**PROYECTO SEGURIDAD INFORMATICA**

**PRESENTADOR POR:**

**JHON ALEJANDRO GIRALDO MEJIA**

**ASDRUBAL ANDRES VELEZ VELEZ**

**LUIS EDIN IBARGUEN MOSQUERA**

**CARLOS ALBERTO LONDOÑO**

**INGENIERO EN SISTEMAS**

**CORPORACION DE ESTUDIOS TECNOLOGICOS DEL NORTE DEL VALLE**

**CIENCIAS INFORMATICA, TECNOLOGICA E INGENIERIA**

**INGENIERIA EN SISTEMAS**

**CARTAGO VALLE**

**2018**

## Tabla de Contenido

[Introducción 3](#_bookmark0)

[Plan de Auditoria 4](#_bookmark1)

[Lista de Verificación 5](#_bookmark2)

Definición………………………………………………………………………………….. 6

[Reporte de Auditoria 8](#_bookmark3)

[Conclusiones 13](#_bookmark4)

El siguiente documento pretende evidenciar el proceso de auditoría que se elabora a Windows 7 Professional x 32 bits, para validar el cumplimiento de una norma, en este caso la norma técnica 27001 de 2013, la cual cuenta con una serie de registros que las empresas deben de cumplir para poder cumplir con la certificación.

Este documento es la elaboración de una auditoria a una empresa que funciona con sistema operativo Windows 7 la cual consiste en encontrar vulnerabilidades por medio de (meterpreter, ingeniería social y credenciales de usuario y contraseña), también vulnerar en la red wifi por medio de wpa2 y además aplicaremos vulnerabilidades a una aplicación web llamada web for pentester, las vulnerabilidades para la aplicación son: file include y command injections.

## OBJETO DE LA AUDITORIA:

Verificar el cumplimiento de la norma ISO 27001 de 2013.

* **ALCANCE**: A nivel geográfico se Windows 7 Professional x 32 bits, donde se auditará:
  + - * Sistemas operativos: Windows 7

1. Meterpreter
2. Ingeniería social
3. Puertas traseras
   * + - Red: Wifi – WPA2
       - Aplicación Web: web for pentester
4. File include
5. Command injections

Donde se habla de la seguridad de las comunicaciones.

* **AREA A AUDITAR:** TECNOLOGIAS DE LA INFORMACIÓN (TI).

## PERSONAS A AUDITAR:

* + Luis Edin Ibargue Mosquera - Analista de Proyectos
  + Asdrúbal Andrés Vélez Vélez - Líder de infraestructura
  + John Alejandro Giraldo mejia - Líder de desarrollo.

## DOCUMENTOS CONSULTADOS:

* + NORMA ISO 27001
  + Seguridad para las tecnologías de la información y las comunicaciones.
  + Documento de configuración inicial del sistema operativo y las autorizaciones para su actualización, pruebas o algún cambio.

## EQUIPO AUDITOR:

* + Luis Edin Ibargue Mosquera
  + Asdrúbal Andrés Vélez Vélez
  + John Alejandro Giraldo mejia
* **FECHA/HORA**: junio 06 de 2018 a las 6:30:00 p.m.
* **OBJETO** Verificar el cumplimiento de la norma ISO 27001 el anexo 12 donde se habla sobre la seguridad de las operaciones y el anexo 13 donde se habla sobre la seguridad de las comunicaciones.
* **FECHA**: junio 07 de 2018
* **AREA A AUDITAR** Tecnologías de la Información.

## AUDITOR(ES):

* + Auditor Líder: Asdrúbal Andrés Vélez Vélez
  + Experto técnico: John Alejandro Giraldo Mejia
  + Auditor Junior: Luis Edin Ibargue Mosquera

DEFINICIÓN:

