**INTRODUCCIÓN AL ÁREA LÓGICA**

En el presente documento se especificará el en que consiste las tareas de auditoria de sistemas: Primero que todo, La seguridad puede dividirse, a grandes rasgos, en dos grandes bloques: seguridad física y seguridad lógica. Para salvaguardar los activos de la empresa no puede existir una sin la otra, ambas son complementarias. De nada sirve controlar los accesos físicos a las instalaciones para no sufrir percances y mantener a salvo los bienes, si un individuo puede acceder a la información confidencial de la compañía cómodamente desde el ordenador de su casa.

El área de seguridad lógica tiene como tarea aplicar mecanismos y barreras que mantengan a salvo la información de la organización desde su propio medio. Algunos de los controles utilizados en la seguridad lógica son:

* Se limita el acceso a determinados aplicaciones, programas o archivos mediante claves o a través de la criptografía.
* Se otorgan los privilegios mínimos a los usuarios del sistema informático. Es decir, sólo se conceden los privilegios que el personal necesita para desempeñar su actividad.

**ORIGEN DE LA AUDITORIA**

La presente auditoria se realiza con el fin de identificar el estado actual de las diferentes tareas y actividades realizadas por el sector lógico en las sucursales de San Rafael y Córdoba.

**OBJETIVOS Y ALCANCE**

**OBJETIVO GENERAL**

Revisar y evaluar las revisiones lógicas planteadas para determinar su eficiencia, seguridad y calidad de los diferentes equipos que son utilizados por el personal y así mismo brindar un cumplimiento de sus objetivos.

**OBJETIVOS ESPECIFICOS**

* Evaluar el sistema lógico.
* Determinar sistema dactilar
* Evaluar y administrar el sistema de cámaras de seguridad y alarmas
* Sistema de Login
* Generar roles para red LDAP
* Revisión lógica de administración

**ENFOQUE A UTILIZAR**

La presente Auditoria se realizará en las sucursales de San Rafael y Córdoba, directamente a las tareas realizadas por el sector lógico de la empresa.

Se aplica los procedimientos de Auditoria que se consideren necesarios para la supervisión y evaluación del sistema lógico para determinar cuál es su estado actual.

**MISION**

El área de Lógica de la empresa [nombre de la empresa], tiene por misión evaluar y revisar el adecuado uso y aprovechamiento de los recursos informáticos; La organización de los diferentes elementos informáticos que posee cada una de las sucursales, mediante el desarrollo, implementación y supervisión de su correcto funcionamiento

**METODOLOGIA EMPLEADA**

Para la realización de este informe de auditoría en los cuatro objetivos específicos a evaluar, se decidió que la metodología adecuada para obtener la información y evidencia utilizada fue:

1. Auditoria de evaluación del sistema lógico:
   * Verificar conexión de trabajadores
   * Asignación de conexiones en el área de diseño
   * Emplear nuevas mejoras en caso de necesitarlo
   * Tamaño y velocidad de la red
   * Información del testeo de envió de paquetes
   * Realizar ataques de prueba
   * Detectar problemas de protección de los datos

Verificar conexión de trabajadores:

Esta tarea se llevó a cabo para que los que trabajan en la Auditoría no presenten discontinuidades de conexión y no pierdan tiempo de su trabajo por no estar conectados. Algunos trabajadores tenían problemas de conexión, lo que involucró una reubicación de equipos tecnológicos para mejorar la versatilidad y eficacia del respectivo sistema lógico.

Realizar Ataques de Prueba:

Los ataques de prueba se realizaron para comprobar la seguridad del sistema lógico y poder sacar conclusiones para mejorar sus imperfecciones. Una de las imperfecciones que se encontró con el uso de **Black Box y White Box** fue que el sistema era vulnerable a ciertas herramientas informáticas, y esto permitió analizarlas con mayor dedicación y comprobar la capacidad de defensa de la Red y así perfeccionar el sistema ante las mismas.

Detectar Problemas de Protección de los Datos:

En esta etapa se detectaron problemas con los datos que resultaron redundantes y resulto conveniente la implementación de la reubicación de los datos para poder mejorar el problema (**Malware, Amenazas Persistentes Avanzadas y Botnets**), esto se llevó a cabo definiendo prioridades a los usuarios midiendo las precedencias de acceso con el uso de las tecnologías NetApp que nos sirvió para gestionar la seguridad de los datos de forma eficiente a lo largo de distintos niveles de almacenamiento y cumplir los requisitos más exigentes de objetivo de punto de recuperación de los Datos.

