde a los criterios de valor que la empresa asigne a su información

Las entidades de control promueven normas que permiten controlar y gestionar los riesgos en un marco ordenado y documentado, es obligación de las empresas adoptar normas que les permitan garantizar la operación segura y de esta manera cumplir con los objetivos que persigue la organización.

La Organización Internacional para la Estandarización es el organismo que propone estándares para el control continuo y homogenización de la calidad de sus productos y sus servicios. El organismo promueve un conjunto de reglas que abarcan muchos aspectos de los ámbitos de operación de las empresas. Es ISO 27001 quien da las pautas para el uso de un Sistema de Seguridad de la Información que certifique que la información sea confidencial, integra y esté disponible siempre que sea requerida acorde a las definiciones del valor asignado al activo.

El propósito del presente trabajo consiste en la adopción de un marco de gobierno que permita la gestión responsable de un servicio corporativo de apoyo basado en la norma ISO 27001.

1.2 Descripción del Problema

La empresa de venta al detalle es una cadena de tiendas a nivel nacional, con diferentes marcas y diferentes tipos de negocios. Tales como supermercados, ferreterías, tiendas por departamento entre otros. Las diferentes líneas de negocios están constantemente realizando solicitudes y demandas al área de IT y sus aplicaciones. El servicio de Directorio es un pilar importante en el desarrollo de las actividades debido a que múltiples aplicaciones corporativas se parametrizan para utilizar este Servicio Corporativo.

Actualmente las operaciones del área de TI se han venido desarrollando en aparente normalidad, pero el Director de Sistemas indica que no observa la existencia de control interno sobre los componentes tecnológicos y una gestión integral a la operación y el acceso al servicio. Expresa además que es necesario la adopción de un marco de mejores prácticas que al ser implementado permita mejorar el control interno del Servicio Corporativo.

Se ha detectado dos puntos clave a tratar, el control de accesos y la seguridad de las operaciones del servicio.

Respecto del Control de Accesos

1. Revisión de la política de accesos
2. Deficiente control de las altas y bajas de los usuarios
3. Acceso a información privilegiada
4. Revisión continua de los controles de acceso y accesos especiales, en casos como el cambio de funciones o de roles de los usuarios.

Respecto de la Seguridad de la Operación

1. Poca documentación de procedimientos en la operación del Servicio Corporativo.
2. Deficiente control en la gestión de cambios que afectan al Servicio Corporativo.
3. Escasa gestión sobre las copias de respaldo para recuperación del Servicio Corporativo.
4. Gestión de Vulnerabilidades, código malicioso y los riesgos que afecten a la operación del Servicio Corporativo

Es de conocimiento general, que la ausencia de control interno y la incapacidad de gestionar correctamente los componentes de TI

ocasionan problemas como fraudes, accesos no autorizados, fugas de información, problemas en la operación, capacidad de recuperación ante problemas, interrupción en la prestación de los servicios. Esta es la razón por la cual es necesario realizar una revisión general de los componentes del servicio, para garantizar que se cumplen los criterios de seguridad de la información y permitan al área de Tecnología satisfacer los nuevos requerimientos y mantener la operación de los sistemas ya vigentes acordes a un Sistema de Gestión de Seguridad de la información adecuado.

1.3 Solución Propuesta

En concordancia con el criterio de que la información es el principal activo de la empresa y el manifiesto de la Dirección del área de Tecnología en la empresa; es necesario desarrollar un esquema de seguridad informática personalizado pero en concordancia en la norma ISO/IEC 27001 – 2013, que permita diseñar e implantar medidas preventivas y correctivas que garanticen la protección y el resguardo de la información para ofrecer la confidencialidad, integridad y disponibilidad que la organización espera respecto de sus activos.

Por medio del diseño y la implementación de un Esquema de Seguridad de la Información basado en estándares ISO/IEC 27001 – 2013, se conseguirá la base para generar el control interno que la empresa y sus

directivos esperan del servicio que brinda el área tecnológica. Constituyéndose en el primer paso para la adopción de buenas prácticas en la administración y operación de los otros servicios corporativos que conforman parte del Catálogo de Servicios.

El análisis con la metodología MAGERIT para el análisis y la gestión de los riesgos para los sistemas de información permitirá detectar los riesgos, ponderar los riesgos detectados acorde a su impacto y probabilidad de materialización y como resultado obtener una clara y precisa visión del apetito del riesgo de la empresa y sus directivos. Este análisis permitirá focalizar las acciones a tomar y establecer los controles necesarios para prevención y mitigación en base a la clasificación obtenida.

De lo expuesto anteriormente se utilizará de la norma ISO/IEC 27001 – 2013 los puntos para el diseño e implementación del Esquema de Seguridad de la Información.

1. Anexo A. 9 Control de Acceso

2. Anexo A. 12 Seguridad en la Operación

Los beneficios que se obtienen de utilizar un esquema de seguridad de la información implementado en estándares ISO son:

1. Generar la visión deseada por la Dirección de la empresa y el Área Tecnológica acerca de control interno en la operación y el acceso a la información de la empresa.

2. Obtener efectividad y eficiencia en la operación del Servicio Corporativo de directorio, así como a todos los demás servicios que utilizan el directorio para su funcionamiento.

3. Incrementar la calidad, disponibilidad y confiabilidad del servicio de directorio;

4. Proteger la información de la empresa de cualquier uso indebido, actos ilegales o irregularidades.

5. Cumplir con disposiciones legales y otras regulaciones o normas gubernamentales, como son los procesos de auditoria externos que la empresa debe cumplir para su operación.

6. Promover la adopción de esquemas de seguridad de información basados en estándares ISO para otros servicios corporativos dentro del portafolio de servicios, constituyendo las primeras actividades encaminadas hacia la adopción de un Sistema de Gestión de Seguridad de la Información.

1.4 Objetivo General

Desarrollar e implementar un Esquema de Seguridad de la Información para el servicio de directorio, según la Norma ISO/IEC 27001 – 2013 para una empresa de ventas al detalle.

1.5 Objetivo Específicos

Los objetivos específicos para este trabajo son:

1. Establecer la situación actual de la empresa mediante la identificación de sus activos y relevamiento de políticas de seguridad de la información relacionadas con el servicio de directorio para definir el alcance del Esquema de Seguridad de la Información.

2. Identificar y Clasificar los riesgos, su criticidad e impacto relacionados al servicio de directorio, a través de Magerit

3. Diseñar e implementar un conjunto de controles para el cumplimiento de las políticas del Esquema de Seguridad de la Información, tomando como base los riesgos críticos y de alto impacto.

4. Establecer un proceso de gestión interno que permita evaluar que los controles implementados continúen con el

cumplimiento continuo de las políticas del Esquema de Seguridad de la Información para el servicio de directorio.

5. Analizar la efectividad de los controles implementados para obtener la eficacia en el cumplimiento de las políticas del Esquema de Seguridad de la Información para el servicio de directorio.

1.6 Metodología

En el presente documento se detalla un marco de seguridad basado en la metodología descrito en la Norma ISO/IEC 27001 – 2013 y sus controles que permita a una organización, la gestión de un proceso de apoyo y que permita la mejora continua. Este marco de seguridad deberá ser flexible y esto se consigue por el uso de las normas ISO como base. Además, el marco constituirá el pivote inicial para una futura implementación de un Sistema de Seguridad de la Información que sea extendido a todos los demás procesos de la organización.

.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Seguridad de la Información

Todas las empresas son entidades relacionadas con su entorno, basadas en gestiones humanas que buscan generar bienes y recursos. En la actualidad las organizaciones o empresas utilizan sistemas informáticos para realizar sus funciones cotidianas, es a través de estos sistemas que se genera información, constituyéndose este producto y sus sistemas de información en los bienes o activos más importantes para el logro de sus metas y objetivos.

Un sistema de información es un conjunto de componentes o elementos cuya directriz es el tratamiento de datos e información, su estructuración y almacenamiento para su uso inmediato o posterior. Entonces la información es una colección de datos procesados y organizados, de fuentes internas y externas, que es de gran importancia para la empresa y sus actividades. La información está presente dentro de la empresa en muchas formas sea esta oral, escrita, transmitida o almacenada en medios sean estos impresos o digitales.

Por medio de esta información la empresa se retroalimenta o conoce de su entorno operativo. Un ejemplo claro de esta afirmación corresponde por ejemplo a los estados financieros que permiten a la empresa, analizar su desempeño histórico, conocer su situación económica actual y planear para aprovechar los recursos con el fin de cumplir sus objetivos.

Lo antes expuesto permite concluir que las empresas deben orientar sus actividades a la creación y mantenimiento de entornos seguros en los que se garantice que los procesos del negocio operen y permitan a la empresa alcanzar sus metas y objetivos.

2.1.1 Criterios de la Información

La información es un insumo importante en la operación de la empresa, ya que permite a la misma efectuar toma de decisiones a fin de lograr un alto nivel de competitividad y crecimiento. La

información posee un ciclo de vida, conocido como ILM por sus siglas en inglés Information Lifecycle Management, que inicia desde su adquisición hasta que es finalmente descartada, a lo largo de este ciclo la información atraviesa fases que alteran su valor en el tiempo [1].

La información posee características que agregan y aportan valor a lo largo de su ciclo de vida presentado en la Figura 2.1 Ciclo de vida de la Información:

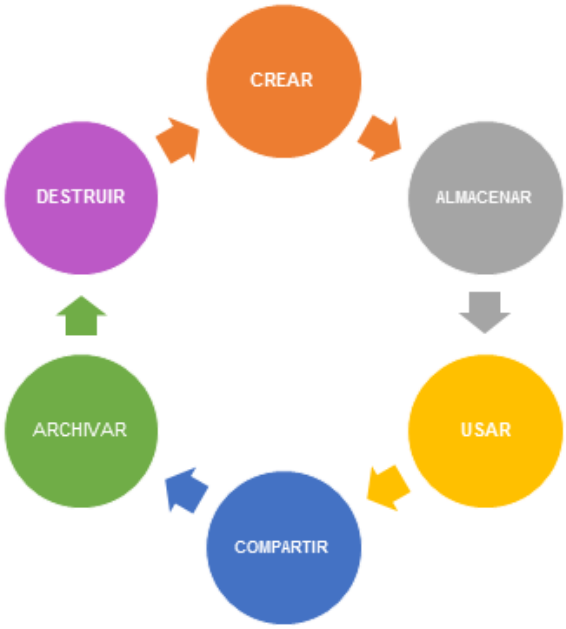


Figura 2.1 Ciclo de Vida de la Información

La información posee tres características importantes y fundamentales, que se deben cumplir para ser considerada como un recurso útil en las actividades de la empresa y la consecución

de sus objetivos. Las características son Confidencialidad, Integridad y Disponibilidad, que constituyen los principios conocidos como la tríada CIA, por sus siglas en inglés Confidentiality, Integrity, Availability, como lo muestra la figura 2.2 Propiedades de la Información [2]:

Figura 2.2 Propiedades de la Información

La Confidencialidad promulga que la información será accedida únicamente por las personas o sistemas que cuenten con la debida autorización.

La Integridad indica que la totalidad y precisión de la información se mantendrá exacta a cuando fue generada y únicamente será

modificada por la persona o sistemas que cuenten con la autorización para hacerlo.

La Disponibilidad declara que la información estará disponible para ser accedida por las personas o sistemas autorizados cuando estos así la requieran.

Siendo la información entonces el soporte básico en la toma de decisiones se observa la importancia para gestionar correctamente la generación, almacenamiento y correcto uso de la misma, así como también la de los sistemas e infraestructura que lo soportan.

2.1.2 Riesgo

En su desempeño, todas las empresas se pueden ver afectadas por situaciones que afecten a sus operaciones. Estas situaciones pueden ser de varios tipos, externas o internas.

En la actualidad, la globalización encamina a las empresas a estar conectadas a redes externas como la Internet, donde se puede obtener muchas ventajas entre las cuales están la adquisición de información, el contacto directo con clientes y proveedores, la expansión a nuevos mercados, la transmisión rápida de información; pero expone a la organización a

situaciones que atentan contra los principios de la información, técnicas variadas como la sustracción, adulteración o denegación de información o servicios que indicen directamente a las organizaciones y sus sistemas informáticos ocasionando pérdida de competitividad, mercado, retraso en sus operaciones, perdida de confiabilidad.

Las situaciones de carácter interno ocurren dentro de la organización y pueden darse por muchos factores, claros ejemplos de estos son falta de alineación del recurso humano con las metas y objetivos de la empresa, desconocimiento de normas y políticas, deficiente interrelación entre áreas operativas o departamentos, incorrecta gestión o administración de sistemas informáticos entre otros.

Lo anteriormente citado son denominadas amenazas, siendo las amenazas eventos potenciales que podrían vulnerar la integridad, disponibilidad y confiabilidad de la información. El riesgo es simplemente la materialización de una amenaza. [3]

El riesgo es siempre evaluado acorde al impacto adverso en los objetivos del negocio y la interrupción de las operaciones de la empresa.

El riesgo es inherente al ámbito de la operación de las empresas y consiste en el riesgo intrínseco de la actividad u operación sin tener en cuenta los controles que se implementen para su gestión. El riesgo residual por su lado es el resultado remanente de riesgo luego de haber implementado respuestas eficaces a las acciones planeadas para mitigar el riesgo inherente

2.1.3 Gestión del Riesgo

La correcta identificación, medición y control por medio de políticas y procedimientos que busquen garantizar el correcto desempeño de la organización y la consecución de sus metas u objetivos son actividades conocidas como Gestión del Riesgo. La gestión de los riesgos tiene que ver mucho más con implantación de políticas eficientes y su aplicación que con los aspectos tecnológicos de cómo implementarlos. Es una actividad cíclica o iterativa, que debe realizarse con orientación a prevenir riesgos futuros y no enfocados a su corrección.

El proceso implica conocimiento del giro del negocio, productos o servicios, procesos, metas y objetivos para entender la prioridad de la empresa.

La identificación de los procesos y el inventario de los activos de información necesarios que apuntalan el óptimo desempeño del proceso.

Identificar las vulnerabilidades presentes o amenazas de estos activos de información, la existencia de controles previamente establecidos e implementados y analizar estrategias para mitigar riesgos tomando en cuenta costo versus beneficio.

Seleccionar la estrategia para el tratamiento de los riesgos y aceptación el riesgo residual y respuesta ante el riesgo por parte de la Alta Gerencia implantar controles seleccionados para mitigar los riesgos y su monitoreo para efectos de medir la eficacia de los controles implementados.

La respuesta al riesgo puede ser mitigar, evitar, transferir y Aceptar, criterios que definiremos a continuación y se aprecian en la Figura 2.3 Respuestas al Riesgo:

Figura 2.3 Respuesta al Riesgo

Mitigar, Implementar los controles con el fin de reducir la probabilidad de ocurrencia del riego o su impacto. Ejemplo Establecer un mecanismo de contingencia que permita la operación de un proceso en condiciones mínimas de operación.

Evitar, Eliminar completamente el riesgo. Ejemplo No utilizar una plataforma de tecnología susceptible de errores.

Transferir, Traspasar el impacto del riesgo a un tercero. Por ejemplo, Contratar una póliza de seguros para el hardware de equipos servidores.

Aceptar. Reconocer la presencia del riesgo y establecer mecanismos para monitorearlo.

La gestión de riesgos es un tema de cultura organizacional y no una tarea exclusiva del área de tecnología, por lo que el equipo que evalué el mismo debe ser conformado e involucrar personal de diferentes áreas incluida la Alta Gerencia. La posición de la empresa debe ser difundida a lo largo de toda la organización, a través de los canales de comunicación y buscando la concienciación del personal de la compañía, proveedores y clientes.

2.1.4 Sistemas de Gestión de Seguridad de la Información

Sistema de Seguridad de la información o por sus siglas SGSI, es un conjunto de políticas para la correcta gestión de la seguridad de la información. La información son los datos organizados o procesados que pertenecen a una organización o empresa que tienen valor para su operación y el logro de sus objetivos. Esto desmitifica el concepto errado de que la seguridad está dada por dispositivos de seguridad perimetral o software especializado, estos simplemente son componentes que permiten al Sistema de Seguridad de Información [4].

Los Sistemas de seguridad de la Información contienen diferentes componentes,

Política y objetivos de seguridad: Es el documento, de carácter general, que establece el compromiso de la Dirección de la empresa y la posición u orientación de la empresa respecto de la seguridad de la información.

Procedimiento y Controles: Son aquellos procedimientos definidos, establecidos que son la base y permiten que regulan la operación del Sistema de Seguridad de la Información.

Enfoque de Evaluación de Riesgos: Especificación de la metodología adoptada para la evaluación de las amenazas y riesgos respecto de los activos de información cubiertos por el alcance definido, criterios de aceptación y niveles de riesgos aceptables.

Informa de Evaluación de Riesgos: Informe resultante de la aplicación de la metodología sobre los activos de información.

Plan de tratamiento de riesgos: Documento que contiene las acciones de la dirección, recursos, las responsabilidades y priorización para gestión del riesgo de seguridad de la información. Básicamente es un plan de acción donde se define de forma clara quienes implementaran el control, cuando se realizará, con cuánto presupuesto se cuenta.

Procedimientos documentados: Documentos formales en los que se detalla de forma clara y concisa la forma de realizar las actividades necesarias para la planificación, operación y control de los procesos de seguridad.

Registros: documentos que muestran los resultados obtenidos o proporciona evidencia de las actividades realizadas.

Declaración de aplicabilidad o SOA: Documento que incluye los objetivos de control y los controles considerados por el Sistema de Seguridad de la Información.

2.1.5 Ciclo PDCA

El circulo o ciclo PDCA (por sus siglas en Ingles Plan, Do, Check, Act) es un modelo de trabajo que tiene como orientación la mejora continua de la calidad [5].

Ideado por William Edwards Demming (1900-1993) es utilizado en los Sistemas de Gestión y consta de cuatros pasos que se realizan de manera consecutiva y de forma cíclica, mostrados en la Figura 2.4 Ciclo PDCA: [6]

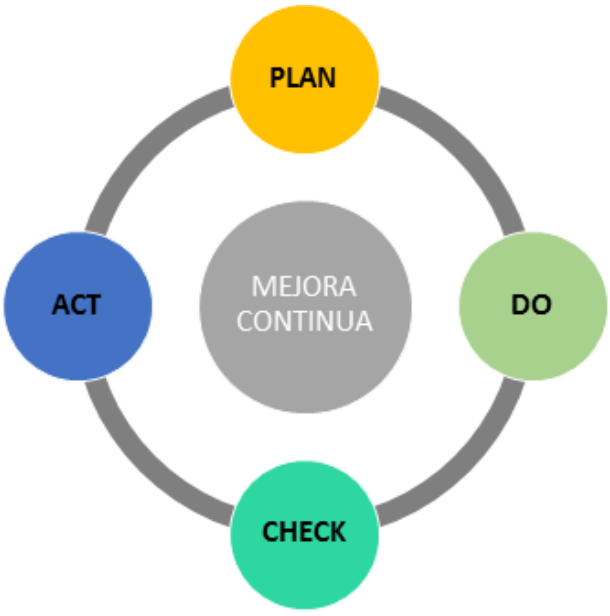


Figura 2.4 Ciclo PDCA

Esta metodología es un gran aliado de las organizaciones, pues permite la reducción de costos y precios, optimiza la competitividad, adiciona mejora los productos y servicios. Desde el punto de vista de los Sistemas de Gestión de Seguridad de la Información conlleva grandes beneficios porque permite a través de sus etapas la mejora continua y por ende elevar el grado de madurez y eficacia.

Las iteraciones dentro del ciclo PDCA buscan aumentar el conocimiento respecto del sistema analizado y una proximidad a la consecución de un objetivo.

Plan o Planificar, es la etapa correspondiente a establecer el objetivo y definir los resultados esperados. Se basa en el conocimiento del proceso o sistema a mejorar para ejecutar un análisis y estudio con el fin de determinar las mejoras buscadas, teniendo en cuenta los resultados que se esperan.

Do o Hacer, es la etapa donde se ejecuta el plan obtenido en la etapa anterior, la ejecución del plan debe generar los registros necesarios para el posterior análisis.

Check o Verificar corresponde a la etapa de validación de lo planificado en base a lo actuado para determinar si la implementación se ha efectuado de manera efectiva.

Act o Actuar consiste en la etapa de corrección o mejoras en el desempeño del Sistema sugeridas en la etapa previa cuando sea necesario.

2.2 Norma ISO/IEC 27001 - 2013

La Norma ISO/IEC 27001 fue desarrollada por la Organización Internacional de Estandarización conocido por sus siglas ISO y especifica cómo gestionar la seguridad de la información en una organización. Su primera revisión fue publicada en el 2005 y su más reciente publicación data del año 2013. Es la principal norma a nivel global para la seguridad de la información.

2.2.1 Conceptos Generales

La Norma ISO/IEC 27001 fue desarrollada por la Organización Internacional de Estandarización conocido por sus siglas ISO y especifica cómo gestionar la seguridad de la información en una organización. Su primera revisión fue publicada en el 2005 y su más reciente publicación data del año 2013. Es la principal norma a nivel global para la seguridad de la información [7].