La auditoría informática tiene como objetivo evaluar independientemente en lo administrativo, operativo y de gestión aspectos tecnológicos y de información, velando por el cumplimiento de las normas y procedimientos de la institución y minimizar la exposición al riesgo, para dar una garantia razonable de la integridad, confiabilidad, disponibilidad y auditabilidad de lainformación de la operatividad institucional.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PREGUNTAS** | **CONFORMIDAD** | | | **DOCUMENTOS**  **CONSULTADOS** | **OBSERVACIONE**  **S** |
| Muéstreme la documentación para el proceso de copias de seguridad. | **C X** | **NC** | **O** | Manual de copias de seguridad | La empresa lleva a cabo un  documento donde anota la  periodicidad con que se realiza la copia de seguridad de cada equipo |
| Muéstreme el plan de contingencia para el levantamiento de la infraestructura en caso de desastres |  | **X** |  | Manual de funcionamiento | La empresa NO cuenta con un plan formal que describa los pasos apropiados que se deben seguir en caso de un  desastre o emergencia |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Cuál es la versión del |  |  |  | Manual de políticas | La empresa tiene |
| documento de | **X** | de la seguridad | la versión |
| confidencialidad que |  | ISO 27001 | actualizada del |
| firman los usuarios, |  |  | documento de |
| proveedores y aliados del |  |  | confidencialidad d |
| área de tecnologías de la |  |  | e la |
| información |  |  | información que |
|  |  |  | solo puede ser |
|  |  |  | accedida |
|  |  |  | por usuarios |
|  |  |  | que tengan permisos |
|  |  |  | para ello |
| Cuál es la versión del |  |  |  | Documento de | La organización |
| software de pruebas que |  | configuración | cuenta con una |
| se tiene del sistema |  | inicial del sistema | versión obsoleta |
| comercial. |  | operativo y las | del software de |
|  | **X** | autorizaciones | pruebas para el |
|  |  | para su | sistema comercial |
|  |  | actualización, |  |
|  |  | pruebas o algún |  |
|  |  | cambio. |  |
| Muéstreme el documento |  |  |  | Manual de | La entidad tiene el |
| donde se evidencia que |  | Funciones, perfiles | documento donde |
| perfiles y roles que debe  tener un usuario | **X** | y  responsabilidades | especifica los  perfiles y roles de |
| administrador y un |  |  | usuario |
| usuario estándar. |  |  |  |
| Cuál es el procedimiento |  |  |  | Manual de la | La empresa cuenta |
| para realizar el cambio de |  | política de | con la |
| cableado estructurado de  un servidor de misión | **X** | seguridad para las  tecnologías de la | infraestructura y  estándares |
| crítica. |  | información y las | adecuados para |
|  |  | comunicaciones. | realizar un sistema |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | de cableado estructurado |
| Muestre el documento y Evidencie como se clasifican y separan las redes de la organización. |  | **X** |  | Manual de política de separación de las redes de la empresa. | La empresa posee el manual de separación de las redes, pero no lo  tiene aplicado. |
| Muestre el documento y evidencia el proceso de transferencia de información a partes externas. |  |  | **X** | Manual de la política de transferencia externa de información de la empresa. | La empresa posee un documento donde se evidencie el proceso de transferencia de información a partes externas, pero no se encuentra  implementado. |
| Evidencia la capacitación de políticas de seguridad relacionada con instalación de software en la empresa. |  |  | **X** | Evidencia fotográfica, listado de asistencia y examen. | La empresa no dispone de evidencias sobre capacitación sobre políticas de seguridad en la instalación de software en la  empresa. |

