GNC

Gestión de Nacimiento y Cría



PLAN DE AUDITORÍA

Integrantes:

Emiliano Silva

Samuel Rodríguez

Agustín Rodríguez

Sebastián Mena

Índice

[Objetivos Generales 3](#_Toc534507826)

[Objetivos Específicos de la Auditoria 3](#_Toc534507827)

[Clasificación de la auditoria 3](#_Toc534507828)

[Alcance 3](#_Toc534507829)

[Metodología de la auditoria 3](#_Toc534507830)

[Recursos Físicos y tecnológicos 4](#_Toc534507831)

[Objetivos de control 4](#_Toc534507832)

[Elaboración de informe 4](#_Toc534507833)

[Vulnerabilidad de un sistema informático 4](#_Toc534507834)

[Importancia del Siniestro Informático 5](#_Toc534507835)

[Auditoria Forense 5](#_Toc534507836)

[Metodología de la Auditoria Informática Forense 5](#_Toc534507837)

[Normas relativas al informe de la Auditoria Informática 6](#_Toc534507838)

## Objetivos Generales

Realizar la auditoría a la red de datos que soportan los sistemas de información en la organización GNC.

## Objetivos Específicos de la Auditoria

Objetivos Específicos de la Auditoria

* Identificar el estado actual de la seguridad de parte lógica y física de la red de datos, en la organización GNC para verificar la existencia de las vulnerabilidades y amenazas existentes en los activos informáticos y de información.
* Elaborar un informe de los resultados obtenidos en la Auditoria que contenga los hallazgos

## Clasificación de la auditoria

Auditoria interna: La auditoría será llevada a cabo por personal de la empresa.

La auditoría será sobre la seguridad Informática, Comunicaciones y Redes.

## Alcance

* Aplicación de instrumentos de recolección de la información
* Realización de un Análisis y Gestión de riesgos informáticos.

Para la aplicación de instrumentos de recolección de la información se tendrá en cuenta:

-Diseño y aplicación de cuestionarios.

-Diseño y aplicación de listas de chequeo

Para la realización del análisis y gestión de riesgos de los hallazgos se tendrá en cuenta:

-Análisis de riesgos de acuerdo a las vulnerabilidades encontradas

-Gestión de riesgos

## Metodología de la auditoria

Fase de recolección de información:

Se revisará la documentación competente a todos los dispositivos utilizados en la red, así como los planos de la red. Además, también se deberá revisar la documentación respecto a la implementación de la red.

Fase de planeación:

Posterior a recoger esa información se deberá identificar y seleccionar los métodos y procesos adecuados.

Fase de ejecución:

Se aplicarán los métodos y procesos seleccionados, así como se realizará un análisis y gestión de riesgos sobre los hallazgos y vulnerabilidades encontrados con los métodos e instrumentos seleccionados.

Fase de auditoria o fase de resultados:2

Se examinará y recopilará la información, los resultados obtenidos en las pruebas y en la auditoria. Posteriormente se elaborará un informe el cual será presentado a la directiva de la Organización GNC.

## Recursos Físicos y tecnológicos

Para recursos de software:

-Software Libre para realizar pruebas de penetración y Ética Hacking, en este caso Kali Linux, el cual cuenta con:

-Herramientas para recolección de información.

-Herramientas para análisis de vulnerabilidades.

-Herramientas de explotación.

## Objetivos de control

Para la seguridad física:

•Control de áreas para los equipos de redes y comunicaciones, previniendo accesos inadecuados.

•Controles de utilización de los equipos de red y de comunicaciones, previniendo accesos inadecuados.

•Controles para la protección y tendido adecuado de cables y líneas de comunicaciones

Para la seguridad lógica

•Controles de contraseñas para limitar y detectar cualquier intento de acceso no autorizado a la red.

•Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.

•Técnicas de cifrado de datos donde haya riesgos de accesos impropios a transmisiones sensibles.

•Controles de Seguridad en la Red.

## Elaboración de informe

Se le presentará de informe a los altos directivos de la organización, con el máximo de detalle posible de todos los problemas y soluciones posibles recomendadas.

Posteriormente se elaborará el informe en donde se muestren los resultados a los responsables de la empresa, el informe presentado dará a conocer todos los puntos evaluados durante la auditoria. La conclusión tendrá como temas los resultados, errores, puntos críticos y observaciones de los auditores. Mientras que en el resumen se verán las posibles soluciones de esos puntos críticos y fallas, así como recomendaciones para el buen uso y también recomendaciones sobre la forma incorrecta de realizar algunos procedimientos.

Finalmente se presentará el informe a la directiva de la empresa.