2.2.2 Beneficios del uso de la Norma ISO/IEC 27001-2013

La Norma ISO/IEC 27001 puede ser implementada en cualquier organización, pública o privada, grande pequeña o mediana. Ha

sido elaborada con el aporte de especialistas en el tema y entrega una metodología para implementar la gestión de la seguridad en las organizaciones. Las empresas pueden certificarse, el proceso implica que una entidad certificadora independiente corrobore que la empresa ha establecido un marco de operación que garantiza que la seguridad de la información se ha implementado acorde a lo establecido a la norma ISO/IEC 27001.

La norma ISO/IEC 27001 tiene como finalidad la protección de la integridad, confidencialidad y disponibilidad de la información. Muchas empresas tienen software muy complejo y hardware especializado en seguridad, pero estos componentes no cumplen su finalidad si no se dispone de un marco de gestión o Sistema de Seguridad de la información que establezca políticas y procedimientos para operar en un ambiente seguro y así mantener las propiedades de la información. El desarrollo de estas políticas proviene del análisis que la organización realiza sobre los riesgos que podrían afectarla y el establecimiento de controles para la correcta gestión de los riesgos detectados.

La adopción de ISO/IEC 27001 ofrece ventajas para las empresas que se detallarán a continuación.

Desde el punto de vista comercial, la Norma ISO/IEC 27001, mejora la competitividad de la empresa, en base a la confiabilidad que perciben los clientes y sus proveedores. Generando una imagen de credibilidad y de calidad de sus servicios o productos.

Desde el punto de vista financiero, las empresas que adoptan de la Norma ISO/IEC 27001 tienen una reducción de los costos por incidentes debido a la gestión correcta de los riesgos operacionales.

Desde el punto vista del recurso humano, la adopción de la Norma ISO/IEC 27001 consigue la concienciación del personal de la empresa y sus proveedores respecto de la importancia de las responsabilidades a nivel personal y organizacional en las medidas de seguridad para el manejo de la información.

Desde el punto de vista funcional, la organización conoce y gestiona efectivamente sus activos de información y los procedimientos relacionados para salvaguardar los mismos, garantizando el cumplimiento de sus objetivos estratégicos.

Desde el punto de vista legal, la organización puede aplicar de manera más ágil y eficaz el cumplimiento de normas legales estipuladas en contratos o solicitadas por entes regulatorios.

La norma se encuentra compuesta por once secciones más un Anexo; las secciones del 0 al 3 no son de carácter obligatorias y corresponden más a un aspecto introductorio, desde la sección cuatro al diez son de carácter obligatorio y toda empresa que desee certificarse debe cumplirlos. Las secciones son mostradas en la Figura 2.5 Secciones Norma ISO 27001:2013:

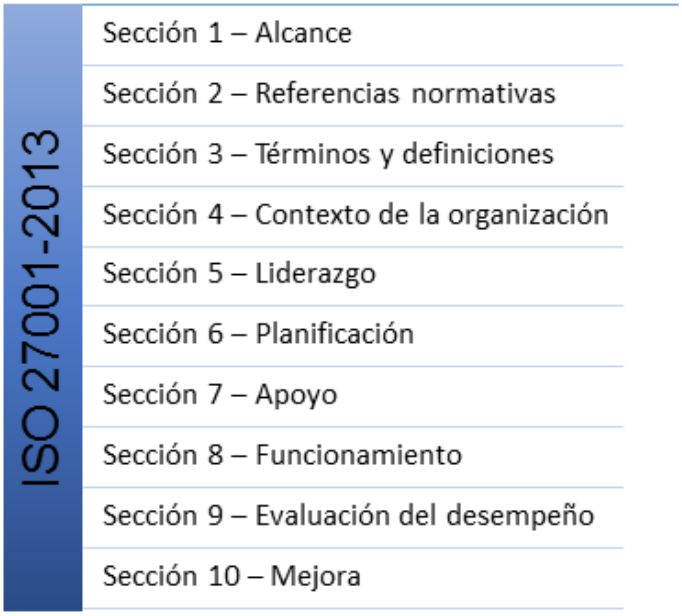


Figura 2.5 Secciones Norma ISO 27001:2013

El Anexo A de la norma ISO es muy conocido debido a su contenido, en ella se describen 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18), indicados en la Figura 2.6 Anexo A Norma ISO 27001:2013:

Figura 2.6 Anexo A Norma ISO 27001:2013

2.2.3 Control de Accesos

Todos los sistemas de información o activos de información que manejan o almacenan información de valor para los procesos de la organización deben ser gestionado de forma que se garantice la integridad, confidencialidad y disponibilidad. De esta manera es importante que la empresa adopte una política de control de

acceso, la misma promoverá los requerimientos de seguridad para la información de los procesos del negocio.

Las actividades necesarias para un efectivo control de accesos serán descritas a continuación.

Implementar procedimientos formales documentados, controlados y comunicados para controlar la asignación de derechos a los usuarios respecto del acceso en los sistemas de información. Estos procedimientos deben abarcar desde el registro de nuevos usuarios hasta el cese de los mismos respecto de los accesos a los sistemas de información.

El Recurso Humano debe estar concienciado respecto de las políticas y procedimientos de seguridad de la información, especialmente con el tema de uso de claves que les han sido otorgadas y la responsabilidad de su custodia.

El control de accesos en seguridad informática se basa 4 ejes esenciales;

Autorizar, Establecer lo que un usuario o sistema puede hacer.

Autenticar, Permitir que un usuario o sistema legitimado pueda acceder

Aprobar, Conceder acceso durante la operación, asociando usuarios versus recursos a los que tiene autorización.

Auditar, Registrar e identificar los accesos de un usuario hacia un recurso.

ISO/IEC 27001 posee un dominio respecto del control de Accesos con catorce controles, como se describen en la Figura 2.7 Control de Acceso – Controles:

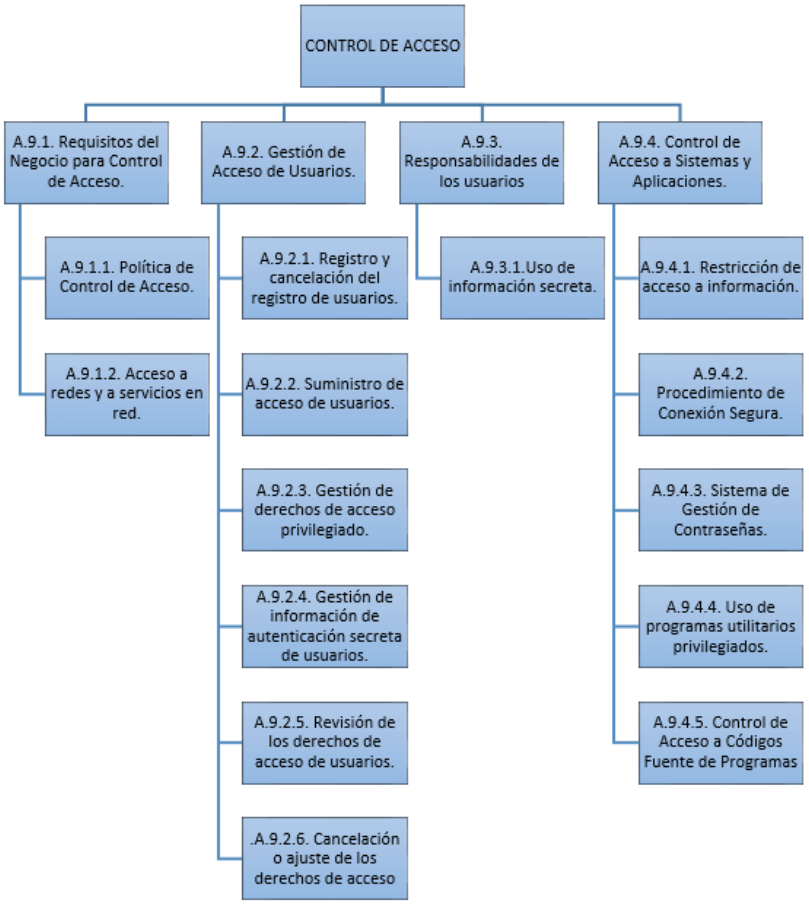


Figura 2.7 Control de Acceso - Controles

2.2.4 Seguridad en la Operación

Todas las empresas que poseen información crítica para la operación de sus procesos deben garantizar la operación de estos procesos a través de un marco que gestione la operación segura. La norma ISO/IEC 27001 posee un dominio que establece los controles necesarios para la correcta gestión de la seguridad en la operación de los sistemas de información de las empresas.

Las actividades para poder garantizar la seguridad en la operación son diversas y las empresas deben estar en la capacidad de atender

Validar la existencia de procedimientos operativos y mantener un control adecuado sobre la documentación relacionado y su correspondiente actualización.

Evaluar el efecto en la operación de los cambios previstos y de su implantación en los sistemas de información y los activos de información.

Gestionar y monitorear correctamente las capacidades de las plataformas de operación actual y planificar de manera adecuada las futuras demandas sobre las mismas.

Definir los controles para la detección y prevención de software malicioso.

Supervisar la creación de copias de respaldo de la información, la prueba cíclica de estos respaldos a través de restauración que permita validar la eficacia para garantizar la recuperación y evitar la pérdida de información.

Validar el cumplimiento de políticas, procedimientos, normas establecidos mediante auditorias y análisis de registros de actividad en los sistemas de información como prevención y detección de riesgos presentes y futuros.

ISO/IEC 27001 posee un dominio respecto del Seguridad en la Operación con catorce controles, a saber:

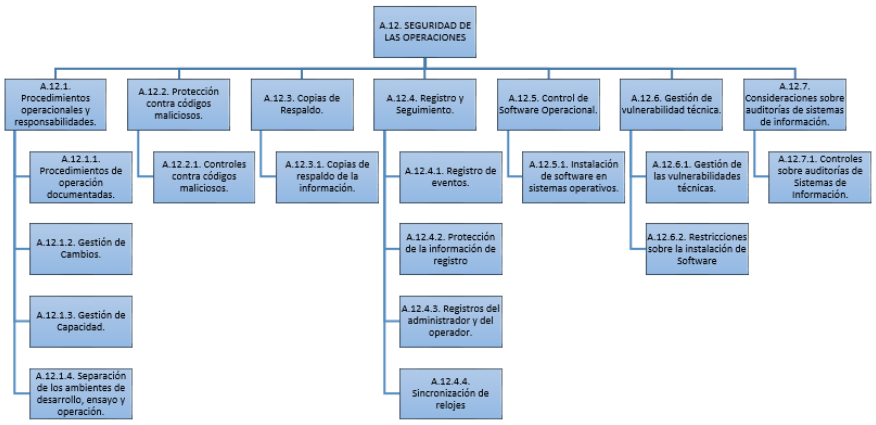


Figura 2.8 Seguridad en la Operación – Controles [7]

2.3 Magerit

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) de carácter público se utiliza en análisis y gestión de riesgos en los Sistemas de Información para reducir los riesgos de implantación y uso de las Tecnologías de la Información.

2.3.1 Generalidades

La tecnología Magerit en su primera versión fue desarrollada por el Consejo Superior de Administración Electrónica en el año 1997 y su enfoque fue hacia los riesgos que provienen del uso de los sistemas de información [8].

La segunda versión de la metodología cuya publicación fue en el año 2005, buscaba realizar la revisión constructiva acerca de los riesgos de las compañías, incluyendo ya cuestionamientos más a detalle sobre la gestión del riesgo y considerando la experiencia que se adquirió desde la versión anterior,

La tercera revisión y actual tiene una visión global de la Seguridad de los Sistemas de Información ISO 27001. Magerit en su estructura se compone de dos libros y una guía de técnicas a saber detallados en la Figura 2.9 Magerit – Libros:

Figura 2.9 Magerit – Libros.

2.3.2 Objetivos de Magerit

Esta metodología persigue los objetivos indicados a continuación

Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos adecuadamente

Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Preparar a las Organizaciones para los procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

2.3.3 Método de Magerit

El primer libro de Magerit comprende una aproximación para los usuarios a las terminologías y conceptos generales además de una explicación acerca de las actividades que se realizarán.

Las tareas o actividades son detalladas como tareas informales, pero dependiendo de factores tales como el alcance o tamaño del sistema, personal o grupos de trabajo involucrados y el tiempo planificado es conveniente formalizar las tareas para que las mismas tengan una correcta gestión y se desarrollen dentro de un marco controlado.

El libro contiene los siguientes capítulos:

Capítulo 1 Introducción. - Explica de manera ágil los conceptos relacionados a la gestión del riesgo, ciclo PDCA, el origen de Magerit, los objetivos de la metodología

Capítulo 2 Visión de Conjunto. - Muestra los conceptos de manera rápida. Las actividades de Análisis y Gestión de Riesgos son delimitadas dentro de un proceso formal de Gestión del Riesgo

Capítulo 3 Método del Análisis de Riesgo. - Enumera los pasos y formaliza las actividades del Análisis de Riegos mostrados en la

Figura 2.10 Magerit – Método de Análisis de Riesgos:

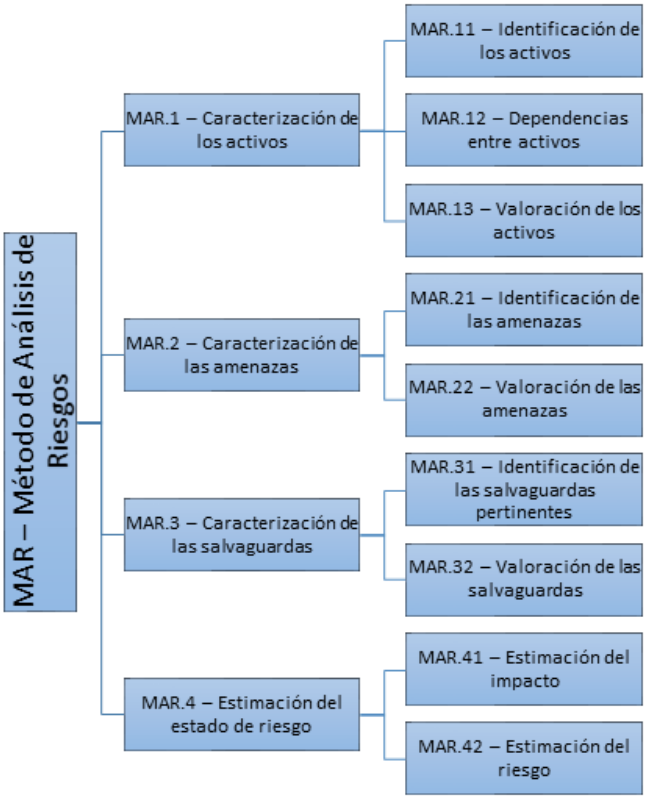


Figura 2.10 Magerit – Método de Análisis de Riesgos

Capítulo 4 Procesos de Gestión de Riesgos. - Expone criterios y opciones para el tratamiento de riesgos y formaliza las actividades de la Gestión del Riesgo.

Capítulo 5 Proyectos del Análisis de Riesgo. - Centrado en los proyectos de análisis de riesgos, desde el primer análisis de riesgos para un sistema y eventualmente cuando existan cambios significativos e implique rediseñar el modelo de manera amplia, como se observa en la figura a continuación:

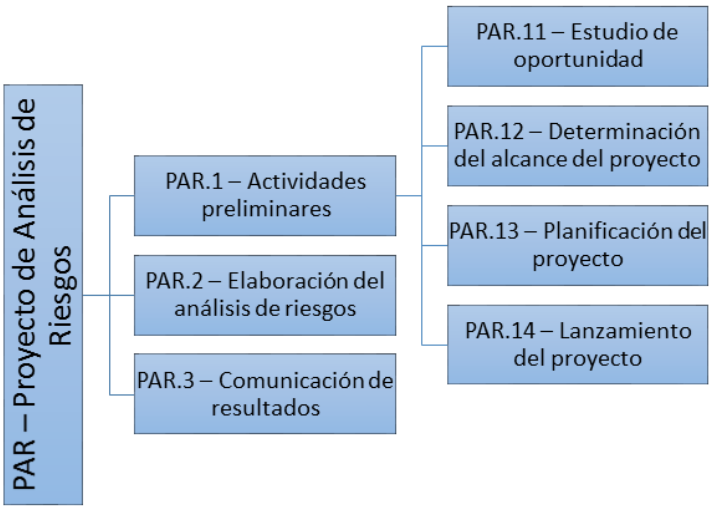


Figura 2.11 Magerit – Proyecto de Análisis de Riesgos

Capítulo 6 Plan de Seguridad. - Formaliza las actividades de los planes de seguridad mostrado en la siguiente figura:

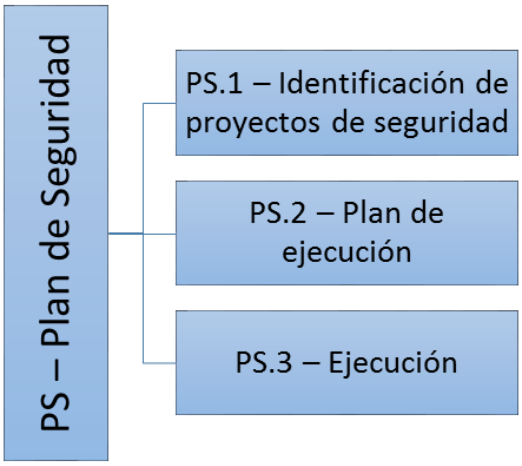


Figura 2.12 Magerit - Plan de Seguridad

Capítulo 7 Desarrollo de Sistemas de Información. - Centrado en el ciclo de vida de los sistemas de información y cómo el análisis de riesgos es utilizado para gestionar la seguridad del producto a lo largo de sus fases, comenzando en el diseño, a través de su desarrollo y finalizando en su puesta en producción.

Capítulo 8 Consejos Prácticos. - Ofrece guía para la resolución de algunos problemas que aparecen frecuentemente en el análisis de riesgos, convirtiéndose en un punto de apoyo para esta actividad.

Los apéndices recopilan diverso material de consulta:

Apéndice 1.- un glosario,

Apéndice 2.- Incluye referencias bibliográficas consideradas para el desarrollo de la metodología,

Apéndice 3.- Anexa referencias al marco legal que enmarca las tareas de análisis y gestión en la Administración Pública Española,

Apéndice 4.- Repasa dos marcos en los que se formaliza la evaluación y certificación.

Apéndice 5.- Describe las características necesarias para las herramientas que buscan dar soporte en el proceso de análisis y gestión de riesgos,

Apéndice 6.- Acerca de la evolución de Magerit a través de sus versiones 1, 2 y 3.

2.3.4 Catálogo de Elementos

El segundo libro Catálogo de Elementos proporciona un detalle actividades ya revisadas en el capítulo 2 del Volumen uno

1. Tipos de activos
2. Dimensiones y criterios de valoración de los activos
3. Amenazas
4. Salvaguardas

Este libro identifica de manera clara dos objetivos que se deben observar en cualquier proyecto de análisis y gestión de riesgos:

1. Por una parte, ofrecer elementos estándar para facilitar la labor de las personas que acometen el proyecto y les permitan enfocarse en lo específico del sistema a ser analizado.

2. Homogeneizar los resultados de los análisis, fomentando terminología y criterios uniformes que permitan comparar e incluso integrar análisis obtenidos por diferentes grupos de trabajo.

2.3.5 Guía de Técnicas

El tercer libro Guía de Técnicas cuyo objetivo es brindar orientación sobre algunas de las técnicas que se emplean para realizar proyectos de análisis y gestión de riesgos.

Para las técnicas referenciadas en este libro:

El objetivo perseguido por la técnica es explicado de manera breve.

Los elementos asociados a la técnica son descritos

Los principios fundamentales de la técnica son expuestos

La notación de la técnica es presentada de manera textual y/o gráfica.

Se citan de fuentes bibliográficas que son estimadas de interés para los usuarios de la metodología.

En el capítulo 2 se detallan técnicas específicas para el análisis de riesgos que son el análisis mediante tablas, análisis algorítmico y árboles de ataque.

En el capítulo 3 se detallan técnicas generales para el análisis de riesgos que son las técnicas gráficas, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi

2.4 Servicios de Directorio

2.4.1 Generalidades

Los servicios de directorio son aplicaciones centralizadas cuyo fin es almacenar y categorizar información acerca de usuarios y recursos en la red. Los administradores pueden gestionar a través de los servicios de directorio los accesos de los usuarios a esos recursos [9].

Existen múltiples implementaciones de directorio a saber, Windows Active Directory de Microsoft, Apple Open Directory de Apple, eDirectory de Novell, OpenLDAP de Linux, entre otros, pero para que una aplicación pueda ser considerada un servicio de directorio es necesario que se cumplan ciertas características funcionales.

1. Los usuarios y administradores del servicio de directorio deben poder realizar búsquedas rápidas de información.

2. El servicio de directorio no tiene dependencias de su ubicación física.

3. El servicio de directorio debe ser distribuido, aunque para temas administrativos es considerado uno solo, es decir que puede estar en diferentes ubicaciones físicas.

4. El servicio directorio debe ser compatible en términos de accesibilidad, puede ser usado desde otros sistemas operativos. Esto se consigue a través del uso del uso de protocolos estandarizados y no propietarios.

5. El servicio de directorio debe ser versátil en términos de poder almacenar nuevos tipos de objetos cuando sea necesario.