**FECHA** junio 06 de 2018

# Reporte de Auditoria

**AREA AUDITADA** Tecnologías de la Información **CARGO** Líder de Desarrollo

**AUDITORES** Asdrubal andres velez - jhon Alejandro mejia - Luis edin ibarguen

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NO**  **CONFORMIDAD** | | | **DESCRIPCION DE LAS NC Y OBS** | **CAUSAS DE LAS NC** | **ACCION A TOMAR C/P** | **FECHA DE EJEC** | **RESP** | **SEGUIMIENTO** | |
| **No.** | **NC** | **O** | **FECHA** | **FIRMA** |
| **1** | **X** |  | Se evidencio que en el área de tecnología de la información no cuentan con ningún plan de contingencia incumpliendo de la norma NTC/ISO 27001:2013 que dice que la organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad | El área de tecnología de la información no ha solicitado un plan de contingencia.  La empresa nunca ha contado con un documento preventivo en caso de riesgos, emergencias y desastres.  La empresa no posee capacitación sobre este tipo de riesgos. | Incluir el Plan de Contingencias en el Plan Estratégico de infraestructura.  Documentar el plan de Contingencia.  Socializar el Plan de contingencias a los miembros de la empresa | Junio 07 de 2018 |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NO**  **CONFORMIDAD** | | | **DESCRIPCION DE LAS NC Y OBS** | **CAUSAS DE LAS NC** | **ACCION A TOMAR C/P** | **FECHA DE EJEC** | **RESP** | **SEGUIMIENTO** | |
| **No.** | **NC** | **O** | **FECHA** | **FIRMA** |
| **2** | **X** |  | Se evidencio en el área de tecnología de la información,  6 equipos con códigos de 01 al 06 no tienen actualizado el software de pruebas que se requiere incumpliendo con el requisito 9.3 de la norma NTC/ISO 27001:2013 que  habla sobre revisar el sistema de la seguridad de la información a intervalos planificados y el anexo  A.12.6.2 que dice que se debe establecer e implementar las reglas para la  instalación de software para los usuarios. | El área de tecnología de la información no ha reportado que la licencia del software de pruebas se encuentra obsoleto.  En el área no hay quien esté pendiente de las fechas en que caduca el software.  La licencia no se encuentra en el plan de compras de la empresa. | Delegar personal para que este pendiente de las fechas de  caducidad de las licencias de software.  Diligenciar reporte para adquisición de software de pruebas.  Instalar y actualizar software. | Junio 07 de 2018 |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NO**  **CONFORMIDAD** | | | **DESCRIPCION DE LAS NC Y OBS** | **CAUSAS DE LAS NC** | **ACCION A TOMAR C/P** | **FECHA DE EJEC** | **RESP** | **SEGUIMIENTO** | |
| **No.** | **NC** | **O** | **FECHA** | **FIRMA** |
| **3** | x |  | Se evidencio en el área de tecnología de la información, los cables de red que llegan al switch identificado con serial número 2345, no se encuentran debidamente separados según al área que pertenecen, representando un peligro para la seguridad de la red.  Incumpliendo así con el requisito 6.1.1.b de la norma NTC/ISO 27001:2013 que  habla sobre prevenir o reducir efectos indeseados y el anexo  A.13.1.3 que dice que los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes. | No tiene conocimiento sobre este requerimiento.  La empresa no considera una vulnerabilidad este concepto. | La empresa contratara a un tercero que se encargara de la implementación y adecuación de este requerimiento.  Capacitar a los empleados sobre vulnerabilidades en las redes, y la necesidad de dividir las redes.  Crear una política que permite verificar el  cumplimiento y que sirva como soporte a las futuras redes  que cree la empresa. | Junio 07 de 2108 |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NO**  **CONFORMIDAD** | | | **DESCRIPCION DE LAS NC Y OBS** | **CAUSAS DE LAS NC** | **ACCION A TOMAR C/P** | **FECHA DE EJEC** | **RESP** | **SEGUIMIENTO** | |
| **No.** | **NC** | **O** | **FECHA** | **FIRMA** |
| **4** |  | X | Comprobando el ordenador con código de inventario 123bd del área de tecnologías se evidencia que se puede instalar software si ninguna restricción.  Incumpliendo el requisito 7.5.1.ab. de la norma NTC/ISO 27001:2013 que  habla sobre que el sistema de gestión de seguridad de la información de la organización debe incluir la información documenta y requerida por la norma y también la información documentad que la organización ha determinado que es necesaria, y el anexo  12.6.2 que habla sobre las restricciones en la instalación de software. | La empresa no posee un manual que regule la instalación de software.  La empresa no considera una vulnerabilidad de seguridad la instalación de software sin control.  La empresa no ha recibido capacitación sobre vulnerabilidades en la instalación de software. | Construir una  política de  seguridad sobre la instalación de software en los equipos.  Capacitar a los empleados, sobre la instalación de software en los equipos.  Contratar a un tercero para capacitar al área de tecnologías sobre las vulnerabilidades en la instalación de software | Junio 07 de 2018 |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NO**  **CONFORMIDAD** | | | **DESCRIPCION DE LAS NC Y OBS** | **CAUSAS DE LAS NC** | **ACCION A TOMAR C/P** | **FECHA DE EJEC** | **RESP** | **SEGUIMIENTO** | |
| **No.** | **NC** | **O** | **FECHA** | **FIRMA** |
| **5** |  | X | Se evidencia en el equipo 123b5 del área de tecnologías de la información, no se encuentra implementado el proceso de transferencia de información a partes externas, ya que, al hacer una prueba, la información no es encriptada y viaja en texto plano.  Incumpliendo el requisito  6.1.1.b de la norma NTC/ISO 27001:2013 que habla sobre prevenir o reducir efectos indeseados y el anexo 13.2.1 que habla sobre políticas y  procedimientos de transferencia de información. | La empresa nunca ha implementado un servicio de encriptación de información para enviarla a partes externas.  La empresa no posee un servicio SSL, que permite encriptar la información.  El empleado a cargo del envió de la información no ha recibido capacitación sobre envió de la información. | Implementar en  todas las  comunicaciones a partes externas de la empresa, el proceso de encriptación de la información.  Comprar un certificado SSL que permita el cifrado de la información.  Capacitar a los empleados en tema de seguridad de la información. | Junio de 07 de 2018 |  |  |  |

# CONCLUSIONES

La Auditoría Integral constituye un enfoque moderno que persigue obtener resultados completos en las evaluaciones efectuadas a los sistemas.

Permite de manera oportuna y completa, presentar los resultados a la alta gerencia para la toma de decisiones.

A través de este proyectos se pudo comprender y poner en practica la norma técnica 27001 de 2013, ya que, dados unos casos, nos dimos a la tarea de buscar en los registros donde correspondía cada uno.

Que la norma técnica les permite a las empresas asegurar sus procesos a través de 114 controles muy rigurosos e importantes.