### Vulnerabilidad de un sistema informático

Es la cualidad que le hace susceptible de ser afectado, alterado o destruido por algún hecho o circunstancia indeseada, de recibir algún daño o perjuicio en cualquiera de las partes o componentes, que afecte al funcionamiento normal o previsto de dicho sistema informático.

### Importancia del Siniestro Informático

En el área informática se pueden producir ataques, y esos ataques van contra la información la que puede sufrir distintos tipos de intromisión para agredirla en su confidencialidad, disponibilidad e integridad.

Cuando el siniestro informático es descubierto, debe asegurarse que hay la máxima información disponible este intacta, clara y que sea la correcta para que el auditor forense informático pueda realizar su trabajo correctamente.

$s importante que haya un auditor forense para evitar los siniestros informáticos y así evitar la destrucción, robo o alteraciones de información valiosa para el desarrollo económico y profesional de la empresa.

### Auditoria Forense

#### Objetivo de la Auditoria Forense

La Auditoria Forense proporciona recomendaciones para asegurar la salvaguarda de los activos de los sistemas de información, manteniendo la integridad de los datos y lograr los objetivos de la organización en forma eficiente y eficaz.

#### Auditoria Informática Forense

La Auditoria Informática Forense puede definirse, como la ciencia que se encarga de analizar sistemas informáticos en busca de evidencia

Es la aplicación de técnicas y herramientas de hardware y software para determinar datos potenciales o relevantes.

### Metodología de la Auditoria Informática Forense

Se debe de establecer una metodología que este, acorde con las irregularidades encontradas.

#### Evidencia

Todo ataque deja evidencia que permite identificar lo ocurrido, lo mismo ocurre con la evidencia computacional.

La evidencia computacional es única, cuando se la compara con otras formas de “evidencia documental”. A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original

#### Evidencia digital

Es un tipo de evidencia física. Está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.

Evidencia Digital: Información de valor para el caso que es transmitida o guardada en formato digital.

* Evidencia digital original
* Evidencia digital duplicada

Objetos de datos: Información valiosa relacionada con el caso asociada a objetos físicos. Debemos procurar trabajar sobre imágenes de discos, esto es así para no trabajar a nivel de sistema de ficheros, pues podemos perder información valiosa.

#### Características del informe

El texto del informe sobre una investigación de auditoria forense debe reunir las siguientes características:

Debe presentarse por escrito. En él debe estar claramente:

* La descripción de los hechos, objeto del peritazgo y deben distinguirse de los pronósticos o conjeturas
* Las operaciones técnicas realizadas.
* Los principios científicos en que se fundamenta.
* Las conclusiones debidamente comprobadas y sustentadas que servirán al juez para valorar la prueba.

Si ciertos hechos parecen contradictorios, deben ser ampliamente discutidos. Un conjunto de hechos debe compararse con otro para llegar a una conclusión, y deben especificarse cuidadosamente las razones que se tengan para ignorar las implicaciones de cualquier hecho.

El informe debe excluir toda referencia a aquellas características de las cuentas que se presten a controversia, a menos que tengan relación con las conclusiones del informe.

### Normas relativas al informe de la Auditoria Informática

Contener observaciones o hallazgos, identificando causas y efectos de los mismos, conclusiones y recomendaciones correspondientes, con señalamiento expreso de que el trabajo ha sido realizado conforme a las Normas Generales de Auditoria.

Ser firmado por el nivel directivo o gerencial, competente para notificar los resultados.

Redactarse de manera objetiva, persuasiva y constructiva y en forma clara, precisa y concreta, insertarse los detalles necesarios que contribuyan a evitar equívocos y ambigüedades.

El informe debe ser presentado oportunamente, a objeto de que la información en él contenida tenga actualidad, utilidad y valor para que las autoridades a quienes corresponda, adopten las medidas inmediatas tendentes a corregir las deficiencias señaladas

En conclusión, las normas internas de auditoria, exigen que el trabajo realizado de auditoria, se establezcan normas mínimas para la ejecución del trabajo, ayuda a emitir una opinión razonable sobre el dictamen de dicho trabajo, evaluando el cumplimiento, leyes, reglamentos, y demás normativas aplicables a la organización a la cual se ha ejecutado una auditoria.

Referencias:

<http://www2.infotelecom.es/~ecampins/Treballs%201r/Virus/hackers.html>

<http://hackersycrackers-yi.blogspot.com/2008/09/>

<https://www.monografias.com/trabajos/hackers/hackers2.shtml>

<https://sites.google.com/site/misitiokol/tipos-de-ataques>

<http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442009000200025&script=sci_arttext>

<https://www.seguridadpublica.es/2010/12/informatica-forense-generalidades-aspectos-tecnicos-y-herramientas/>