2.4.2 Servicios de Dominio de Active Directory

Microsoft tiene una implementación de Servicio de Directorio desde la versión del su Sistema Operativo Windows 2000 Server hasta su versión Actual conocida como Active Directory Domain Services o sus siglas (ADDS), incluida es Windows Server 2016.

Es importante aclarar los términos utilizados dentro de Directorio Activo.

Directorio

Es el único almacén para la información de los recursos y los usuarios dentro de una organización. El servicio de directorio contiene la ubicación y las propiedades de los diferentes recursos dentro de la red. Esta información es utilizada por los usuarios, así como por sus administradores y permite localizarlos con simpleza.

La implementación de Microsoft utiliza el protocolo LDAP (Lightweight Directory Access Protocol, en español, Protocolo Ligero de Acceso a Directorios) que permite la búsqueda contenida dentro del directorio. Pero además se puede hacer uso del conjunto de herramientas orientas a objetos y son proveidas por Microsoft. Son denominadas ADSI (Active Directory Services Interface, en español, Interfaces de Servicio de Active Directory) y no están soportadas por LDAP.

Dominio

Es un grupo de objetos dentro del Directorio, son parte de un mismo conjunto segmentado con fines de administración. Cada

Dominio contiene sus propios objetos y unidades organizativas. El dominio posee un nombre y para esto se utiliza el protocolo DNS, de donde se deriva que para la implementación es necesario que exista un servidor DNS en la red.

Objeto

Los objetos con componentes que forman parte del directorio, el cual podría ser una impresora, usuario, carpeta compartida, grupo, entre otros. Todos los objetos un nombre que permite identificarlo y los objetos poseen características específicas. Las características de cada tipo diferente de objeto dentro del directorio se encuentran definidas dentro del Esquema.

Controlador de dominio

Los controladores de dominio es uno o más equipos servidores que cuyo sistema operativo es Windows Server y ejecutan Directorio Activo. Su función principal es almacenar la base de datos del servicio de directorio y los datos relacionados a la seguridad.

Los controladores de dominios tienen particiones, las mismas que se detallan a continuación.

Partición de Configuración, que es de carácter obligatoria y es donde está la almacenada la topología del bosque y la información que permite funcione la replicación del directorio, también se encuentra los conjuntos de réplica y sus usuarios.

Partición de Esquema, que también es obligatoria y contiene los tipos de datos que se pueden guardar dentro del directorio y sus definiciones. Esta partición proporciona la coherencia de datos. Esta partición se puede extender para permitir a aplicaciones crear tipos de datos y definiciones personalizadas.

Partición de Aplicaciones, es de carácter opcional y contiene datos que son usados por aplicaciones. Puede ser creada durante la instalación del servicio o después. Las aplicaciones pueden ser modificar el esquema de manera automática o esta modificación se puede realizar de manera manual.

Arboles

Los árboles son colecciones de dominios que tienen una raíz en común y cuya organización posee una jerarquía. DNS nos permite representar esta jerarquía.

Los arboles permiten la fragmentación de los datos del Directorio Activo y su beneficio se observa en la replicación, donde solo

replican las partes necesarias y permite optimizar el uso del ancho de banda.

Bosques

Los bosques contienen todos los dominios, estos dominios a su vez están relacionados a través de las relaciones de confianza generadas de manera automática. Así todos los arboles del domino confían entre sí y compartirán sus recursos, aunque no su espacio de nombres en DNS.

Unidades Organizativas

Las Unidades Organizativas, también conocidas como O.U., son contenedores almacenar objetos incluidas otras unidades organizativas. Es un pilar básico en la administración del servicio de directorio dado que facilitan administrar los usuarios recursos de grandes organizaciones de forma ordenada y flexible.

Esquema

El esquema es la base de datos que contiene la definición de cada objeto que puede contener el directorio. Todos los objetos dentro del esquema poseen características propias conocidas como atributos.

El esquema de este sistema de servicio de directorio es extensible, es decir puede ser modificado para incluir nuevas características sobre los objetos ya existentes o nuevos objetos en sí. En el caso de una compañía que necesita almacenar el número del documento de identidad del usuario encontrará que el servicio de directorio puede ser modificado para incluir este atributo a través de la modificación de su esquema

Sitio

El sitio es un conjunto de equipos relacionados lógicamente entre sí y comparten una localización geográfica.

Relaciones de confianza.

Las relaciones de confianza son el mecanismo de comunicación entre los bosques, árboles y dominios. Pueden ser unidireccionales o bidireccionales y son de carácter transitivo.

2.4.3 Beneficios

Active Directory es una de las implementaciones más utilizadas dentro de las organizaciones debido a la madurez de la plataforma y a sus múltiples prestaciones.

Escalabilidad: Active Directory es compatible con aplicaciones de terceros y posee la capacidad de extender el esquema para soportar nuevos objetos permitiendo versatilidad en la operación.

Almacenamiento Distribuido y Replicación: Los datos contenidos del directorio se encuentran unificados, pero a la vez están distribuidos a través de los controladores de dominio de modo que permiten la optimización de recursos.

Centralización y Delegación de la Administración: Se gestiona unificadamente el control de privilegios para la administración y la seguridad basado en jerarquías. La delegación de administración de los objetos puede realizarse de forma granular.

Alta Disponibilidad y Tolerancia a Fallos: Su implementación permite elaborar esquemas de alta disponibilidad basados en la presencia de múltiples controladores de dominio que garantizan la tolerancia a fallos

Gestión de Seguridad, Control de Accesos y Autenticación: La seguridad se garantiza a través del uso de políticas de seguridad que permiten controlar de forma global y granular equipos, usuarios y recursos, claves entre otras. El Servicio de Directorio sirve como un punto centralizado de autenticación permitiendo a

los usuarios y aplicaciones utilizar el directorio como autoridad de autenticación a través de sus credenciales.

CAPÍTULO 3

LEVANTAMIENTO DE NECESIDADES

3.1 Modelo Organizacional y Operacional

El grupo empresarial CER inició sus operaciones en el año 1936 con la modalidad de supermercados de autoservicio. Actualmente es un grupo empresarial ubicado entre las primeras diez empresas importantes del Ecuador. Cuenta con diferentes líneas de negocios tales como cadenas de supermercados, jugueterías, tiendas departamentales, ferreterías y posee presencia en ocho provincias en Ecuador.

El modelo organizacional del grupo empresarial CER es el modelo organizacional mixto es decir aprovecha las ventajas de los modelos

jerárquico y modelo funcional. Así puede mantener una estructura jerárquica, pero aplica mayor especialización.

El grupo empresarial CER dispone de muchas líneas de negocios todas ofrecen servicios y productos variados para atender a sus clientes. Las unidades organizacionales apoyan a través de sus funciones en la generación de los mismos.

La empresa se encuentra dividida en cuatro direcciones, detallados en la figura Figura 3.1 Organigrama - Grupo Corporativo CER a continuación:

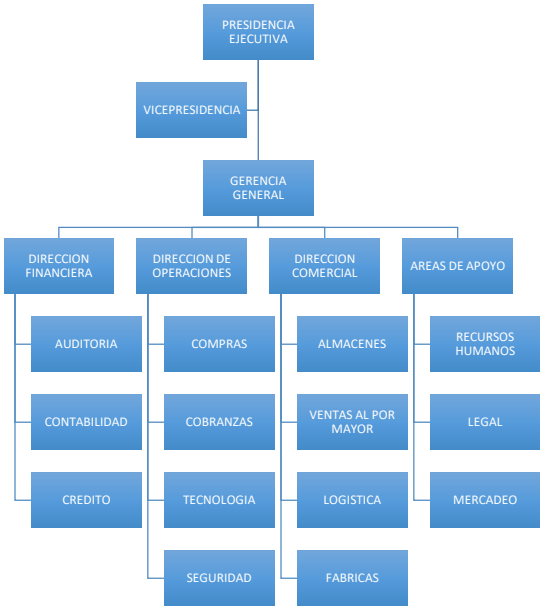


Figura 3.1 Organigrama - Grupo Corporativo CER

La Dirección Financiera está relacionada con la gestión económica y financiera del grupo corporativo. Se encuentra integrada por el área de Auditoría, Contabilidad y Crédito. Sus funciones incluyen las actividades

de control de la contabilidad, análisis de costos, elaborar informes y balances de manera periódica, presupuestos, análisis de inversión, auditoría y control interno, análisis del flujo de efectivo entre otras. Se encuentra compuesta por tres áreas organizacionales que son Auditoría, Contabilidad y Crédito.

La Dirección de Operaciones comprende las funciones que generan valor de los recursos que dispone el grupo corporativo. Sus funciones en una forma más genérica permiten la integración de los procesos del grupo, la sustentabilidad y posibilidad de ejecución de los procesos, gestión de recursos internos, estrategia relacionada al desarrollo de los productos y servicios. Se encuentra compuesta por cinco áreas organizacionales Compras, Importaciones, Cobranzas, Tecnología y Seguridad Física

La Dirección Comercial comprende las funciones relacionadas con la logística del negocio y cadena de distribución. Constituye básicamente el núcleo del negocio y es el área más visible del grupo. Se encuentra compuesto por cuatro áreas organizacionales Almacenes, Ventas al por Mayor, Bodegas y Fabricas.

Las áreas de apoyo ofrecen servicios a todas las demás direcciones o áreas organizacionales. Se encuentran aquí las áreas organizacionales de Recursos Humanos, Área Legal, Mercadeo y Publicidad

Dentro de la estructura el área organizacional de Tecnología posee su propia organización. En el nivel jerárquico más alto se encuentra el Gerente de Tecnología, que se encarga de la dirección del departamento

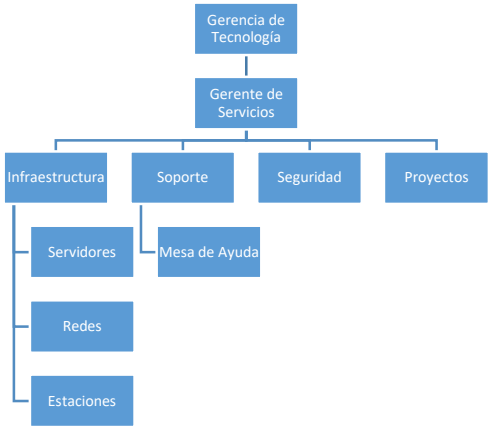


Figura 3.2 Organigrama - Área de Tecnología

3.2 Entorno Organizacional

El grupo empresarial CER centra sus operaciones en Ecuador, se encuentra posicionado entre las grandes cadenas de venta al detalle contando con un numero grande de almacenes. Su imagen organizacional es el de una empresa muy sólida económicamente y socialmente. Es una de las empresas que genera muchas oportunidades laborales y plazas de trabajo.

Dentro su portafolio de productos ofrece una alta gama de productos propios generados en sus modernas plantas de manufactura, productos de proveedores locales e importados. Posee una infraestructura muy alta

y madura en su cadena logística pues ha implementado una cadena de proveedores necesaria para cumplir con el suministro de sus operaciones.

El entorno interdepartamental dentro del grupo empresarial CER es de cooperación, existe una cultura organizacional madura. Existe un canal de comunicación muy eficiente gracias al uso de herramientas tecnológicas como G-Suite. Además, una intranet que permite la notificación oportuna de novedades y transmisión de notificaciones.

El área organizacional de Recursos Humanos posee muy buen canal de comunicación con el personal a través de estas herramientas, el canal de comunicación con los empleados es bidireccional y muchos de sus procesos se basan en el uso de herramientas tecnológicas como sitios web de autoaprendizaje, formularios, mesa de servicios, entre otras.

El área de Tecnología posee un canal de comunicación bastante desarrollado hacia toda la organización por medio del uso de herramientas tecnológicas. La mesa de servicios es la que permite

3.3 Recopilación de Requerimientos

El grupo empresarial CER, al igual que todas las empresas, ha observado una oportunidad para la expansión de su mercado a través de uso de tecnologías disponibles en internet. Esta oportunidad ha sido

debidamente analizada desde el punto de vista estratégico para los productos y servicios ofertados, pero del análisis se han desprendido riesgos inherentes al uso de nuevas tecnologías que hacen necesaria una revisión del marco de operación de los servicios que el área de Tecnologías de la Información ofrece.

El requerimiento inicial acerca del uso de un marco operacional estándar para los servicios se inicia en la gerencia de las áreas de Tecnologías. La gerencia del área ha expresado su preocupación acerca de la operación y administración de los servicios de apoyo. El control interno es calificado como no perceptible.

La gerencia del área de Tecnologías de la Información en el grupo empresarial CER es ocupada por el Ingeniero Victor Ibarra que ocupa el cargo desde hace ya seis años. Se realizó una entrevista a fin de establecer un panorama general del estado global del área, sus proyectos y su visión frente a los retos que tiene el área respecto de los requerimientos.

Del análisis de la entrevista se obtiene premisas que permitirán establecer directrices que nos permitan adoptar un marco de buenas prácticas. Las características del marco serán

Estandarizado. El marco final resultante debe estar alineado a las buenas practicas sugeridas en la Norma ISO/IEC 27001 – 2013, siendo esta

norma la referencia el estándar para la inclusión del marco en la operación del servicio de Directorio Corporativo y su uso posterior en todos los otros servicios del Grupo.

Extensible. El marco final resultante deberá proveer la capacidad de ser utilizado posteriormente en los otros demás servicios ofrecidos por el área de Tecnologías de Información, esto será posible debido al uso de la Norma ISO/IEC 27001 - 2013 y su capacidad para ser implementado para todo tipo de empresas sin importar su tamaño y por procesos independientemente de su complejidad.

Flexible. El marco final permitirá al Servicio de Directorio un entorno operativo que cumpla con el aseguramiento de los criterios de la información, pero a su vez permita fluidez en la operación del día.

Medible El marco dispondrá de los mecanismos necesarios para permitir medir eficazmente su operación a través de la evaluación del proceso, lo cual permitirá establecer las correcciones necesarias que otorguen calidad al servicio y posibiliten su mejora continua.

3.4 Identificación y Matriz de Interesados

De la entrevista con la Gerencia del Área de TI se obtiene la información necesaria para realizar la identificación y Matriz de Interesados necesaria para la realización del presente proyecto.

La identificación de interesados y establecer los canales adecuados es de vital importancia en la consecución del resultado deseado como muestra la Figura 3.3 Estrategias de Comunicación con Interesados:

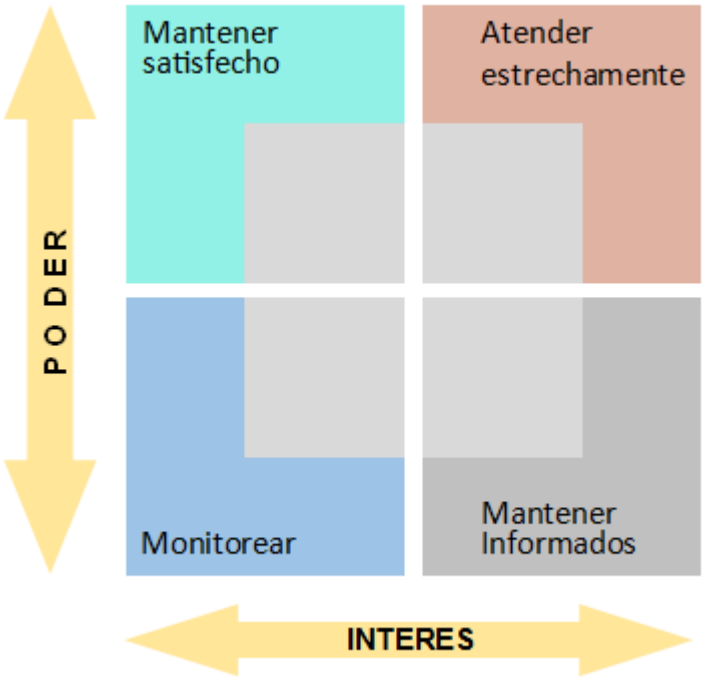


Figura 3.3 Estrategias de Comunicación con Interesados

Como principal interesado se identificó a Victor Ibarra, Gerente del área de Tecnología que toma parte vital en la concepción de este proyecto. El Gerente solicitó se le mantenga bien informado acerca de los hallazgos y se le notificará acerca de los avances o riesgos, además expresó su total apoyo para facilitar las tareas necesarias para el diseño e implementación del marco de Seguridad para el Servicio; por lo antes indicado se lo definió como principal interesado y patrocinador del proyecto.

La administración del servicio de Directorio Corporativo está a cargo de la Ingeniera Priscilla Mendoza, quien fue designada como responsable en el proyecto y facilitadora debido al conocimiento del servicio en aspectos tales como infraestructura, el conocimiento de la criticidad del servicio, además de sus conocimientos técnicos. Las actividades del diseño e implementación fueron coordinadas gracias a su colaboración y constituyó el principal recurso para el éxito del proyecto.

El jefe de Seguridad Luis Rodriguez y el Gerente de Servicios que respaldan la adopción de estándares que permitan una gestión y operación que avale la protección de la confidencialidad, integridad y disponibilidad de la información fueron considerados de alto interés para el desarrollo de este proyecto.

Se identificaron como interesados a los operadores del servicio y los ingenieros encargados de otros servicios que utilizan al servicio de Directorio como apoyo para el funcionamiento de sus aplicativos, pero su peso no es relevante para la elaboración del diseño e implementación del marco. Sus servicios son vitales para la operación y el desarrollo de las actividades del grupo empresarial por lo que se adoptara la estrategia de mantenerlos informados

Se calendarizó una reunión con los interesados del proyecto; el fin buscado fue involucrar a los interesados y notificar para notificar el interés

manifestado por la Gerencia de Tecnología y a la vez comunicar el inicio de las actividades. Los canales de comunicación establecidos para los interesados identificados para la realización de este proyecto se definieron como se registran en la Tabla 1 Matriz de Interesados - Estrategias de Comunicación:

Tabla 1 Matriz de Interesados - Estrategias de Comunicación

Cargo	Nombre	Roles
Responsable del Servicio	Priscilla Mendoza	Atender estrechamente
Operador Servicio 1	Carlos Villao	Monitorear
Operador Servicio 2	Carlos Carranza	Monitorear
Gerente de Tecnología	Victor Ibarra	Mantener satisfecho
Jefe de Seguridades	Luis Rodriguez	Mantener Informado
Usuarios Servicio	Otros Usuarios	Monitorear
Gerente de Servicios	Luis Ruiz	Supervisor del Servicio y el Cambio.

3.5 Recurso Humano: Responsabilidades y Roles

Durante las entrevistas realizadas se analizó la operación del servicio y se obtuvo los perfiles existentes y necesarios para la correcta operación del servicio.

El servicio de Directorio Corporativo es un pilar base en la operación de los servicios que generan servicios y producto. El servicio de directorio demanda una administración de alto nivel y a continuación se elaboró un

desglose de las tareas que deben realizarse para garantizar la operación correcta y segura de del servicio.

1. Administración de cuentas de usuarios, computadores y grupos.
2. Administración de recursos de red a través de la red.
3. Administración de directivas de Grupo (GPO)
4. Administración de sistema de nombres de dominio (DNS)
5. Administración de topología y replicación del directorio
6. Administración de configuración del directorio
7. Administración de la base de datos de esquema
8. Administración del catálogo Global
9. Administración de la seguridad del directorio

La Tabla 2 Servicio de Directorio Corporativo - Recurso Humano contiene el personal asignado para la operación del servicio:

Tabla 2 Servicio de Directorio Corporativo - Recurso Humano y Roles

Cargo	Nombre	Roles
Responsable del Servicio	Priscilla Mendoza	Administrador del Servicio
Operador Servicio 1	Carlos Villao	Respaldos Operación
Operador Servicio 2	Carlos Carranza	Operación
Gerente de Servicios	Luis Ruiz	Supervisor del Servicio y el Cambio.
Gerente de IT	Victor Ibarra	Aprobación del Cambio.