1. Determinar sistema dactilar:
   * Emplear automatización para el sistema
   * Encontrar un Software para la gestión
   * Perfeccionar la seguridad del sistema

Emplear Automatización para el Sistema:

La automatización permitió perfeccionar el Sistema para así poder recopilar datos rápidamente y con riesgos de fallos relativamente bajos, hoy por hoy los sistemas dactilares son muy precisos y tienen todos los datos almacenados en bases de datos con una seguridad muy alta, lo que permite una integridad de los datos constante.

Encontrar un Software para la Gestión y Perfeccionar la Seguridad del Mismo:

Para realizar la Auditoría se implementó el uso del Software **LiveScan** que recopila rápido (tarda aproximadamente 10 min en brindar la información de una persona) y fácilmente datos biométricos para el registro de las personas de la empresa con cada verificación de identidad y así poder tener un Sistema Dactilar seguro y factible. Este uso del sistema se llevó por pedido de una autorización para su respectivo uso e implementación.

1. Evaluar y administrar el sistema de cámaras de seguridad y alarmas:
   * Restringir acceso al software a los encargados de las cámaras
   * Establecer mecanismo de copias de seguridad
   * Implementación de RAID para discos de cámaras

Restringir Acceso al Software a los Encargados de las Cámaras:

Esta decisión se llevó a cabo para el beneficio de la seguridad de la Empresa, porque si hay muchas personas con este privilegio puede ser algo problemático dado que se presta para la asociación de los encargados para fines drásticos como es el robo de objetos, información, entre otros.

Establecer Mecanismo de Copias de Seguridad:

Las copias de Seguridad juegan un papel muy importante en una empresa como la que se está auditando, dado que existen muchos motivos por los cuales se pueden perder los datos, ya sea por robos, pérdidas, etc. La copia de seguridad se lleva a cabo por Google Drive mediante la contratación de un servicio de almacenamiento en la nube, esto permite el fácil acceso a la información para la restauración de la misma en caso de encontrarse con algún problema de extravío de los datos.

Implementación RAID para Discos de las Cámaras

La implementación que se llevó a cabo para el sistema de vigilancias fue el uso del RAID **10** que es una combinación entre el RAID **1** que funciona en forma de espejo y la del RAID **0** el cual reparte la información, con este uso cada disco tendría un disco de respaldo.

Otra alternativa en caso de que ocurran muchas fallas con los RAID, es la implementación de un sistema de vigilancia mediante un servidor de almacenamiento masivo (NAS, SAN, DAS por ejemplo) dependiendo de cual sea compatible con el grabador del sistema.

1. Sistema de Login:
   * Elaborar la lógica del formulario de Login
   * Realizar la vista del formulario
   * Emplear automatización para el sistema
   * Encontrar un software para la gestión
   * Perfeccionar la seguridad del sistema
2. Generar roles para red LDAP:
   * Ordenar el acceso al servicio
   * Buscar información en el Entorno de la Red
3. Revisión Lógica de administración:
   * Verificar prioridades de acceso a los recursos
   * Asignar prioridades de red a los usuarios
   * Firewalls y VPN de administración
   * Permitir comunicaciones aseguradas

**ALCANCE DE LA AUDITORIA**

De acuerdo a lo anterior nuestro alcance es:

1. Hacer auditoria sobre el sistema de información en las sucursales de San Rafael y Córdoba de la empresa [nombre de la empresa] determinando los riesgos posibles en cada uno de los elementos del área Lógica, donde se evaluará lo siguiente:
   * Datos: Evaluar, examinar y analizar el proceso de uso de datos mediante información recolectada
   * Usuarios: Evaluar y administrar el proceso de manipulación del sistema de información
   * Instalaciones Físicas: Examinar la seguridad y el buen uso de las instalaciones del área de cámaras y alarmas
   * Proceso: Analizar el cumplimiento de los procesos, según lo establecido por la entidad
   * Hardware: Evaluar el cuidado en el uso y los posibles riesgos lógicos de los equipos del área
   * Software: Examinar su buen funcionamiento, licencias y la seguridad de la información
2. Realizar la clasificación y análisis de la información suministrada por el sistema dactilar, sistema de Login y la revisión lógica de la administración presentado por las sucursales
3. Llevar acabo la evaluación del hardware y software mediante el sistema AIDA64 de dos equipos de cómputos con el fin de emitir los informes que suministra el programa