Las funciones se encuentran consolidadas en el siguiente diagrama descrito en la figura 3.4 Servicio de Directorio - Detalle de Funciones por Rol:

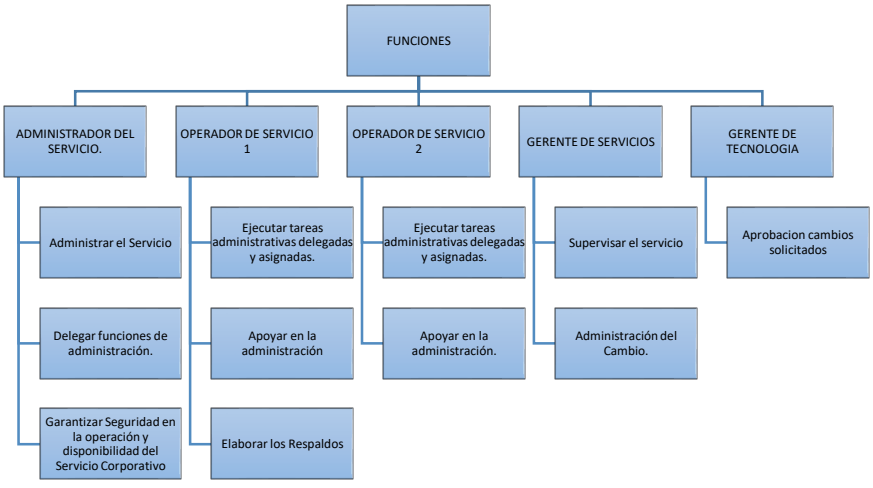


Figura 3.4 Servicio de Directorio - Detalle de Funciones por Rol

3.6 Levantamiento de Información. Arquitectura TI

El servicio de Directorio Corporativo se encuentra conformado por 4 sitios con la siguiente distribución geográfica apreciado en la Figura 3.5 Servicio de Directorio Corporativo – Esquema que lo detalla a continuación:

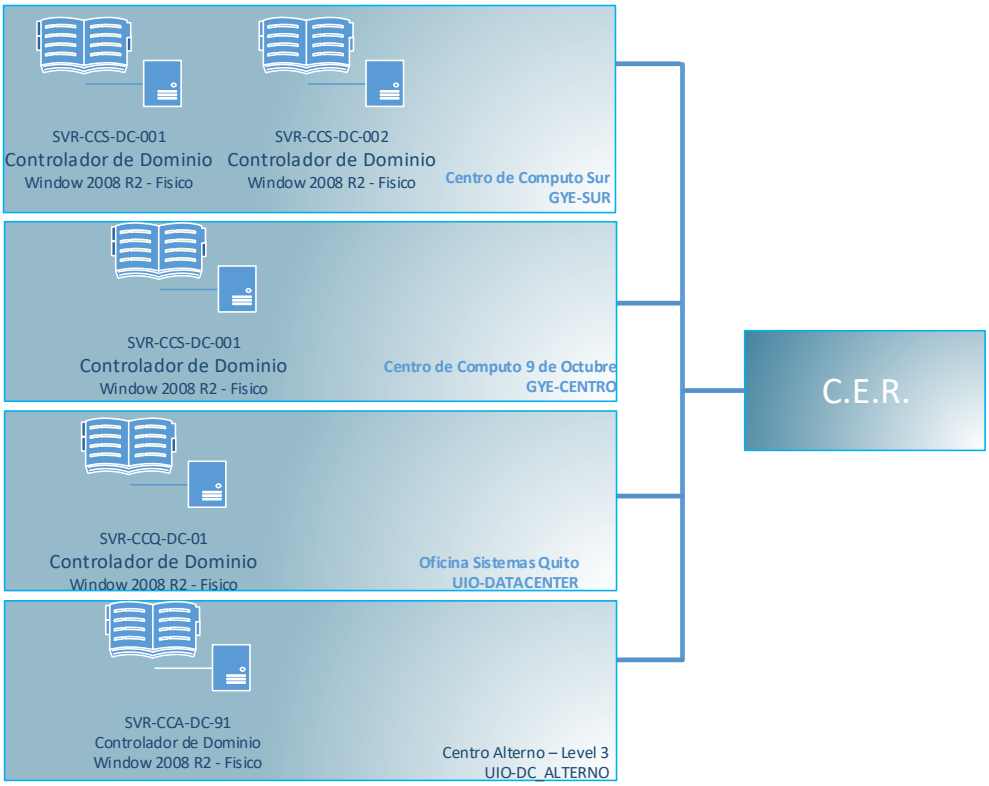


Figura 3.5 Servicio de Directorio Corporativo - Esquema

Guayaquil Centro. - (GYE-CENTRO) Este sitio de Active Directory ubicado en la ciudad de Guayaquil, sector Centro, dentro de un centro de datos secundario en el que se encuentran servidores redundantes que alojan servicios no críticos. El sitio de Active Directory contiene un

controlador de dominio que posee una copia del Catálogo Global y tiene activos roles de Active Directory Domain Services y DNS.

Por diseño Microsoft recomienda utilizar servidores controladores de dominio en sitios de gran concentración de usuarios o ubicaciones lejanas y está basándose en análisis y diseño inicial el administrador del servicio instaló un controlador de dominio que provee el servicio a la mayor concentración de usuarios dentro del grupo corporativo. El centro de datos posee dos enlaces de datos para garantizar disponibilidad de los servicios a los usuarios del edificio.

Quito Centro Altermo - (UIO-DC_ALTERNO) Este sitio de Active Directory ubicado en la ciudad de Quito, sector del Batán, dentro del centro de datos alterno de la empresa Level 3 en modalidad de hosting, Dentro del espacio contratado al proveedor Level 3 se encuentran servidores redundantes que alojan servicios del nucleo del negocio. El sitio de Active Directory contiene un controlador de dominio que posee una copia del Catálogo Global y tiene activos roles de Active Directory Domain Services y DNS.

La existencia de este sitio se debe a que en centro alterno existen albergados servidores que tienen servicios críticos para la operación. El centro de datos alterno constituye parte del plan de recuperación de desastres, he ahí la importancia de este controlador de dominio. El centro

de datos posee dos enlaces de datos para garantizar disponibilidad de los servicios a los usuarios del edificio.

Oficinas Quito – (UIO-DATACENTER) Este sitio de Active Directory ubicado en la ciudad de Quito, sector de la Carolina, dentro de un centro de datos secundario en el que se encuentran servidores redundantes que alojan servicios no críticos. El sitio de Active Directory contiene un controlador de dominio que posee una copia del Catálogo Global y tiene activos roles de Active Directory DomainServices y DNS.

Este sitio es necesario por diseño ya que se encuentra en otra ubicación geográfica y posee un número considerable de usuarios. El sitio es considerado clave en el plan de recuperación de desastres pues todas las funciones de los usuarios críticos para la operación de la empresa se encuentran reflejadas en los usuarios de las oficinas de Quito. El centro de datos posee dos enlaces de datos para garantizar disponibilidad de los servicios a los usuarios del edificio.

Guayaquil Sur - (GYE-SUR) Este sitio de datos de Active Directory se encuentra ubicado en la ciudad de Guayaquil, Sector del Centro Sur, dentro del centro de datos principal del grupo Corporativo. En este centro de datos se alojan todos los servidores principales y secundarios, con servicios críticos, prioritarios y secundarios necesarios para garantizar la operación. Es el más completo de los centros de datos, aunque todos

están equipados con las mismas tecnologías, climatización, generación eléctrica, sistema de alimentación eléctrica ininterrumpida, enlaces redundantes, seguridades perimetrales.

El sitio de Active Directory contiene dos controladores de dominio, entre ellos se encuentran distribuidos los roles FSMO, necesarios para el correcto funcionamiento de dominio. Dada la topología de la red de datos y la existencia de la mayor concentración de servidores este constituye el centro de datos más importante para las operaciones de la empresa, pero esta criticidad en la disponibilidad es administrada de buena forma a través de la distribución de servidores dentro de los otros centros de datos.

Los datos se encuentran resumidos en la Tabla 3 Servicio de Directorio Corporativo - Resumen de Esquema:

Tabla 3 Servicio de Directorio Corporativo - Resumen de Esquema

Sitios	Controlador de Dominio	Ubicación	Catalogo	Roles
GYE-CENTRO	SVR-CCS-DC-001	Centro de Computo 9 de Octubre	Global	AD / DNS
UIO-DATACENTER	SVR-CCQ-DC-01	Oficina Sistemas Quito	Global	AD / DNS
UIO-DC_ALTERNO	SVR-CCA-DC-91	Quito Centro Alterno	Global	AD / DNS
GYE-SUR	SVR-CCS-DC-001	Centro de Computo Sur	Global	AD / DNS
GYE-SUR	SVR-CCS-DC-002	Centro de Computo Sur	Global	AD / DNS

3.6.1 Administración de Activos

Durante la revisión inicial se comprueba que el área de Tecnología posee un control maduro de la infraestructura.

El equipamiento de la línea de servidores corporativos es de la empresa IBM, con el cual mantienen contratos de mantenimiento en la modalidad 24/7 y reemplazo de partes y piezas. La operación desde el punto de vista del hardware es óptima, no se han presentado problemas y es debido a los planes de mantenimientos preventivos realizados sobre los equipos, en lo que se le realizan limpiezas, reemplazo de partes, actualizaciones de firmware.

Los activos de software necesarios para la operación del servicio corporativo poseen contratos de licenciamiento y soporte con el fabricante.

Los sistemas operativos de los servidores controladores de dominio se encuentran incluido en el plan de mantenimientos de sistemas operativos corporativos y se realiza mantenimientos semestrales que incluyen escaneo de vulnerabilidades, solución a vulnerabilidades, actualizaciones y optimización.

La plataforma antimalware que es McAfee Threat Prevention y se controla desde la consola McAfee Policy Orchestrator que permite la administración completa de todas las estaciones y servidores corporativos a través de agentes. La consola permite automatizar muchas tareas dentro de los clientes tales como el control de dispositivos externos bloqueando los puertos USB, filtrado de firewall que permite únicamente los puertos mínimos necesarios para la operación, una búsqueda residente de programas activos en memoria y valida el acceso a los archivos, además de análisis completos del sistema operativo.

La plataforma para realizar respaldos es IBM Spectrum Protect, que permite un manejo de los respaldos. Esta herramienta es totalmente automatizada y tiene a su cargo la programación y ejecución de los respaldos de todos los servidores corporativos. Los servidores controladores de dominio.

3.6.2 Administración de la Continuidad del Negocio

El grupo empresarial CER mantiene una clara visión respecto de los procesos críticos para la operación y que les permite generar sus servicios y productos. Están identificados y los mismos se encuentran replicados en sus centros alternos y secundarios garantizando la disponibilidad de los mismos.

Durante el diseño e implementación del servicio de directorio corporativo, se tomó en cuenta las recomendaciones de Microsoft, respecto de la cantidad de usuarios y la distribución geográfica. Atendiendo a estos criterios es que se distribuyó los controladores iniciales a través de los centros de datos disponibles en ese momento. Pero el grupo empresarial ha crecido y el directorio se ha rediseñado de su configuración inicial a otra que abarca los nuevos nodos u oficinas brindando el servicio y a la vez atendiendo los criterios de seguridad de la información.

La arquitectura de directorio activo de Microsoft está diseñada para operar con un único controlador de dominio de ser necesario y en caso que los otros no estén disponibles. La empresa tiene la política de realizar dos pruebas semestrales moviendo sus procesos críticos a los servidores alternos y operando desde esas ubicaciones.

El servicio de directorio almacena todos sus objetos en la base de datos antes mencionada y llamada Catalogo Global. Esta base se respalda diariamente con el fin de garantizar la recuperación de la misma en caso de corrupción o perdida..

3.6.3 Administración del Cambio

El grupo empresarial CER, se encuentra calificado como uno de los más grandes de las cadenas de tiendas al detalle; esto implica que constantemente sus usuarios y servicios estén constantemente demandando cambios sobre el servicio. Los cambios de plataforma incluyen la administración de los objetos del directorio tales como usuarios, grupos, recursos, equipos, políticas, entre otras.

Existe un control en la solicitud de los mismos que es realizado manualmente a través de formularios impresos, en donde se registran los cambios solicitados con su respectiva justificación y las autorizaciones necesarias del solicitante. Este documento atraviesa un flujo manual de aprobaciones y al final de la misma se gestiona el cambio para que sea analizado por el administrador del servicio y su aplicabilidad. En caso de ser factible el cambio, acorde a los criterios de criticidad e impacto sobre las operaciones, el mismo se realiza o en caso contrario se justifica la razón de no realizarlo. Al final se notifica al solicitante el resultado de su solicitud.

En el caso de gestión de usuarios, los requerimientos son canalizados a través de correos electrónicos en los que el jefe

del departamento indica la necesidad de la creación de un usuario con el perfil necesario para que su subordinado puede ejecutar las tareas correspondientes a sus funciones. El cese de actividades de los empleados se ejecuta de similar manera.

3.6.4 Seguridad de la Información

Para el servicio de Directorio Corporativo basado en Active Directory de Microsoft las seguridades están dadas por la aplicación a través de los grupos de seguridad que permiten modificación en el aplicativo, la base de datos del catálogo global, los objetos dentro del directorio tales como usuarios, equipos, recursos o la base de datos. El acceso a los mismos está dado por la autenticación.

El fabricante garantiza la comunicación a través de protocolos seguros que permiten que el servicio de directorio cumpla con los criterios de seguridad de la información.

3.6.5 Operaciones

El grupo empresarial CER, posee una infraestructura para la generación de servicios y elaboración de sus productos, esta infraestructura comprende los edificios de oficinas centros de distribución y tiendas de venta al detalle que operan en diferentes horarios para ofrecer los mismos a sus clientes.

El grupo posee muchos procesos críticos plenamente identificados; el servicio de Directorio Corporativo es un servicio de apoyo de estos servicios críticos y prioritarios; por lo que su operación es continua e ininterrumpida. Los administradores y operadores del servicio trabajan en horario de oficina, pero disponen de ayuda de la mesa de servicios corporativas a la cual le han sido delegadas a través de las herramientas capacidad básicas como el reseteo de cuentas de usuarios entre otras con las correspondientes seguridades. Las actividades registradas y que no puedan ser atendidas en el primer nivel debido a su complejidad o la necesidad de autorizaciones son atendidas por el administrador y los operadores en sus jornadas de trabajo.

3.6.6 Privacidad y protección de la Información

En el grupo corporativo CER tiene muchos servicios y plataformas con datos confidenciales, el acceso a los mismo está dado por usuarios y contraseñas que garantizan a los usuarios a utilizar a la información necesaria para sus funciones.

Los servicios críticos y de apoyo utilizan al servicio de directorio corporativo como centro de autenticación, pues precisamente este es uno de las principales funciones del directorio. Como se indicó previamente el servicio de directorio asegura sus canales

y protocolos para garantizar el acceso no deseado a sus objetos y componentes. La base de datos y el esquema poseen seguridades de diseño que garantizan que no se accedan a los mismos sin las debidas credenciales.

Es importante destacar en este punto que el directorio por sí solo no protege la información, deben considerarse la concienciación a los usuarios acerca de la propiedad de la clave y sus responsabilidades, el uso de software legal, sistemas operativos seguros, protección malware y perimetral, entre otras..

3.6.7 Administración de los Problemas

El grupo corporativo CER posee una plataforma de mesa de servicios. La misma es uno de los servicios básicos para la operación. Este servicio es maduro y representa el canal de comunicación entre el área de Tecnología con los usuarios finales además de los proveedores.

Los problemas son reportados a la mesa de servicios corporativos y se generan solicitudes atendiendo a la a criticidad del evento acorde a los SLA ya definidos. La mesa de servicios corporativos asigna el requerimiento acorde a la naturaleza del evento reportado. Los problemas de hardware y sistema operativo de los controladores de dominio o referentes al servicio

son reportados al área de Servidores, quienes en colaboración del administrador del servicio realizan una evaluación detallada del caso y toman las acciones correctivas en caso de ser necesarias. Existen niveles de escalamiento en las solicitudes y tiene como límite superior a la Gerencia de Servicios y Gerencia de Tecnología.

Los problemas que no pueden ser solucionados por los ingenieros de soporte son reportados a los proveedores de servicios con los que se mantiene contratos de soporte y servicios. Los proveedores poseen ingenieros certificados que solucionan los problemas detectados y el ultimo nivel de revisión corresponde a casos abiertos directamente con el fabricante del hardware o software que necesita ser atendido.

La plataforma del Servicio de Directorio Activo es madura, los problemas que se detectan son errores conocidos, esto permite una rápida respuesta del equipo a cargo de la solución de los problemas.

CAPÍTULO 4

ANÁLISIS Y DISEÑO

El grupo corporativo CER opera posee un entorno de operación muy maduro en el cual sus procesos generan productos y servicios, esto se puede comprobar en los años de trayectoria de la empresa, su crecimiento y su constante expansión.

La preocupación del Área Tecnológica ha dado como origen el presente proyecto en el que se desea adoptar un esquema de seguridad que permitirá evaluar el entorno de operación de los servicios y que se haga extensible en lo posterior a todos los demás servicios y procesos adoptando normas.

En este capítulo procederemos a la revisión de los temas relacionados al Control de Accesos y Seguridad de la Operación descritos en la Norma ISO/IEC 27001 para el servicio seleccionado.

4.1 Control de Accesos.

4.1.1 Análisis, Diseño, Mejora de Política de Control de Accesos

El grupo Corporativo CER poseía dos políticas que apuntalan el control de accesos y son:

1. POL-SIS-071 CONTROL DE ACCESOS, en el Anexo 1
2. POL-SIS-014 POLITICA DE CONTRASEÑAS, en el Anexo 2

La política de control de accesos en vigencia permitía al área de Tecnología establecer lineamientos muy generales para aplicativos y procesos a su cargo. La última actualización de la política de control de accesos es de septiembre de 2016, fecha en la cual se efectuó su última revisión cuya versión era 02. La política ha permitido durante este tiempo operar a los servicios de apoyo, pero la política solo formula directrices para la operación de los servicios y su administración. El principal inconveniente de la política es que la misma de por si es estática, esto se evidencia en la falta de un ciclo de mejora continua.

Para política de Contraseñas existente en la empresa su última fecha de modificación era Agosto de 2010. Es una política muy robusta pues tiene directrices generales basadas en buenas técnicas de creación de contraseñas y lineamientos de protección de las mismas.

El proceso de análisis de la política de control de acceso y contraseñas se realizó en equipo con el Jefe de Seguridad, el Administrador del Servicio y Gerente de Servicios a través de una reunión Las dos políticas se evaluaron y se evidencia la existencia de controles dentro de las mismas a través de sus directrices. Durante el proceso de análisis los controles existentes dentro de la política se contrastaron contra lo implementado en el servicio de Directorio Corporativo logrando evidenciar uniformidad entre el servicio y la política. Cabe anotar que se evidencia dentro de estas políticas la falta de una revisión periódica de su contenido lo cual denota políticas estáticas que no evolucionan para acoplarse a las demandas de los constantes cambios en la operación del Grupo Corporativo.

El cambio necesario en la política de Control de Accesos es el de incluir una sección que indique que es prioritario ejecutar

procesos de evaluación interna para determinar la aplicación de lo incluido en la misma.

4.1.2 Definición y Análisis de Riesgos

Para el desarrollo de la fase de definición se procedió a realizar reuniones con el personal de Administración del Directorio, Gerente de Servicios y Jefe de Seguridad para determinar los riesgos que afecten a la operación del Servicio desde el punto de vista del control de Accesos enfocados en lo descrito en la NORMA ISO/IEC 27001 – 2013 para el servicio de Directorio Corporativo.

Es importante acotar que la implementación de Directorio de Microsoft, funciona en dos partes. En primer lugar, la autenticación que valida la identidad de los usuarios y solo se otorga acceso a los que realizan una autenticación efectiva. Seguido del uso de descriptores de seguridad en los objetos del directorio para determinar a qué objetos del directorio tiene derecho de acceso el usuario que se ha autenticado.

La Tabla 4 Servicios de Directorio Corporativo - Riesgos de Control de Acceso contiene un resumen de los riesgos obtenidos de la revisión con el grupo de interés:

Tabla 4 Servicios de Directorio Corporativo - Riesgos de Control de Acceso

Clasificación	Riesgo	Descripción
ROS-01	Cambios en configuración del Servicio por usuarios no autorizados	Cambios en la configuración del Servicio realizado por usuarios no autorizados
ROS-02	Acceso a la configuración del Servicio por usuarios no autorizados	Acceso a la configuración del Servicio por usuarios no autorizados.
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	Incumplimiento de los usuarios autorizados a las políticas de seguridad de claves y su uso responsable

4.1.3 Plan de Gestión de Riesgos

Una vez concluida la fase en la que se determinó los potenciales riesgos para el Servicio de Directorio Corporativo es necesario determinar la criticidad de los mismos.

La primera tarea fue convocar a los interesados y determinar escalas con valores que calificarían la frecuencia y el posible impacto dentro del servicio de cada riesgo encontrado como se aprecia en las tablas a continuación:

Tabla 5 Ponderación Frecuencia

Descripción	Ponderación
Alto	3
Medio	2
Bajo	1

Tabla 6 Ponderación Impacto

Descripción	Ponderación
Alto	3
Medio	2
Bajo	1

Los riesgos fueron evaluados y se obtuvo una calificación para todos ellos. El resumen de las calificaciones se muestra en la siguiente tabla:

Tabla 7 Riesgos Control de Accesos - Calificación

Clasificación	Riesgo	Frecuencia	Impacto	Calificación
ROS-01	Cambios en servicios o sistemas por usuarios no autorizados	1	3	3
ROS-02	Acceso a servicios o sistemas por usuarios no autorizados	2	2	4
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	2	3	6

El resultado obtenido es que el riego ROS-03 Perdida de confidencialidad de contraseñas de los usuarios es el riesgo de ponderación más alta. El resultado es coherente con el criterio de que los sistemas se vuelven cada vez más fuertes y los ataques que se realizan y obtienen mejores resultados son

aquellos en los que el objetivo es el usuario y sus credenciales. Una vez obtenidas sus credenciales el atacante puede obtener acceso a la información de los sistemas o servicios que tiene autorizado el usuario

4.1.4 Diseño de Controles para Control de Accesos

Para proseguir la siguiente fase se solicitó al grupo de interesados que se estableciera el apetito del riesgo para en base a esta métrica efectuar el diseño de los controles que permitirían gestionar de manera eficaz los riesgos. Se obtuvo una métrica en que los riesgos superiores a seis serán atendidos de manera prioritaria. Esta métrica se consultó con el Gerente de Tecnología que aprobó el valor para el apetito del riesgo.

Durante el análisis de la de las políticas de control de acceso y políticas de contraseñas en los pasos previos se evidencio que esta esta política contiene los controles necesarios para mitigar este riesgo el riesgo que con calificación superior a 6. El riesgo es ROS-03 Pérdida de confidencialidad de contraseñas de los usuarios

Los siguientes controles son incluidos en la norma ISO/IEC 27001 – 2013 y que podremos utilizar para tratar el riesgo

obtenido son mostrados en la Figura 4.1 Control de Accesos - Controles ISO 27001:2013:

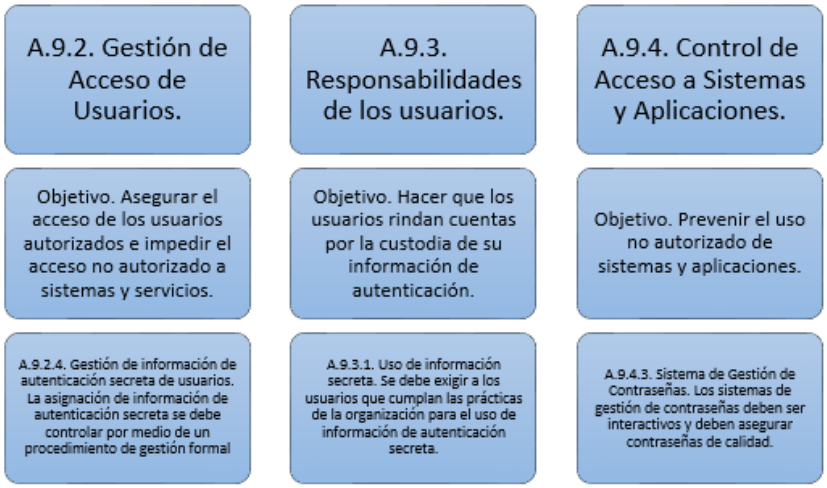


Figura 4.1 Control de Accesos - Controles ISO 27001:2013

Las políticas de control de accesos y la política de contraseñas vigentes definen controles para los accesos y se detallan en la siguiente tabla

Tabla 8 Control de Accesos - Controles Existentes

Riesgo	Política	Control
ROS-03	POL-SIS-071 CONTROL DE ACCESOS	Se asignará una identificación de usuario única a cada persona
ROS-03	POL-SIS-014 POLÍTICA DE CONTRASEÑAS	Todas las contraseñas a nivel de usuario y de sistema se deben ajustar a las directrices descritas a continuación. A. Construcción de la contraseña
ROS-03	POL-SIS-071 CONTROL DE ACCESOS	Se deberá forzar a los usuarios el cambio de su contraseña en su primer inicio de sesión
ROS-03	POL-SIS-071 CONTROL DE ACCESOS	Se deberá verificar la identidad del usuario antes de proveer una contraseña de reemplazo a través de su número de cedula y código de empleado
ROS-03	POL-SIS-071 CONTROL DE ACCESOS	El departamento de Recursos Humanos deberá realizar la suscripción de un Acuerdo de Confidencialidad con las

		nuevas adquisiciones de personal y personal que ya mantenga una relación de dependencia laboral con Grupo Empresarial CER
ROS-03	POL-SIS-071 CONTROL DE ACCESOS	El escritorio y lugar de trabajo de los usuarios no debe contener información relativa a sus credenciales de acceso
ROS-03	POL-SIS-071 CONTROL DE ACCESOS	Presentación de un mensaje de bienvenida como noticia de aviso general acerca del uso autorizado y no autorizado (login banner)
ROS-03	POL-SIS-071 CONTROL DE ACCESOS	No desplegar las contraseñas al ingresarlas
ROS-03	POL-SIS-071 CONTROL DE ACCESOS	Limitar número de intentos fallidos de inicio de sesión en un periodo de tiempo

4.2 Seguridad en la Operación.

4.2.1 Análisis, Diseño, Mejora y Procedimientos de Operación

El grupo empresarial CER posee varias políticas que conforman una base sólida para las operaciones de sus servicios, pero carentes de un proceso de auditorías internas o revisiones cíclicas que permitan encontrar errores en operaciones, riesgos de exposición y oportunidades de mejora. Esto se evidencio en el análisis del control de Accesos. Las políticas son enumeradas a continuación.

1. POL-SIS-023 GESTION DE SERVICIOS CORPORATIVOS, incluida en el Anexo 3

2. POL-SIS-020 POLITICA DE ANTIVIRUS, en el Anexo 4

3. POL-SIS-018 POLITICA DE ESCANEO Y GESTION DE VULNERABILIDADES incluida en el Anexo 5

4. POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS) incluida en el Anexo 6

La Norma ISO/IEC 27001 – 2013 posee un control en el que se revisa la Seguridad en la Operación, este aspecto es muy importante pues refleja la operación de los procesos, su documentación, la gestión de vulnerabilidades, respaldos. El análisis realizado en esta fase se centra en tres políticas resultantes del análisis de riesgos.

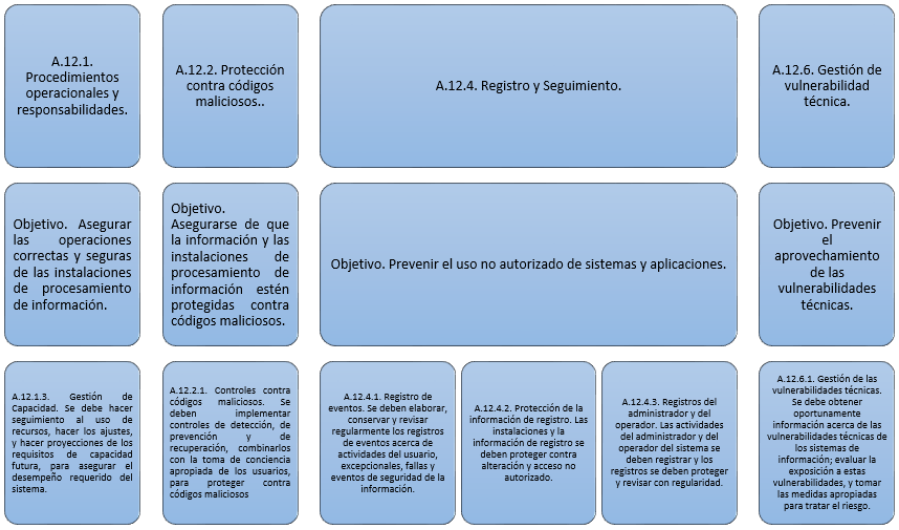


Figura 4.2 Seguridad en la Operación - Controles ISO 27001:2013

Las políticas de Antivirus, Escaneo y Gestión de Vulnerabilidades, Registros de eventos y Gestión de Servicios

fueron revisadas en conjunto con el Jefe de Seguridad y se agregaron puntos nuevos para que puedan ser consistentes con el ciclo de mejora continua y permitan la evaluación de los servicios. Las políticas se encuentran en los anexos.

4.2.2 Definición y Análisis de Riesgos

Al igual que en la etapa de control de accesos a través de una reunión con el grupo de interesados se determinaron los riesgos que afectan la operación del servicio de directorio Corporativo. La Tabla 10 Servicio de Directorio Corporativo - Riesgos Seguridad de la Operación contiene los riesgos encontrados y una breve descripción de cada uno de ellos.

Tabla 9 Servicio de Directorio Corporativo - Riesgos Seguridad de la Operación

Clasificación	Riesgo	Descripción
ROS-04	Deficiente documentación de procedimientos operativos del Servicio	Documentación deficiente o nula de los procedimientos operativos del servicio para uso del personal autorizado
ROS-05	Deficiente comunicación de los procedimientos operativos del Servicio	Difusión deficiente o nula de los procedimientos operativos asignados a los usuarios involucrados en la administración del Servicio acorde a su funciones asignadas.
ROS-06	Existencia de cambios no autorizados en la operación del Servicio	Gestión de Cambios deficiente o nula para autorización de cambios a realizarse en el Servicio
ROS-07	Fallos en Operación del servicio por mala gestión de Recursos	Gestión de Recursos de Hardware o Software deficiente o nula que permita establecer la salud del servicio y su disponibilidad
ROS-08	Fallos en Operación del servicio por cambios no probados	Gestión de cambios de puesta en producción de cambios deficiente o nula
ROS-09	Fallos en disponibilidad del Servicio debido a exposición a malware o	Gestión de Malware o vulnerabilidades deficiente o nula

	vulnerabilidades no gestionadas.	
ROS-10	Fallos en recuperación del Servicio desde respaldos	Gestión deficiente o nula de respaldos y su validez para garantizar la recuperación del servicio
ROS-11	Incapacidad para realizar actividades de trazabilidad de eventos debido a carencia de registros de auditoria	Gestión de Registros de Auditoria o Logs deficiente o nula que afectan directamente la trazabilidad de eventos

4.2.3 Plan de Gestión de Riesgos

El proceso de evaluación de los riesgos de Operación se realizó de manera similar al proceso efectuado en el control de accesos, se tomó como referencia la misma ponderación. La Tabla 10 Riesgos Seguridad en la Operación – Calificación resume los riesgos y su ponderación.

Tabla 10 Riesgos Seguridad en la Operación - Calificación

Clasificación	Riesgo	Frecuencia	Impacto	Calificación
ROS-04	Deficiente documentación de procedimientos operativos del Servicio	2	2	4
ROS-05	Deficiente comunicación de los procedimientos operativos del Servicio	2	2	4
ROS-06	Existencia de cambios no autorizados en la operación del Servicio	2	2	4
ROS-07	Fallos en Operación del servicio por mala gestión de Recursos	3	3	9
ROS-08	Fallos en Operación del servicio por cambios no probados	2	2	4

ROS-09	Fallos en disponibilidad del Servicio debido a exposición a malware o vulnerabilidades no gestionadas.	2	3	6
ROS-10	Fallos en recuperación del Servicio desde respaldos	2	2	4
ROS-11	Incapacidad para realizar actividades de trazabilidad de eventos debido a carencia de registros de auditoria	3	3	9

En la fase de análisis de control de accesos se obtuvo el apetito del riesgo, donde se especifica que se deben mitigar los riesgos con ponderación superior a 6. Los riesgos ROS-07 Fallo en la Operación del servicio por mala gestión de Recursos, ROS-09 Fallos en la disponibilidad del servicio debido a exposición a malware y ROS-11 Incapacidad para realizar actividades de trazabilidad de eventos debido a carencia de registros de auditoria.

4.2.4 Diseño Controles para Seguridad en la Operación

En esta fase se atenderán los tres riesgos obtenidos referentes a la seguridad en la operación. Los controles necesarios son descritos en la Norma ISO/IEC 27001 – 2013. La siguiente tabla muestra un resumen

Tabla 11 Seguridad en la Operación - Controles Existentes

Clasificación	Riesgo	Frecuencia	Impacto	Calificación del Riesgo	Control
ROS-07	Fallos en Operación del servicio por mala gestión de Recursos	3	3	9	Política de Gestión de Servicios Corporativos.
ROS-09	Fallos en disponibilidad del Servicio debido a exposición a malware o vulnerabilidades	2	3	6	Política de Antivirus Política de Escaneo y Gestión de Vulnerabilidades
ROS-11	Incapacidad para actividades de trazabilidad de eventos debido a existencia de registros de auditoria	3	3	9	Política de Administración de Registros de Seguridad _Logs

Las políticas corporativas descritas de antivirus, vulnerabilidades, gestión del servicio y registros de seguridad establecen dentro de sus lineamientos los siguientes controles descritos en la Tabla 11 Seguridad en la Operación - Controles Existentes.

Tabla 12 Seguridad en la Operación - Controles Existentes

Riesgo	Política	Control
ROS-07	POL-SIS-023 GESTION DE SERVICIOS CORPORATIVOS	Elaboración reporte acorde a las directrices de la POL-SIS-023 GESTION DE SERVICIOS CORPORATIVOS
ROS-09	POL-SIS-020 POLITICA DE ANTIVIRUS	La herramienta antivirus protegerá a los servidores y estaciones en tiempo real
ROS-09	POL-SIS-020 POLITICA DE ANTIVIRUS	La herramienta antivirus y anti spam realizará actualizaciones al menos una vez por día y envía alertas de correo electrónico
ROS-09	POL-SIS-020 POLITICA DE ANTIVIRUS	Las búsquedas de virus y malware serán realizadas una vez por semana en estaciones y servidores mediante programación de la herramienta a través de la consola centralizada
ROS-09	POL-SIS-020 POLITICA DE ANTIVIRUS	La consola administrativa deberá emitir registros, alertas y notificaciones para permitir una fácil administración y resolución de incidentes

ROS-09	POL-SIS-018 POLITICA DE ESCANEO Y GESTION DE VULNERABILIDADES	Se deberá realizar un escaneo de vulnerabilidades: 1.Trimestralmente, 2.Cuando se realicen cambios significativos en la infraestructura.
ROS-09	POL-SIS-018 POLITICA DE ESCANEO Y GESTION DE VULNERABILIDADES	Se deberán remediar todas las vulnerabilidad es con riesgo Alto y Critico seguidos de las Medianas, o todas con un una puntuación total de riesgo del Common Vulnerability Scoring System (CVSS) mayor o igual a 4.0 o se establecerá un control compensatorio para aquellas que no se puedan remediar
ROS-09	POL-SIS-018 POLITICA DE ESCANEO Y GESTION DE VULNERABILIDADES	Los Administradores de Servicios o Aplicaciones deberán controlar apropiadamente los recursos tecnológicos validando que las aplicaciones y sistemas sigan operando correctamente luego de ser actualizados
ROS-11	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	La capacidad de generación de Registro de Eventos deberá ser activada en todo dispositivo que tenga capacidad para generarlos y cuyas actividades conformen infraestructura de un servicio corporativo
ROS-11	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	Se deben capturar los eventos y tipos de datos especificados en la política directriz B Generación
ROS-11	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	Los Registro de Eventos serán retenidos por un periodo de tres meses mantenidos en línea preferiblemente. Luego de esto podrán ser destruidos
ROS-11	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	Los Registro de Eventos serán protegidos dentro de la infraestructura de gestión por las facilidades que esta ofrezca teniendo en cuenta que: • El acceso a ellos estará limitado al personal autorizado ya sea por sus tareas diarias o por ser parte del equipo de trabajo que realiza una investigación o auditoria. • Los archivos estarán protegidos de modificaciones no autorizadas. Se tratara de preservar el formato nativo de los mismos en lo que sea posible
ROS-11	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	Los eventos deberán estar disponibles para su análisis.

4.3 Diseño de Indicadores.

Durante el análisis realizado a la operación del servicio seleccionado respecto del control de acceso y la seguridad de la operación, se planeó el uso de algunos controles para poder mitigar los riesgos y realizar una

medición precisa de lo que está ocurriendo en las actividades claves del proceso de acuerdo a los riesgos estimados.

Para esta valoración se acordó con la Gerencia de Servicios realizar una ponderación porcentual del 100% cada riesgo critico asociado al Control de Accesos y de igual manera para cada riesgo critico asociado a la Seguridad de la Operación. Estos valores serán asignados acorde a si se evidencia el cumplimiento de mitigación para el riesgo como nos muestra la Tabla 12 Riesgos - Indicadores Mitigación.

Tabla 12 Riesgos - Indicadores Mitigación

Riesgo	Ponderación	Política
ROS-03	100%	Pérdida de confidencialidad de contraseñas de los usuarios
ROS-07	100%	Fallos en Operación del servicio por mala gestión de Recursos
ROS-09	100%	Fallos en disponibilidad del Servicio debido a exposición a malware o vulnerabilidades
ROS-11	100%	Incapacidad para actividades de trazabilidad de eventos debido a existencia de registros de auditoria

A su vez cada uno de los controles recibirá una parte proporcional para su calificación, como se observa en la Tabla 13 Controles - Indicadores Mitigación:

Tabla 13 Controles - Indicadores Mitigación

Riesgo	Ponderación	Política	Control
ROS-03	10%	POL-SIS-071 CONTROL DE ACCESOS	Se asignará una identificación de usuario única a cada persona
ROS-03	15%	POL-SIS-014 POLÍTICA DE CONTRASEÑAS	Todas las contraseñas a nivel de usuario y de sistema se deben ajustar a las directrices descritas a continuación. A. Construcción de la contraseña
ROS-03	10%	POL-SIS-071 CONTROL DE ACCESOS	Se deberá forzar a los usuarios el cambio de su contraseña en su primer inicio de sesión
ROS-03	10%	POL-SIS-071 CONTROL DE ACCESOS	Se deberá verificar la identidad del usuario antes de proveer una contraseña de reemplazo a través de su número de cedula y código de empleado
ROS-03	15%	POL-SIS-071 CONTROL DE ACCESOS	El departamento de Recursos Humanos deberá realizar la suscripción de un Acuerdo de Confidencialidad con las nuevas adquisiciones de personal y personal que ya mantenga una relación de dependencia laboral con Grupo Empresarial CER
ROS-03	10%	POL-SIS-071 CONTROL DE ACCESOS	El escritorio y lugar de trabajo de los usuarios no debe contener información relativa a sus credenciales de acceso
ROS-03	10%	POL-SIS-071 CONTROL DE ACCESOS	Presentación de un mensaje de bienvenida como noticia de aviso general acerca del uso autorizado y no autorizado (login banner)
ROS-03	10%	POL-SIS-071 CONTROL DE ACCESOS	No desplegar las contraseñas al ingresarlas
ROS-03	10%	POL-SIS-071 CONTROL DE ACCESOS	Limitar número de intentos fallidos de inicio de sesión en un periodo de tiempo
ROS-07	100%	POL-SIS-023 GESTION DE SERVICIOS CORPORATIVOS	Elaboración reporte acorde a las directrices de la POL-SIS-023 GESTION DE SERVICIOS CORPORATIVOS
ROS-09	20%	POL-SIS-020 POLITICA DE ANTIVIRUS	La herramienta antivirus protegerá a los servidores y estaciones en tiempo real
ROS-09	15%	POL-SIS-020 POLITICA DE ANTIVIRUS	La herramienta antivirus y anti spam realizará actualizaciones al menos una vez por día y envía alertas de correo electrónico
ROS-09	15%	POL-SIS-020 POLITICA DE ANTIVIRUS	Las búsquedas de virus y malware serán realizadas una vez por semana en estaciones y servidores mediante programación de la herramienta a través de la consola centralizada
ROS-09	10%	POL-SIS-020 POLITICA DE ANTIVIRUS	La consola administrativa deberá emitir registros, alertas y notificaciones para permitir una fácil administración y resolución de incidentes

ROS-09	20%	POL-SIS-018 POLITICA DE ESCANEO Y GESTION DE VULNERABILIDADES	Se deberá realizar un escaneo de vulnerabilidades: 1.Trimestralmente, 2.Cuando se realicen cambios significativos en la infraestructura.
ROS-09	10%	POL-SIS-018 POLITICA DE ESCANEO Y GESTION DE VULNERABILIDADES	Se deberán remediar todas las vulnerabilidad es con riesgo Alto y Critico seguidos de las Medianas, o todas con un una puntuación total de riesgo del Common Vulnerability Scoring System (CVSS) mayor o igual a 4.0 o se establecerá un control compensatorio para aquellas que no se puedan remediar
ROS-09	10%	POL-SIS-018 POLITICA DE ESCANEO Y GESTION DE VULNERABILIDADES	Los Administradores de Servicios o Aplicaciones deberán controlar apropiadamente los recursos tecnológicos validando que las aplicaciones y sistemas sigan operando correctamente luego de ser actualizados
ROS-11	20%	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	La capacidad de generación de Registro de Eventos deberá ser activada en todo dispositivo que tenga capacidad para generarlos y cuyas actividades conformen infraestructura de un servicio corporativo
ROS-11	20%	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	Se deben capturar los eventos y tipos de datos especificados en la política directriz B Generación •
ROS-11	20%	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	Los Registro de Eventos serán retenidos por un periodo de tres meses mantenidos en línea preferiblemente. Luego de esto podrán ser destruidos
ROS-11	20%	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	Los Registro de Eventos serán protegidos dentro de la infraestructura de gestión por las facilidades que esta ofrezca teniendo en cuenta que: • El acceso a ellos estará limitado al personal autorizado ya sea por sus tareas diarias o por ser parte del equipo de trabajo que realiza una investigación o auditoria. • Los archivos estarán protegidos de modificaciones no autorizadas. Se tratara de preservar el formato nativo de los mismos en lo que sea posible
ROS-11	20%	POL-SIS-062 ADMINISTRACION DE REGISTROS DE SEGURIDAD (LOGS)	Los eventos deberán estar disponibles para su análisis.

Las métricas serán utilizadas para el informe final a Gerencia de Tecnologías de modo que aporten a la percepción de control sobre la infraestructura y los procesos

4.4 Diseño Plan de Implementación de Controles

Una vez definidos los controles fue necesario determinar que controles están implementados y cuales deben analizarse para obtener la escala de tiempo necesaria para la implementación de los controles faltantes. En reunión con los interesados se estima la siguiente escala de tiempo necesaria para la implementación de los controles resumida en la siguiente tabla:

Tabla 14 Controles - Implementación y Validación

Actividad	Tiempo
Revisión Políticas de Acceso y Seguridad Operación	2 días
Diseño de Controles	2 días
Valoración de Controles Existentes	2 días
Implementación de controles faltantes y afinamiento de Controles existentes.	8 días
Entrega de Controles Implementados y Operativos	1 día

La estimación de tiempos fue acordada con el Administrador del servicio y corresponden a todas las actividades relacionadas.

4.5 Diseño de Plan de Auditoria Interna

A lo largo de esta etapa se ha evidenciado que no existe un proceso formal de auditoria interna que permita al área de Tecnología establecer

una situación actual de sus procedimientos y potenciar el proceso de mejora continua. Es necesario y vital que se efectué la guía para un proceso de evaluación que gestioné las oportunidades de mejora para esto diseñaremos lo siguientes documentos:

1. PLAN ANUAL DE AUDITORIAS, incluida en el Anexo 7
2. PRO-REC-003 AUDITORIAS INTERNAS SERVICIO DE DIRECTORIO, incluida en el Anexo 8
3. FORMATO DE PLAN DE AUDITORIAS, incluida en el Anexo 9
4. FORMATO DE HOJA DE RUTA ,incluida en el Anexo 10
5. FORMATO DE INFORME DE LA AUDITORIA INTERNA, incluida en el Anexo 11

4.5.1 Metodología

La Organización Internacional para la Estandarización establece en la ISO 9001:2015 las auditorías internas como el mecanismo para la evaluación que dispone una empresa para determinar si se cumplen los requisitos de sus sistemas a través de procesos, documentados, independientes y sistemáticos para lograr recolección de evidencias y su posterior análisis.

La norma solicita que nombre un auditor interno, que conozca de la norma y posea conocimiento de los procesos a auditar. La norma indica además que el auditor no puede ser la persona que audite su propio trabajo, debido a que es probable que no se obtenga una calificación objetiva y que el conocimiento previo de las acciones realizadas puede ocasionar que se pasen por alto detalles dentro del proceso que si pueden ser detectados por un tercero.

Se determinan los puntos que serán sujetos a la validación, se elaborará hojas de ruta o listas de control, que deben ser utilizador por el auditor designado para que se comprueben y documenten que se opera acorde a lo establecido. En caso de no cumplirse lo establecido se deberá registrar a través de una no conformidad que deberá reflejarse en el informe final de auditoria. Las no conformidades deben analizarse y efectuar acciones con el fin de aplicar acciones correctivas.

4.5.2 Diseño Plan de Auditoría Interna

Acorde a lo mencionado en la norma ISO 9001:2015 inicialmente se debe seleccionar un Auditor Interno, debido a su conocimiento de los sistemas internos y el entorno organizacional. Los auditores para durante este requerimiento serán el Jefe de

Seguridades y el autor del presente proyecto en calidad de consultor para la primera auditoría y en la calendarización posterior esta actividad será realizada por el personal designado por la Gerencia de Tecnología.

La frecuencia de las auditorias será semestral acorde a lo detallado en la Tabla 15 Auditorías Internas - Calendario y Programación:

Tabla 15 Auditorías Internas - Calendario y Programación

Auditoria	Inicio	Entrega de Informe	Auditor	Informe dirigido a
Semestre 1	Enero	Primera Semana Julio	Jefe de Seguridad Consultor	Gerente de Tecnología
Semestre 2	Julio	Primera Semana Agosto	Jefe de Seguridad	Gerente de Tecnología

La primera auditoria empezará en el mes de enero y se extenderá durante el mismo, será ejecutada por el auditor designado en acompañamiento por el autor del presente proyecto. El informe deberá ser entregado en la primera del mes de febrero al Director de Tecnología.

La segunda auditoria empezará en el mes de Julio y se extenderá durante el mismo, será ejecutada por el auditor designado. El

informe deberá ser entregado en la primera del mes de agosto al Director de Tecnología.

Auditorias extraordinarias pueden programarse acorde a los siguientes criterios:

1. Cambios en la plataforma que ameriten la consideración de una revisión del esquema de Seguridad.

2. Aplicación de acciones correctivas.

3. La planeación semestral no sea suficiente y sea necesario un proceso de auditoría adicional.

Los criterios para evaluación serán los descritos en el Esquema de Seguridad para el Servicio de Directorio Corporativo.

La ejecución del proceso de auditorías internas se ejecutará en las fechas programadas. El proceso arranca con la notificación del comienzo de la auditoria interna al personal que interviene en la operación del Servicio de Directorio.

A continuación, realizarán las actividades de la auditoría en compañía del responsable del Servicio. Se procederá a validar y valorar con la ayuda de la hoja de ruta, cada uno de los requisitos solicitados. Conforme se descubra la evidencia de no

conformidades u oportunidades de mejora, se registrarán estas en la hoja de ruta y aceptadas por el responsable del servicio.

Las conclusiones obtenidas serán registradas por el auditor en el Informe de la Auditoria Interna. El informe será revisado en conjunto con el Responsable del Servicio de Directorio Corporativo logrando que se reconozca la situación actual y la necesidad de tomar las medidas correctivas precisas. Se convocará a una reunión donde se aceptará el Informe de Auditoria Interna con la firma de todos los involucrados. El documento original se entregará al Gerente de Tecnologías. El administrador del servicio recibirá una copia para empezar a realizar el proceso de rediseño del esquema que se enfoque en solventar las no conformidades o aprovechas las oportunidades de mejora continua. Una vez realizado el proceso se deberá realizar una auditoría interna para determinar que las acciones correctivas han solucionado lo evidenciado garantizando que se cumple el ciclo de mejora continua.

Las responsabilidades de los diferentes implicados son las que se detallan a continuación:

Auditores Internos, notificar el comienzo de las Auditorías Internas. Auditar el Servicio conforme a lo establecido en el

procedimiento de Auditorías Internas. Elaboran el Informe de Auditoria Interna. Colaborar en formular acciones necesarias para solucionar las no conformidades o aprovechas las oportunidades de mejora.

Administrador del Servicio, Acompañar en el proceso de la auditoria en calidad de facilitador de las actividades agendadas. Comprender las no conformidades y oportunidades de mejora encontradas en el servicio. Formular acciones necesarias para aprovechas las oportunidades de mejoras o solventar las no conformidades.

Para todo el personal, colaborar en la auditoría en caso de que se solicite su colaboración.

4.6 Revisión, Mejora y Aprobación de Esquema

La ISO 27001 - 2013 establece la creación de una Declaración de Aplicabilidad o SOA por sus siglas en inglés, que es básicamente el documento recopilatorio de la evaluación y gestión de los riesgos con el fin de certificar lo actuado. El documento DECLARACIÓN DE APLICABILIDAD SERVICIO DE DIRECTORIO CORPORATIVO se encuentra en el Anexo 12

Para nuestro análisis la declaración de aplicabilidad se adaptó a una recopilación los resultados de todas las fases para su formalización en un documento. El Documento va detallando las acciones necesarias para garantizar que se efectué la mitigación de los riesgos resultantes del análisis realizado a lo largo de este capítulo.

También se recopilo todos los componentes del Esquema en el documento ESQ-SEG-001 ESQUEMA DE SEGURIDAD SERVICIO DE DIRECTORIO CORPORATIVO, incluido en el Anexo 13.

Cabe anotar que a lo largo de todas las fases se involucró a los interesados de manera que resulte mucho más fácil y comprensible para ellos y sobre todo para la Gerencia de Tecnología la aprobación de lo realizado a través de todas y cada una de las fases. El Gerente de Tecnología aprobó el esquema y la declaración de aplicabilidad para su difusión y puesta en marcha.

CAPÍTULO 5

IMPLEMENTACIÓN Y PRUEBAS

El presente capítulo se procederá a realizar las actividades de Implementación y Pruebas de del esquema diseñado para el Servicio de Directorio Corporativo.

5.1 Difusión de Políticas y procedimientos aprobados

En este paso se procedió a realizar la publicación oficial de los documentos aprobados y necesarios para la ejecución del esquema diseñado. Para la publicación se eligió utilizar la plataforma existente de publicación de políticas y procedimientos. El gestor documental es una plataforma madura y de amplio uso dentro del grupo corporativo llamado INFOCER observado en la Figura 5.1 Gestor Documentar – Infocer.

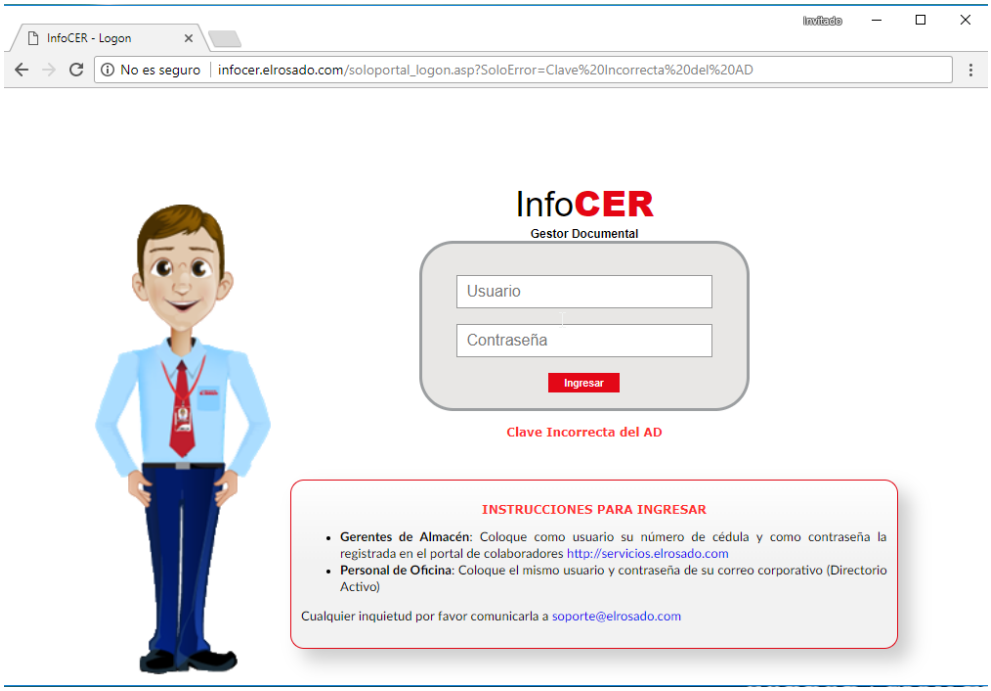


Figura 5.1 Gestor Documentar - Infocer

El gestor documental es un portal mediante el cual la compañía maneja las políticas y procedimientos existentes para que estos estén disponibles a los usuarios corporativos para su revisión. El mismo posee mecanismos de autenticación y registro de los documentos, su fecha de publicación, accesos por usuario y notificaciones electrónicas para mantener la comunicación con los usuarios de esta plataforma como se muestra en la Figura 5.2 Gestor Documental - Registro. La plataforma no es utilizada únicamente para este fin, entre otras de sus aplicaciones realiza la documentación de proyectos del área por lo que los usuarios están ampliamente familiarizados con el sistema de notificaciones y acceso a la herramienta. En nuestro caso se utilizó para la publicación de las

políticas, de modo que todos los usuarios estuvieran informados de las actividades y los cambios en las políticas, como se observa en la Figura 5.3 Gestor Documental – Políticas.

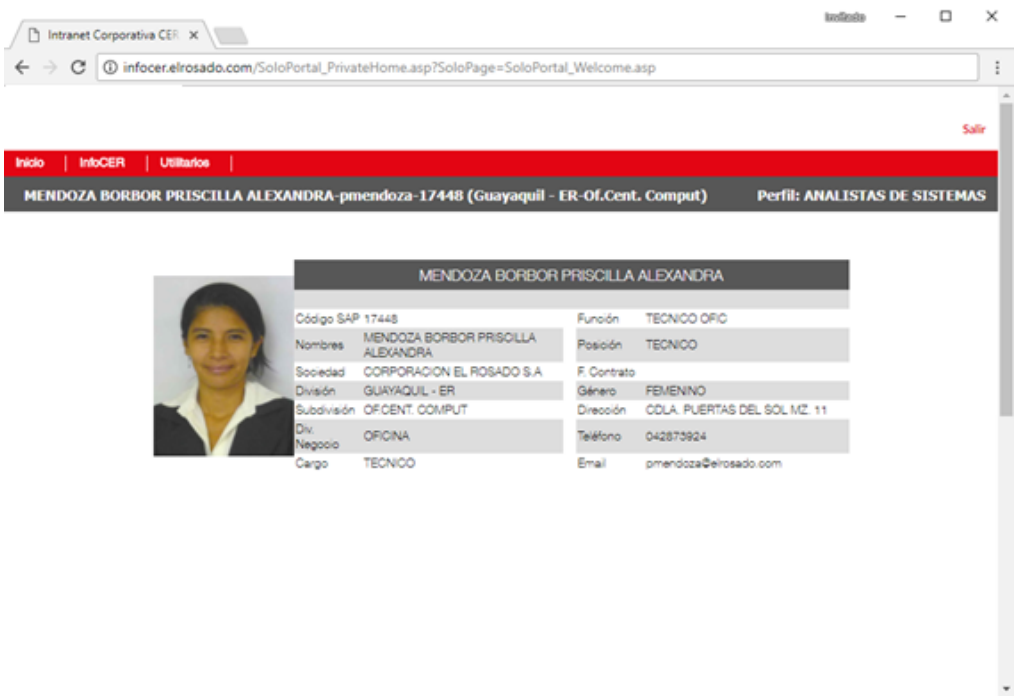


Figura 5.2 Gestor Documental - Registro

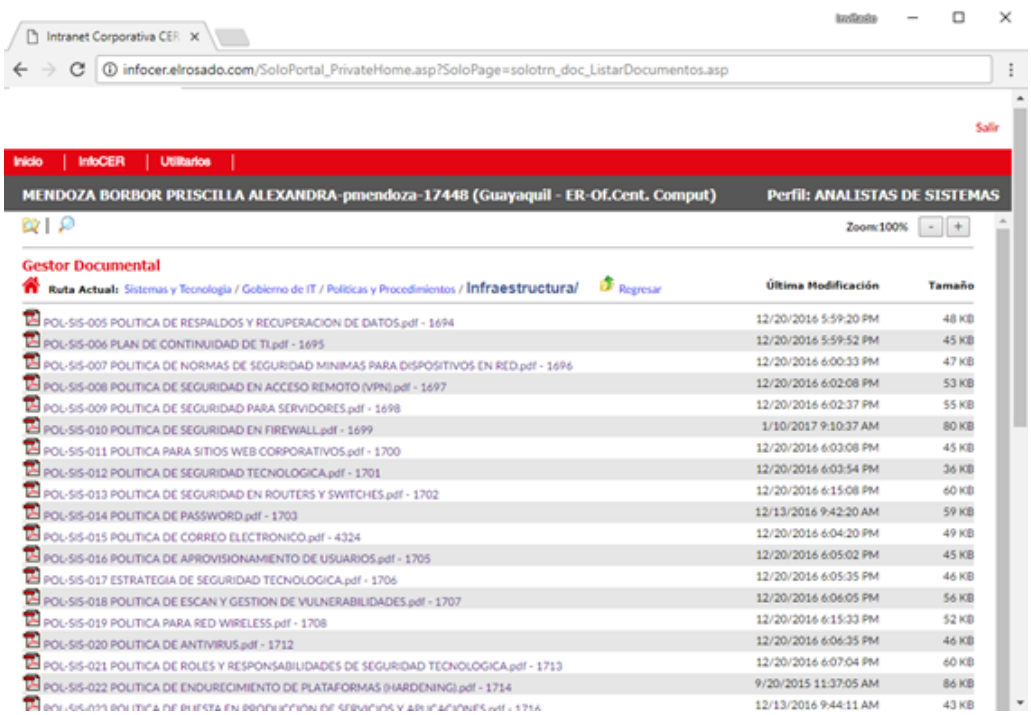


Figura 5.3 Gestor Documental - Políticas

Adicionalmente, dado que en el proceso de diseño detallado en el capítulo cuatro del presente proyecto, se involucró a todos los interesados y que las políticas ya existían el proceso de difusión fue transparente y alejado de dudas

5.2 Ejecución de Plan de Implementación de Controles

El siguiente paso dentro de las actividades de ejecución, es el plan de Implementación de Controles y corresponden a las actividades indicadas en el capítulo anterior de este documento.

En las actividades del plan intervienen el Administrador del Servicio, Jefe de Seguridad y el autor del presente documento en calidad de consulto.

El administrador dio inicio a las actividades desde la etapa del diseño donde hizo contrastar configuraciones del servicio de Directorio Corporativo contra los controles especificados en las políticas necesarias y que se encuentran vigentes.

El administrador procedió acorde a lo descrito en el plan realizando todas las etapas bajo la revisión del consultor y finalizó la entrega de los controles en concordancia con los tiempos pactados debido a que los controles estaban implementados por lo que no existieron controles faltantes y tampoco fue necesario el tiempo de su implementación destinando este tiempo a la mejora de los controles existentes.

En resumen, en esta etapa se validó la existencia de todos los controles y su desempeño será validado en la etapa de Auditorías Internas

5.3 Ejecución de Auditoria Interna

El proceso de auditoría interna es el mecanismo por el que este esquema puede obtener la información para realizar el proceso de mejora continua en el que está basada la Norma ISO/IEC 27001-2013. La validación de cada uno de los controles seleccionados para mitigar los riesgos detectados y calificados como críticos para la operación del servicio es la actividad principal en la auditoría.

La fase de ejecución de auditorías internas se desarrolló con el personal indicado dentro del PLAN ANUAL DE AUDITORIAS y el PROCEDIMIENTO DE AUDITORIA INTERNA DE SERVICIO DE DIRECTORIO CORPORATIVO, a saber, Jefe de Seguridad, Administrador del Servicio y el autor del presente documento.

El proceso arrancó con la notificación a los involucrados como se establece en procedimiento y prosiguió con la elaboración de los documentos necesarios descritos en el PROCEDIMIENTO DE AUDITORIA INTERNA DE SERVICIO DE DIRECTORIO CORPORATIVO. Seguido de las actividades de validación de controles, captura de evidencias, registro de no conformidades y oportunidades de mejora para su posterior análisis.

El registro de la ejecución de las auditorias se encuentra en los REGISTROS DE AUDITORIA incluidas en el anexo 14

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 Análisis de Resultados Auditoria Interna

El proceso de auditoría interna se realizó con facilidad gracias a la cooperación del equipo asignado para realizarlas. El proceso arrancó acorde al procedimiento con la creación del Plan de Auditorias Adjunto Anexo #, además de la Hoja de Ruta que contiene los controles que se deben validar para el servicio de Directorio Corporativo dentro del Grupo Corporativo CER.

El plan de Auditorias fue presentado al Gerente de Tecnología para su aprobación, se indicó que esta auditoria es de carácter extraordinario

porque no se encuentra dentro del Plan anual de Auditorias y corresponde a la fase de pruebas del Esquema diseñado para el servicio seleccionado. La Auditoría fue aprobada por la Gerencia de Tecnologías.

Durante el proceso de Auditorias se convocó al personal necesario para la recolección de evidencias de controles implementados. En esta fase se utilizó la Hoja de Ruta que poseía los controles necesarios para mitigar los riesgos críticos obtenidos del Análisis de Riesgos clasificados en base al apetito del Riesgo.

Los auditores internos registraron 22 controles necesarios para la mitigación de los riesgos dentro de la Hoja de Ruta. Al final del ciclo se encontraron 2 no conformidades y 5 oportunidades de mejora. El detalle y análisis de los mismos se ofrece a continuación.

ROS-03 Pérdida de confidencialidad de contraseñas de los usuarios

Control: El departamento de Recursos Humanos deberá realizar la suscripción de un Acuerdo de Confidencialidad con las nuevas adquisiciones de personal y personal que ya mantenga una relación de dependencia laboral con Grupo Empresarial CER

Se evidencia no Conformidad debido a la carencia de un Acuerdo de Confidencialidad del Grupo Corporativo con los usuarios. Se encuentra la existencia de un formato de Acuerdo de Confidencialidad dentro del

Área de Recursos Humanos que no es aplicado. Se solicitó al área Legal de la empresa el análisis de mismo, obteniendo como respuesta que el mismo carece de valor legal debido su contenido.

Es necesario implementar de manera urgente un acuerdo de confidencialidad, que tenga un amparo legal en favor del Grupo Empresarial CER. El mismo debe poseer el aval del área Legal para que se definan en él los obligaciones y responsabilidades asignadas al usuario cuando se le otorgan credenciales para el acceso y uso de los activos de información de propiedad de la empresa.

Control: Se deberá verificar la identidad del usuario antes de proveer una contraseña de reemplazo a través de su número de cedula y código de empleado

Se evidencia una oportunidad de mejora. Esta puede conseguir por medio de una implementación de autoservicio que permita a los usuarios recuperar u obtener sus contraseñas a través de sus respuestas a preguntas aleatorias en una plataforma especializada.

ROS-11 Incapacidad para realizar actividades de trazabilidad de eventos debido a carencia de registros de auditoria

Control: Los Registro de Eventos serán retenidos por un periodo de tres meses mantenidos en línea preferiblemente. Luego de esto podrán ser destruidos

Se observa durante la revisión que los servidores controladores de dominio que los registros de eventos están configurados por medio de políticas de directorio y se establece el tamaño máximo de los eventos de auditoria a 30 días con método de retención por días o un máximo de 195 Megabytes lo que ocurra primero. A partir los eventos comenzaran a ser eliminados para ser reemplazados por los del día en curso. La política de Administración de Registros de Seguridad expresa que se deben mantener registros de 90 días.

Control: La capacidad de generación de Registro de Eventos deberá ser activada en todo dispositivo que tenga capacidad para generarlos y cuyas actividades conformen infraestructura de un servicio corporativo

Control: Se deben capturar los eventos y tipos de datos especificados en la política directriz B Generación

Estos dos controles ofrecen una oportunidad de mejora debido a que se debería activar la generación de registro de eventos de auditoria en los equipos de cliente de manera que permite a los procesos de gestión de incidentes de seguridad obtener más información para los análisis

incrementando poder brindar un mejor detalle de lo acontecido de lo que se investiga.

Control: Los Registro de Eventos serán protegidos dentro de la infraestructura de gestión por las facilidades que esta ofrezca teniendo en cuenta que:

El acceso a ellos estará limitado al personal autorizado ya sea por sus tareas diarias o por ser parte del equipo de trabajo que realiza una investigación o auditoria.

Los archivos estarán protegidos de modificaciones no autorizadas. Se tratará de preservar el formato nativo de los mismos en lo que sea posible

Control: Los eventos deberán estar disponibles para su análisis.

Estos dos controles funcionan, pero es posible mejorar aún más la gestión de eventos de seguridad analizando e implementando un Sistema de Administración de Eventos e Información de Seguridad y adicionando un proceso de eficiente manejo de los aspectos relevantes a la seguridad permitirían un operación más segura y confiable.

Se procede a armar el informe acorde al Formato de Informe de la Auditoria Interna para su revisión con el administrador del Servicio. Durante la entrevista el Administrador del servicio está de acuerdo en lo

incluido dentro del informe y se evidencia que lo obtenido refleja la situación actual de la operación del Servicio de Directorio Corporativo

6.2 Presentación de Resultados

Una vez concluida la fase anterior es necesario realizar una reunión que cumple dos propósitos. La entrega del diseño implementado y el informe de Auditorías Internas. De esta manera se convoca a los interesados en el proceso de Diseño e Implementación del Esquema de Seguridad para el Servicio de Directorio Corporativo y el personal descrito en el procedimiento de Auditorías Internas.

Durante la reunión se realiza un repaso del esquema de Seguridad a manera de repaso para revisar las etapas del proyecto. La revisión resulta muy rápida debido a que se involucró a todos en el presente proyecto. Una vez concluida la revisión del esquema se procedió a entregar los resultados de la auditoria demostrando el propósito de este proyecto. Mejorar al proceso, a través de un proceso de mejora continua y una eficiente gestión del riesgo

6.3 Resolución de Observaciones

El Gerente de Tecnología se siente muy complacido con el resultado obtenido a pesar de notar la existencia de dos no conformidades, pero adicional expresa su conformidad con lo realizado pues su percepción no

estaba alejada de lo que ocurre en el servicio. Se dispone como conclusión de la reunión que se establezca el análisis de las recomendaciones para los resultados de la auditoria interna con una proyección a un mes de forma que esto mejore el nivel de mitigación de los indicadores para los riesgos críticos. Se atenderán en primera instancia las no conformidades y luego se harán estudios para determinar la factibilidad de adoptar las sugerencias en las oportunidades de mejora.

El Gerente de Tecnología manifiesta su compromiso en extender el marco hacia otros procesos de apoyo a fin de que se genere un empuje por la adopción de buenas prácticas en la operación que ayude al Grupo Empresarial CER a seguir ofreciendo sus productos y servicios a sus clientes.

CONCLUSIONES Y RECOMENDACIONES

1. Se logró cumplir el objetivo principal de este proyecto, desarrollar e implementar un esquema de seguridad para la operación del Servicio de Directorio Corporativo basado en la Norma ISO/IEC 27001 – 2013 para una empresa cuyo giro del negocio es la venta al detalle.

2. Se explicó de manera detallada conceptos básicos acerca de la información y sus propiedades disponibilidad, integridad y confidencialidad, los activos de información y su importancia para el desarrollo de las actividades y operaciones de la empresa

3. Se evidenció la importancia de adoptar normas como referencia o buenas prácticas para el diseño de esquemas de seguridad para la operación de servicios que avalen la protección de la información.

4. Se comprobó las características de las normas de Organización Internacional de Normalización, tanto su diversidad como flexibilidad para su utilización en empresas de todo tamaño y cualquier tipo de actividad, en especial la Norma ISO/IEC 27001 – 2013 que constituye el núcleo de este proyecto.

5. Se consiguió establecer la situación real del Servicio de Directorio Corporativo por medio de la identificación de los activos involucrados en la infraestructura del servicio y de las políticas o procedimiento existentes.

6. Se obtuvo la identificación de los riesgos potenciales del Servicio de Directorio Corporativo y determinar en un análisis la métrica respecto de su criticidad e impacto, tomando como referencia a Magerit.

7. Se consolidó la base necesaria para fomentar la implantación del proceso de mejora continua en la operación de los servicios del Grupo Empresarial CER.

RECOMENDACIONES

1. Es recomendable que se amplié el espectro del análisis del esquema de seguridad implementado hacia otros controles descritos en la Norma

ISO/IEC 27001 – 2013 por ejemplo, la administración de incidentes de seguridad, administración de recursos, administración de la continuidad del negocio entre otros. Por medio de este crecimiento en etapas se encamine a la organización hacia la adopción de un Sistema de Seguridad de la Información robusto que sea el pilar de apoyo de la empresa en su operación, generación y la producción de sus servicios y productos.

BIBLIOGRAFÍA

[1] Gartner, «Information Life Cycle Management (ILM),» [En línea]. [Último acceso: Septiembre 2017].

[2] ISOTools Excellence, «¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información?,» [En línea]. Available: http://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/.

[3] Iso27000.es, «¿Qué es un SGSI?,» [En línea]. Available: http://www.iso27000.es/sgsi.html. [Último acceso: Septiembre 2017].

[4] Miguel Angel Mendoza, «De la identificación y análisis a la gestión de riesgos de seguridad,» [En línea]. Available: https://www.welivesecurity.com/la-es/2015/07/16/analisis-gestion-de-riesgos-seguridad/. [Último acceso: Septiembre 2017].

[5] PDCA HOME, «Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua,» [En línea]. Available: https://www.pdcahome.com/5202/ciclo-pdca/. [Último acceso: Septiembre 2017].

[6] Deming, W. Edward, Calidad, Productividad y Competitividad. La Salida de la Crisis, Ed. Díaz de Santos, 1989.

[7] International Organization for Standardization, «ISO/IEC 27001 - Information security management,» 2013. [En línea]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. [Último acceso: Septiembre 2017].

[8] Gobierno de España, «PAE Portal de Administración Electrónica MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WoYJqkDOWM8. [Último acceso: Septiembre 2017].

[9] Microsoft, «Active Directory Structure and Storage Technologies,» [En línea]. Available: https://technet.microsoft.com/en-us/library/cc759186(v=ws.10).aspx. [Último acceso: Septiembre 2017].

ANEXOS

ANEXO 1

	CONTROL DE ACCESOS	Fecha:12/09/16
	POL-SIS-71	Versión: 03 Fecha:04-12-2017
	Departamento de Tecnología	
Elaborado por: Angel Elizalde	Revisado por: Luis Rodriguez	Aprobado por: Victor Ibarra

1.- Objetivo

Otorgar acceso a la información residente en los sistemas, aplicaciones y procesos únicamente a aquellas personas o aplicaciones a los que se haya concedido derechos de acceso plenamente justificados luego de su autenticación.

2.- Alcance

Todo el personal de Grupo Corporativo CER contratistas, proveedores y asociados en general que utilizan el Servicio de Directorio Corporativo como centro de Autenticación.

3.- Políticas

A. Administración de acceso a usuarios

1 Registro de Usuarios

- Se asignará una identificación de usuario única a cada persona;
- La creación de un usuario debe originarse por medio de una solicitud a través de la Mesa de Servicio y debe contar con la aprobación del jefe inmediato superior antes de ser procesada;
- No se deben crear cuentas genéricas o cuentas para uso compartido;
- Mantener un registro actualizado de todos los usuarios autorizados,
- Cambiar / eliminar los derechos de acceso para los usuarios que han cambiado de roles o han cesado;

2 Administración de privilegios

- Se debe crear el usuario utilizando el criterio de "menor privilegio", esto es, negar todo acceso por defecto para otorgarlos expresamente a los roles establecidos;

3 Administración de contraseña de usuarios

- El administrador o personal a cargo de la administración deberá crear contraseñas temporales en base a la política de seguridad: POL-SIS-014 Política de Contraseñas. Directriz A Construcción de la contraseña
- Se deberá forzar a los usuarios el cambio de su contraseña en su primer inicio de sesión;
- Se deberá verificar la identidad del usuario antes de proveer una contraseña de reemplazo a través de su número de cedula y código de empleado.

4 Aprovisionamiento de usuarios

- Los usuarios cesados deben ser desactivados a través de un proceso automático, solicitud del Jefe inmediato superior o el área de Recursos Humanos.

B. Responsabilidades de usuarios

1 Uso de contraseñas

- Según lo indicado en la política de seguridad: POL-SIS-014 Política de Contraseñas, Directriz B Protección de la contraseña
- El departamento de Recursos Humanos deberá realizar la suscripción de un Acuerdo de Confidencialidad con las nuevas adquisiciones de personal y

ANEXO 2

	POLÍTICAS DE CONTRASEÑAS	Fecha: 31/08/2010
	POL-SIS-014	Versión: 04 Fecha: 02/12/2017
	Departamento de Sistemas y Tecnología	
Elaborado por: Angel Elizalde	Revisado por: Luis E. Rodriguez	Aprobado por: Victor Ibarra

1.- Objetivo

El propósito de esta política es el de establecer un estándar para la creación de contraseñas fuertes, su protección y frecuencia de cambio.

2.- Alcance

El alcance de esta política incluye todo el personal que:

- Tiene, o es responsable por una cuenta de usuario (o cualquier forma de acceso que soporte o requiera una contraseña) en cualquier sistema que resida en la red en cualquier instalación de Grupo Corporativo CER.
- Tenga acceso a la red de Grupo Corporativo CER. o
- Almacene cualquier información de Grupo Corporativo CER.

3.- Políticas

3.1 General

- Todas las contraseñas administradas por el departamento de Tecnología y que cuenten con un sistema automatizado de gestión deben ser cambiados cada tres meses.
- Las contraseñas e IDs asignados a usuarios y administradores no deben ser publicados en redes sociales o aplicaciones de intercambio de información en comunidad. El envío de información de contraseñas y usuarios deben ser realizados por medios diferentes, en el caso de usar medios tecnológicos.
- No utilizar nombres comunes.

3.2 Directrices

Todas las contraseñas a nivel de usuario y de sistema se deben ajustar a las directrices descritas a continuación.

A. Construcción de la contraseña

Una contraseña robusta tiene las siguientes características:

- Contienen mayúsculas y minúsculas (ej.: a-z, A-Z)
- Contienen dígitos y caracteres especiales junto con letras ej: 0-9 !@#$%&*()_+|~-=\{}[]:";'<>?,./
- Tiene por lo menos ocho caracteres de largo (ej.: Oh-un3j3mpl0).

B. Protección de la contraseña

- No se utilizará la misma contraseña de cuentas pertenecientes a Grupo Empresarial CER para el acceso a sus cuentas personales.
- Todas las contraseñas son personales y deben ser tratadas como Información Sensitiva y Confidencial
- Todo usuario deberá realizar un cambio de contraseña si se sospecha que la cuenta de usuario o contraseña han sido comprometidas y notificar inmediatamente al área de Tecnología.

C. Desarrollo de Aplicaciones

ANEXO 3

	POLÍTICA DE GESTION DE SERVICIOS CORPORATIVOS	Fecha: 2/12/2017
	POL-SIS-023	Versión: 01 Fecha:
	Departamento de Sistemas y Tecnología	
Elaborado por: Angel Elizalde	Revisado por: Luis E. Rodríguez	Aprobado por: Victor Ibarra

1.- Objetivo

Definir los pasos necesarios para administrar y monitorear la calidad de los servicios tecnológicos, obteniendo así operación e infraestructura estable y segura de los servicios.

2.- Alcance

Administrador del Servicio de Directorio Corporativo.

3.- Política

1. El Responsable de la aplicación o servicio deberá emitir informes trimestrales de la operación de su servicio. Los informes deberán entregarse la primera semana de los meses de Enero – Abril – Julio – Octubre.
2. El reporte del servicio deberá incluir
   - Fecha
   - Nombre del Servicio
   - Nombre del Administrador
   - Infraestructura utilizada, servidores y sistemas operativos
   - Tiempos fuera de línea del servicio.
   - Mantenimientos programados
   - Incidentes
   - Observaciones
3. Revisión, el reporte debe ser revisado en conjunto con el Gerente de Servicios y Jefe de Seguridades, al final de su aprobación entregado a la Gerencia de Tecnología.

4.- Ejecución

Cualquier empleado, contratista o proveedor que haya violado esta política puede estar sujeto a acción disciplinaria que incluso puede llegar a terminación de relación laboral o contrato.

5.- Auditoría

Para el servicio de Directorio Corporativo se evaluarán los controles heredados de la presente política que sean necesarios y estén detallados en ESQ-SEG-001 Esquema de Seguridad

ANEXO 4

	POLÍTICA DE ANTIVIRUS	Fecha: 10/11/2010
	POL-SIS-020	Versión: 03
	Departamento de Sistemas y Tecnología	Fecha: 2/12/2017
Elaborado por: Angel Elizalde	Revisado por: Luis Ruiz	Aprobado por: Victor Ibarra

1.- Objetivo

Esta política interna define el control antivirus, actualizaciones del mismo y la periodicidad con la que se realizan las búsquedas de virus informáticos y malware en cada computador de Corporación El Rosado cubierto por el alcance de esta política.

2.- Alcance

Proteger los recursos organizacionales contra el ataque de virus informáticos y otro tipo de malware.

3.- Políticas

Se utilizará una única herramienta antivirus que permita actualizar, desplegar y monitorear a través de una consola de administración. El producto aprobado a la fecha de publicación de esta Política es McAfee Threat Prevention administrado con EPO (EPolicy Orchestrator)

Los siguientes son los requerimientos mínimos con los que debe operar la herramienta:

- La herramienta antivirus estará instalada en todos los servidores y estaciones descritas en el alcance.
- La herramienta antivirus protegerá a los servidores y estaciones en tiempo real.
- La herramienta antivirus y antispam realizará actualizaciones al menos una vez por día y envía alertas de correo electrónico.
- Las búsquedas de virus y malware serán realizadas una vez por semana en estaciones y servidores mediante programación de la herramienta a través de la consola centralizada.
- La herramienta antivirus centraliza las funciones en su consola de administración, lo que permite un ambiente centralizado de administración y monitoreo.
- La consola administrativa deberá emitir registros, alertas y notificaciones para permitir una fácil administración y resolución de incidentes.
- La retención de registros de eventos en el servidor antivirus se almacenará:
  (a) Eventos de menos de 3 meses en la base de datos del servidor Antivirus
  (b) Eventos mayores a 3 meses y menores a un año serán almacenados en un archivo de respaldo de la base de datos.
- El esquema de validación de usuarios y clave de la administración de la consola así como la población y actualización de equipos es contra la base del Directorio Activo.
- Sólo los administradores podrán realizar cambios en la configuración de la consola, detener los servicios de actualización antivirus, y las búsquedas programadas de virus siguiendo los lineamientos de la política Órdenes de Cambio.
- Los usuarios finales no tienen capacidad de cambiar la configuración de

ANEXO 5

	POLÍTICA DE ESCANEO Y GESTIÓN DE VULNERABILIDADES	Fecha: 29/07/2016
	POL-SIS-018	Versión: 05
	Departamento de Tecnología	Fecha: 2/12/2017
Elaborado por: Angel Elizalde	Revisado por: Luis Rodriguez	Aprobado por: Victor Ibarra

1.- Objetivo

Establecer la metodología para conducir los escaneos de vulnerabilidades de software de los dispositivos en la red y la administración de sus resultados.

2.- Alcance

Personal de Sistemas y Tecnología de Corporación El Rosado S.A. cubriendo las funciones referidas en esta política y/o administrando los recursos afectados.

3.- Política

3.1 Escaneo de vulnerabilidades

A. La evaluación consistirá en buscar puertos de comunicación activos, detección de sistemas operativos y detección de aplicaciones para identificar si existen vulnerabilidades conocidas y documentadas así como debilidades en la configuración de los sistemas.
B. Se deberá realizar un escaneo de vulnerabilidades:
   1. Trimestralmente,
   2. Cuando se realicen cambios significativos en la infraestructura.
C. El responsable de Seguridad TI validará los resultados para el efecto de remediar con el equipo de remediación las vulnerabilidades encontradas y establecer el alcance y la estrategia basado en la priorización de lo encontrado.

3.2 El proceso de remediación.

A. El personal que participará en realizar los procedimientos de remediación serán:
   a. El equipo a cargo de servidores en Infraestructura;
   b. Los Responsables de servicios o aplicaciones corporativas
   c. Consultor o proveedor contratado, en caso de ser necesario
   d. Seguridad Tecnológica;
B. Se deberán remediar todas las vulnerabilidad es con riesgo Alto y Critico seguidos de las Medianas, o todas con un una puntuación total de riesgo del Common Vulnerability Scoring System (CVSS) mayor o igual a 4.0 o se establecerá un control compensatorio para aquellas que no se puedan remediar
C. De ser factible se realizará la aplicación de parches y/o actualizaciones de manera automática utilizando herramientas existentes.
D. Después de aplicar el parche o la actualización se debrá validar que las amenazas han sido mitigadas ya sea por un nuevo escaneo o por revisión de la documentación del parche y el efecto que este debiera causar en el comportamiento del recurso.
E. Toda vulnerabilidad a nivel de aplicaciones será analizada por el equipo de desarrollo y su re-codificación se deberá efectuar siguiendo los estándares de desarrollo seguro que apliquen a su ambiente.

3.3 Los Administradores de Servicios o Aplicaciones.

A. Son responsables directos de que la aplicación a su cargo, en coordinación con los administradores de infraestructura, tenga la configuración apropiada.
B. Proveerán información al Equipo de Remediación para la evaluación del impacto luego de analizar los resultados de un escaneo de vulnerabilidades.

ANEXO 6

CORPORACIÓN EL ROSADO	ADMINISTRACIÓN DE REGISTROS DE SEGURIDAD (LOGS)	Fecha: 12/09/2016
	POL-SIS-062	Versión: 03
	Departamento de Sistemas y Tecnología	Fecha: 02/12/2017
Elaborado por: Angel Elizalde	Revisado por: Luis Ruiz	Aprobado por: Victor Ibarra

1.- Objetivo

Establecer responsabilidades para administrar los Registros de Eventos de Seguridad (Logs) de activos tecnológicos

2.- Alcance

Toda persona relacionada a la administración de servicios y servidores.

3.- Política

Para establecer y mantener una gestión exitosa de la infraestructura de administración de Registro de Eventos, se debe cumplir lo siguiente:

A. Grupos, Roles y sus responsabilidades

- Administradores de Servicios:
  - Deberán configurar la función de Registros de Eventos en los sistemas individuales, dispositivos de red, dispositivos de seguridad (Firewall, Intrusion Protection System, Antivirus, Data Loss Protection, etc.).
  - Realizar mantenimiento regular de los Registros de Eventos y el software que lo genera.
- Administradores de Seguridad:
  - Administración de la infraestructura de gestión de Registro de Eventos
  - Reportar sobre los resultados de las actividades de gestión de Registro de Eventos
  - Identificar cambios necesarios en los sistemas que generan los Registro de Eventos e informar a los administradores de los sistemas de cambios necesarios.
  - Validar con Administración de Data Center, que la información antigua en los Registro de Eventos está siendo archivada apropiadamente.
  - Utilizar la información de los Registro de Eventos al manejar diferentes tipos de incidentes
- Desarrolladores de aplicaciones:
  - Deben diseñar o adaptar aplicaciones para que realicen la grabación de eventos de seguridad de acuerdo a los requerimientos y mejores practicas
- Responsable de Seguridad Tecnológica:
  - Supervisa la infraestructura de administración de Registro de Eventos
- Gerencia de Tecnología:
  - Aprueba las políticas necesarias para el correcto uso de los recursos tecnológicos que generan, transmiten y almacenan los Registro de Eventos

B. Generación

- La capacidad de generación de Registro de Eventos deberá ser activada en todo dispositivo que tenga capacidad para generarlos y cuyas actividades conformen infraestructura de un servicio corporativo.
- Los siguientes tipos de acciones deben ser capturadas y monitoreadas:
  - Eventos de inicio de sesión de cuenta

ANEXO 7

ANEXO #

Grupo Corporativo CER	**PLAN DE AUDITORIAS INTERNAS DE ESQUEMA DE SEGURIDAD DE SERVICIO DE DIRECTORIO CORPORATIVO**	Fecha: 01-12-2017
	PRO-REC-003	Versión: 01
	Departamento de Tecnología	
Elaborado por: Angel Elizalde	Revisado por: Victor Ibarra	Aprobado por: Victor Ibarra

Objetivos de la Auditoría	1. Valorar la situación actual del esquema de seguridad para el servicio de Directorio Corporativo basado en la NORMA ISO/IEC 27001 – 2013 2. Identificar las No conformidades encontradas dentro de la operación del servicio de Directorio Corporativo respecto de su esquema de seguridad 3. Proponer acciones correctivas para las no conformidades
Alcance de la Auditoría	Esta auditoria tiene como alcance la operación del Servicio de Directorio Corporativo dentro de su esquema de seguridad basado en la NORMA ISO/IEC 27001 – 2013. Los controles a auditar son los descritos en el documento. DECLARACIÓN DE APLICABILIDAD Al finalizar la auditoria se entregará el Informe de Auditoría Interna que contiene; • Plan de Auditoria • Hojas de Ruta correspondiente a la Auditoria Interna en curso • Las observaciones obtenidas • Las no conformidades detectadas • Posibles acciones correctivas propuestas
Personas Involucradas	Luis Rodriguez (Jefe de Seguridades) Priscilla Mendoza (Administrador de servicio) Luis Ruiz (Gerente de Servicios) Victor Ibarra (Gerente Tecnología) Angel Elizalde (Consultor)

ANEXO 8

Grupo Corporativo CER	PROCEDIMIENTO DE AUDITORIA INTERNA DE SERVICIO DE DIRECTORIO CORPORATIVO	Fecha: 01-12-2017
	PRO-REC-003	Versión: 01
	Departamento de Sistemas y Tecnología	
Elaborado por: Angel Elizalde	Revisado por: Victor Ibarra	Aprobado por: Victor Ibarra

1. OBJETIVO

El presente procedimiento documentado define los pasos para ejecutar eficazmente el proceso de auditoría interna y comunicación de resultados.

2. DEFINICIONES

- **Auditor:** La persona que se encarga de realizar las auditorías del Esquema de Seguridad. La persona debe reunir las cualidades necesarias para el desempeño del rol.
- **Auditoria:** Las actividades de evaluación metódica y documentada para determinar que las disposiciones previamente establecidas, se realizan y analizar si estas son eficaces para alcanzar los objetivos propuestos.
- **Auditoría Interna:** Procesos de auditoria periódicos ejecutados por la organización para determinar que los objetivos propuestos se cumplen de manera eficaz.
- **No Conformidad:** Incumplimiento de los requisitos establecidos por esquema de seguridad para la operación del Servicio.
- **Hallazgos de auditoría:** Resultados obtenidos del análisis de la evidencia de la auditoria. Los hallazgos expresan conformidad o no conformidad con los requisitos establecidos.
- **Conclusión de la Auditoria:** Resultado final de un proceso de auditoría que entrega el auditor tras evaluar los hallazgos de auditoria.

3. EJECUCION

El auditor interno deberá realizar la notificación de inicio de actividades a:

- Administrador de Servicios
- Gerente de Servicios
- Gerente de Tecnología
- Jefe de Seguridad
- Personal Operativo del Servicio

El auditor interno debe realizar el plan de Auditoria correspondiente a la auditoria en el calendario. Deberá utilizar el FORMATO DE PLAN DE AUDITORIAS que se encuentra en los anexos de este procedimiento.

El auditor interno debe realizar la auditoria interna con el Administrador del

ANEXO 9

Grupo Corporativo CER	PLAN DE AUDITORIA INTERNA
	Departamento de Sistemas y Tecnología

Pág. __ de __

Auditoria Número	Alcance de la auditoria	Hoja de ruta	Auditor	Inicio Auditoria	Fin de Auditoria

APROBACION DE PLAN DE AUDITORIAS

Observaciones:	Aprobado por:
	Firma:
	Fecha:

ANEXO 10

Grupo Corporativo CER	HOJA DE RUTA
	Departamento de Sistemas y Tecnología

Pág. __ de __

Servicio Auditado:		N° Hoja de Ruta:
Responsable del servicio:	Auditor:	Fecha Auditoria:

Leyenda: 1 = Correcto 2= Oportunidad de Mejora 3= No Conformidad 4= Observaciones

	Requisito	1	2	3	4	Observaciones
RIESGO	CONTROL DE ACCESOS					
RIESGO	SEGURIDAD EN LA OPERACION					

APROBACIÓN DE HOJA DE RUTA

Observaciones:	Aprobado por Administrador del Servicio
	Firma
	Fecha

ANEXO 11

Grupo Corporativo CER	INFORME DE AUDITORIA INTERNA
	Departamento de Sistemas y Tecnología

			Pág. __ de __
Servicio Auditado:		Hoja de Ruta:	
Responsable del servicio:	Auditor:	Auditoria numero:	
		Fecha:	

N° de No conformidad	Descripción de la No Conformidad	Gravedad	Observación

APROBACION DE INFORME DE LA AUDITORIA INTERNA	
Observaciones:	APROBADO POR:
	Firma
	Fecha

ANALISIS Y RECOMENDACIONES

Riesgo

Control

<< >>

INDICADORES

Tabla de Ponderación de Mitigación por Riesgo

Riesgo	Ponderación	Política

Tabla de Ponderación de Mitigación de Riesgo con detalle por cada control

Riesgo	Ponderación	Política	Control

ANEXO 12

DECLARACIÓN DE APLICABILIDAD

La presente declaración de aplicabilidad contiene los riesgos resultantes de análisis realizado para el Servicio de Directorio Corporativo. Los interesados encabezados por la Gerencia de Tecnología aprueban el tratamiento de los riesgos descritos a continuación.

Riesgo	Descripción	Política	Control
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	Se asignará una identificación de usuario única a cada persona
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-014 POLÍTICA DE CONTRASEÑAS	Todas las contraseñas a nivel de usuario y de sistema se deben ajustar a las directrices descritas a continuación. A. Construcción de la contraseña
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	Se deberá forzar a los usuarios el cambio de su contraseña en su primer inicio de sesión
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	Se deberá verificar la identidad del usuario antes de proveer una contraseña de reemplazo a través de su número de cedula y código de empleado
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	El departamento de Recursos Humanos deberá realizar la suscripción de un Acuerdo de Confidencialidad con las nuevas adquisiciones de personal y personal que ya mantenga una relación de dependencia laboral con Grupo Empresarial CER
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	El escritorio y lugar de trabajo de los usuarios no debe contener información relativa a sus credenciales de acceso
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	Presentación de un mensaje de bienvenida como noticia de aviso general acerca del uso autorizado y no autorizado (login banner)
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	No desplegar las contraseñas al ingresarlas
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	Limitar número de intentos fallidos de inicio de sesión en un periodo de tiempo

ANEXO 13

Grupo Corporativo CER	ESQUEMA DE SEGURIDAD SERVICIO DE DIRECTORIO CORPORATIVO	Fecha: 01-12-2017
	ESQ-SEG-001	Versión: 01
	Departamento de Sistemas y Tecnología	

Elaborado por: Angel Elizalde	Revisado por: Victor Ibarra	Aprobado por: Victor Ibarra

1. OBJETIVO

El presente esquema documentado define los pasos para ejecutar eficazmente el esquema de seguridad de la información para el servicio de Directorio Corporativo

2. ALCANCE

Todo el personal involucrado en la operación y administración del Servicio

3. DIRECTRICES

1. Planeación
   - Definir Servicio a Evaluar
   - Definir Alcance
   - Realizar entrevistas con los interesados
   - Obtener Matriz de Interesados
   - Obtener Inventario de Activos
   - Definir y Seleccionar Riesgos
   - Análisis Diseño de Controles de Mitigación
   - Diseñar Plan de Auditoria
2. Ejecución
   - Implementar Controles Seleccionados
3. Medición
   - Ejecutar Plan de Auditorías Internas
   - Elaborar y Entregar Informe
4. Mejora Continua
   - Revisión de no conformidades y oportunidades de mejora.

ANEXO 14

Grupo Corporativo CER	ESQUEMA DE SEGURIDAD SERVICIO DE DIRECTORIO CORPORATIVO	Fecha: 01-12-2017
	ESQ-SEG-001	Versión: 01
	Departamento de Sistemas y Tecnología	
Elaborado por: Angel Elizalde	Revisado por: Victor Ibarra	Aprobado por: Victor Ibarra

1. OBJETIVO

El presente esquema documentado define los pasos para ejecutar eficazmente el esquema de seguridad de la información para el servicio de Directorio Corporativo

2. ALCANCE

Todo el personal involucrado en la operación y administración del Servicio

3. DIRECTRICES

1. Planeación
   - Definir Servicio a Evaluar
   - Definir Alcance
   - Realizar entrevistas con los interesados
   - Obtener Matriz de Interesados
   - Obtener Inventario de Activos
   - Definir y Seleccionar Riesgos
   - Análisis Diseño de Controles de Mitigación
   - Diseñar Plan de Auditoría
2. Ejecución
   - Implementar Controles Seleccionados
3. Medición
   - Ejecutar Plan de Auditorías Internas
   - Elaborar y Entregar Informe
4. Mejora Continua
   - Revisión de no conformidades y oportunidades de mejora.

ANEXO #

Grupo Corporativo CER	**PLAN DE AUDITORIAS INTERNAS DE ESQUEMA DE SEGURIDAD DE SERVICIO DE DIRECTORIO CORPORATIVO**	Fecha: 01-12-2017
	PRO-REC-003	Versión: 01
	Departamento de Tecnología	
Elaborado por: Angel Elizalde	Revisado por: Victor Ibarra	Aprobado por: Victor Ibarra

Objetivos de la Auditoria	1. Valorar la situación actual del esquema de seguridad para el servicio de Directorio Corporativo basado en la NORMA ISO/IEC 27001 – 2013 2. Identificar las No conformidades encontradas dentro de la operación del servicio de Directorio Corporativo respecto de su esquema de seguridad 3. Proponer acciones correctivas para las no conformidades
Alcance de la Auditoria	Esta auditoria tiene como alcance la operación del Servicio de Directorio Corporativo dentro de su esquema de seguridad basado en la NORMA ISO/IEC 27001 – 2013. Los controles a auditar son los descritos en el documento. DECLARACIÓN DE APLICABILIDAD Al finalizar la auditoria se entregará el Informe de Auditoría Interna que contiene: • Plan de Auditoria • Hojas de Ruta correspondiente a la Auditoría Interna en curso • Las observaciones obtenidas • Las no conformidades detectadas • Posibles acciones correctivas propuestas
Personas Involucradas	Luis Rodriguez (Jefe de Seguridades) Priscilla Mendoza (Administrador de servicio) Luis Ruiz (Gerente de Servicios) Victor Ibarra (Gerente Tecnología) Angel Elizalde (Consultor)

Grupo Corporativo CER	PROCEDIMIENTO DE AUDITORIA INTERNA DE SERVICIO DE DIRECTORIO CORPORATIVO PRO-REC-003 Departamento de Sistemas y Tecnologia	Fecha: 01-12-2017 Versión: 01
Elaborado por: Angel Elizalde	Revisado por: Victor Ibarra	Aprobado por Victor Ibarra

1. OBJETIVO

El presente procedimiento documentado define los pasos para ejecutar eficazmente el proceso de auditoría interna y comunicación de resultados.

2. DEFINICIONES

- **Auditor:** La persona que se encarga de realizar las auditorías del Esquema de Seguridad. La persona debe reunir las cualidades necesarias para el desempeño del rol.
- **Auditoria:** Las actividades de evaluación metódica y documentada para determinar que las disposiciones previamente establecidas, se realizan y analizar si estas son eficaces para alcanzar los objetivos propuestos.
- **Auditoría Interna:** Procesos de auditoria periódicos ejecutados por la organización para determinar que los objetivos propuestos se cumplen de manera eficaz.
- **No Conformidad:** Incumplimiento de los requisitos establecidos por esquema de seguridad para la operación del Servicio.
- **Hallazgos de auditoría:** Resultados obtenidos del análisis de la evidencia de la auditoria. Los hallazgos expresan conformidad o no conformidad con los requisitos establecidos.
- **Conclusión de la Auditoria:** Resultado final de un proceso de auditoría que entrega el auditor tras evaluar los hallazgos de auditoria.

3. EJECUCION

El auditor interno deberá realizar la notificación de inicio de actividades a:

- Administrador de Servicios
- Gerente de Servicios
- Gerente de Tecnología
- Jefe de Seguridad
- Personal Operativo del Servicio

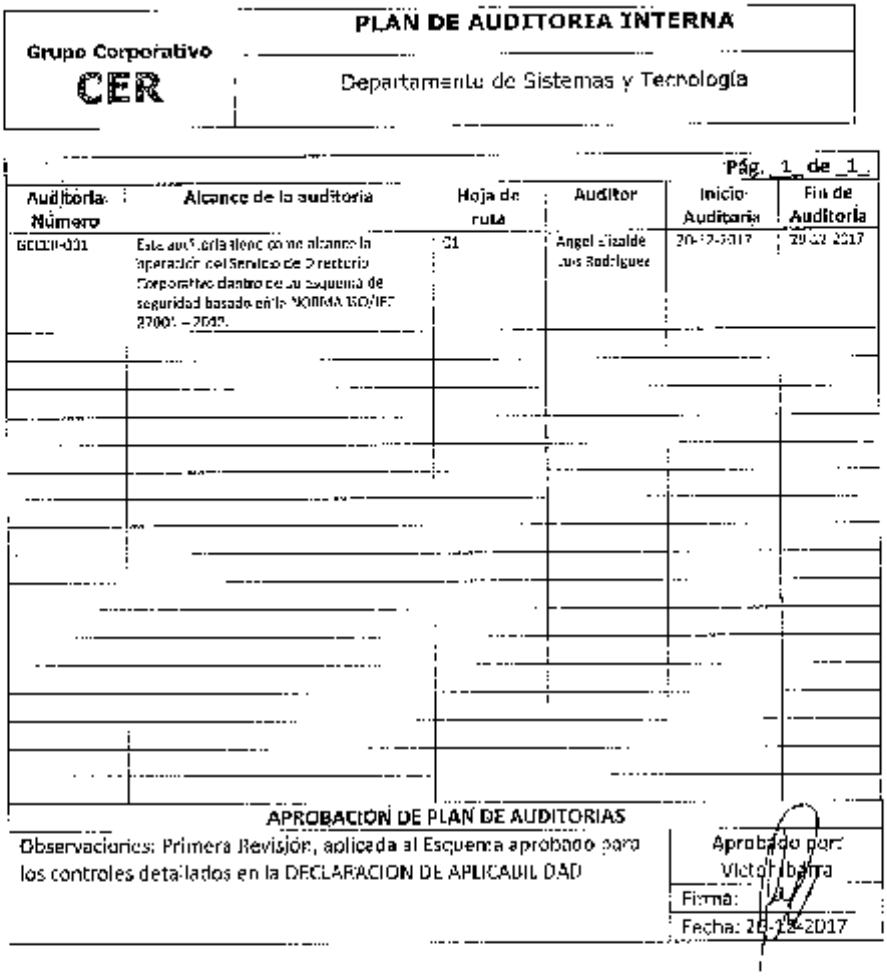
El auditor interno debe realizar el plan de Auditoria correspondiente a la auditoria en el calendario. Deberá utilizar el FORMATO DE PLAN DE AUDITORIAS que se encuentra en los anexos de este procedimiento.

El auditor interno debe realizar la auditoria interna con el Administrador del

DECLARACIÓN DE APLICABILIDAD

La presente declaración de aplicabilidad contiene los riesgos resultantes de análisis realizado para el Servicio de Directorio Corporativo. Los interesados encabezados por la Gerencia de Tecnología aprueban el tratamiento de los riesgos descritos a continuación.

Riesgo	Descripción	Política	Control
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	Se asignará una identificación de usuario única a cada persona
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-01A POLÍTICA DE CONTRASEÑAS	Todas las contraseñas a nivel de usuario y de sistema se deben ajustar a las directrices descritas a continuación. A. Construcción de la contraseña
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS 071 CONTROL DE ACCESOS	Se deberá forzar a los usuarios el cambio de su contraseña en su primer inicio de sesión
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	Se deberá verificar la identidad del usuario antes de proveer una contraseña de reemplazo a través de su número de cedula y código de empleado
ROS 03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	El departamento de Recursos Humanos deberá realizar la suscripción de un Acuerdo de Confidencialidad con las nuevas acquisiciones de personal y personal que ya mantenga una relación de dependencia laboral con Grupo Empresarial CLR
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	El escritorio y lugar de trabajo de los usuarios no debe contener información relativa a sus credenciales de acceso
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	Presentación de un mensaje de bienvenida como noticia de aviso general acerca del uso autorizado y no autorizado (login banner)
ROS-03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-SIS-071 CONTROL DE ACCESOS	No despiegar las contraseñas al ingresarlas
ROS 03	Pérdida de confidencialidad de contraseñas de los usuarios	POL-S S-071 CONTROL DE ACCESOS	Limitar número de intentos fallidos de inicio de sesión en un periodo de tiempo



PLAN DE AUDITORIA INTERNA

Grupo Corporativo
CER

Departamento de Sistemas y Tecnología

Pág. 1 de 1

Auditoria: Número	Alcance de la auditoria	Hoja de ruta	Auditor	Inicio Auditaria	Fin de Auditoria
GCCER-001	Esta auditoria tiene como alcance la operación del Servicio de Directorio Corporativo dentro de su Esquema de seguridad basado en la NORMA ISO/IEC 27001 – 2013.	01	Angel Lizalde Luis Rodriguez	20-12-2017	29-12-2017

APROBACION DE PLAN DE AUDITORIAS

Observaciones: Primera Revisión, aplicada al Esquema aprobado para los controles detallados en la DECLARACION DE APLICABILIDAD

Aprobado por: Victor Ibarra
Firma:
Fecha: 26-12-2017

Grupo Corporativo CER	HOJA DE RUTA
	Departamento de Sistemas y Tecnología

Pág. 1 de 1

Servicio Auditado:		N° Hoja de Ruta:
Servicio de Directorio Corporativo		01
Responsable del servicio:	**Auditor:**	**Fecha Auditoria:**
Priscilla Mendoza	AElizalde LRodriguez	20-12-2017

Leyenda: 1 = Correcto 2= Oportunidad de Mejora 3= No Conformidad 4= Observaciones

	Requisito	1	2	3	4	Observaciones
RIESGO	**CONTROL DE ACCESOS**					
ROS-03	Se asignará una identificación de usuario única a cada persona	X				Por diseño el directorio solo permite creación de username único, el cual se liga a una estación asignada al usuario. Anexo 1
ROS-03	Todas las contraseñas a nivel de usuario y de sistema se deben ajustar a las directrices descritas a continuación. A. Construcción de la contraseña	X				La Default Domain Policy tiene habilitado la complejidad Anexo 2
ROS 03	Se deberá forzar a los usuarios el cambio de su contraseña en su primer inicio de sesión	X				La creación de usuarios se realiza con la opción para que el usuario debe cambiar la contraseña en su primer inicio de sesión. Anexo 3
ROS-03	Se deberá verificar la identidad del usuario antes de proveer una contraseña de reemplazo a través de su número de cedula y código de empleado		X			El administrador y los proveedores solicitan datos de verificación, cedula y código de empleado para proceder a gestionar un cambio de contraseñas
ROS-03	El departamento de Recursos Humanos deberá realizar la suscripción de un Acuerdo de Confidencialidad con las nuevas adquisiciones de personal y personal que ya mantenga una relación de dependencia laboral con Grupo Empresarial CER			X		El acuerdo de confidencialidad para los usuarios no existe a pesar de estar implementado.

Grupo Corporativo CER	INFORME DE AUDITORIA INTERNA
	Departamento de Sistemas y Tecnologia

Pág. 1 de 1

Servido Auditado:		Hoja de Ruta:	
Servicio de Directorio Corporativo		01	
Responsable del servicio:	Auditor:	Auditoria numero:	GECER 001
Priscilla Mendoza	Angel Elizalde Luis Rodriguez	Fecha:	04-03-2018

N° de No conformidad	Descripción de la No Conformidad	Gravedad	Observación
001	Se deberá verificar la identidad del usuario antes de proveer una contraseña de reemplazo a través de su número de cedula y código de empleado ROS-03 Pérdida de confidencialidad de contraseñas de los usuarios	Oportunidad de Mejora	Se puede adoptar una herramienta de autoservicio que evite la interacción entre usuario y administradores para entrega de claves y recuperación
002	El departamento de Recursos Humanos deberá realizar la suscripción de un Acuerdo de Confidencialidad con las nuevas adquisiciones de personal y personal que ya mantenga una relación de dependencia laboral con Grupo Empresarial CER ROS-03 Pérdida de confidencialidad de contraseñas de los usuarios	No Conformidad	Se debe establecer de manera prioritaria la firma del acuerdo de confidencialidad por parte de área de Recursos Humanos que haya sido avalado por el área Legal. Todos los usuarios conocen de la política pero no existe un registro físico de aceptación.
003	La capacidad de generación de Registro de Eventos deberá ser activada en todo dispositivo que tenga capacidad para generarlos y cuyas actividades conformen infraestructura de un servicio corporativo ROS-11 Incapacidad para realizar actividades de trazabilidad de eventos debido a carencia de registros de auditoria	Oportunidad de Mejora	Se evidencia captura de eventos en los servidores controladores de dominio y servidores miembro, pero no en las estaciones, se podría mejorar la capacidad de análisis forense de incidentes de seguridad con esta información