## Tabla de Contenido

[Introducción 3](#_bookmark0)

[Plan de Auditoria 4](#_bookmark1)

[Lista de Verificación 5](#_bookmark2)

[Reporte de Auditoria 8](#_bookmark3)

[Conclusiones 13](#_bookmark4)

**Introducción**

El siguiente documento pretende evidenciar el proceso de auditoría que se elabora en una empresa, 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.

**Plan de Auditoria**

## OBJETO DE LA AUDITORIA:

Verificar el cumplimiento de la norma ISO 27001 de 2013.

* **ALCANCE**: A nivel geográfico se auditará la empresa MIRADO de Pereira ubicada en la carrera 3N # 21-20, donde se auditará el requisito 9 que habla de la EVALUACION DEL DESEMPEÑO y los anexos 12 donde se habla sobre la seguridad de las operaciones y el anexo 13 donde se habla de la seguridad de las comunicaciones.
* **AREA A AUDITAR:** TECNOLOGIAS DE LA INFORMACIÓN.

## PERSONAS A AUDITAR:

* + Hurtado Beltrán Leidy Joanna- Analista de Proyectos
  + Mosquera Velásquez Ángela Julieth-Líder de infraestructura
  + Arboleda Abad Andrés Felipe-Líder de desarrollo.

## DOCUMENTOS CONSULTADOS:

* + Itil Fundamentos
  + NORMA ISO 27001
  + Manual de documentación de procesos.
  + Manual de Funciones, perfiles y responsabilidades.
  + Manual de la política de 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:

* + Auditor Líder: Andrés Felipe Farfán Hernández
  + Auditor Junior: Natalia Isaza Serrano
* **FECHA/HORA/LUGAR**: junio 1 de 2017 a las 9:00 a.m. en la Dirección de tecnologías de la información de la empresa **MIRADO** de Pereira ubicada en la carrera 3N # 21-20

**Lista de Verificación**

* **OBJETO** Verificar el cumplimiento del requisito 9 de la norma ISO 27001 de 2013 que habla sobre la EVALUACION DEL DESEMPEÑO y los anexos 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 1 de 2015
* **AREA A AUDITAR** Tecnologías de la Información.

## AUDITOR(ES):

* + Auditor Líder: Andrés Felipe Farfán Hernández
  + Auditor Junior: Natalia Isaza Serrano

## PERSONAS A AUDITAR:

* + Hurtado Beltrán Joanna
  + Mosquera Velásquez Ángela

**SISTEMA OPERATIVO**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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 Documento donde se evidencia los cambios hechos al software comercial de la empresa. | **X** |  |  | Manual de documentación Itil. | La empresa cuenta con el documento de registros para la actualización o  cambios de software |
| Muéstreme el plan de contingencia para el levantamiento de la |  | **X** |  | Manual de funcionamiento | La empresa NO cuenta con un plan formal que describa los pasos |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Infraestructura en caso de desastres. |  |  |  |  | apropiados que se deben seguir en caso de un  desastre o emergencia |
| Cuál es el plan de contingencia por  eliminación de información de vital importancia de los usuarios | **X** |  |  | Manual de planes de emergencia | La entidad tiene un Plan que permite la protección de la información ante la posible pérdida, destrucción, robo y  otras amenazas |
| 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 permis |
|  |  |  | os 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. |

**RED**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PREGUNTAS** | **CONFORMIDAD** | | | **DOCUMENTOS**  **CONSULTADOS** | **OBSERVACIONE**  **S** |
| Muéstreme la documentación para el servidor de datos | **C X** | **NC** | **O** | Manual de datos | La empresa lleva a cabo un  documento donde anota la  periodicidad con que se realiza la copia de servidor de datos |
| Muéstreme el Documento donde se evidencia los permisos de usuarios y facilidad de administración de la red local. | **X** |  |  | Manual de documentación Itil. | La empresa cuenta con el documento de registros para la actualización o  Cambios del dominio |
| Cuál es el plan de contingencia de la política de contraseñas adecuada y copias de seguridad definidas | **X** |  |  | Manual de planes de emergencia | La entidad tiene un Plan que permite la protección de la información ante la posible pérdida, destrucción, robo y  otras amenazas |
| Muestreme el documento donde se evidencia licencias de programas instalados en la red por posibles inspecciones | **X** |  |  | Manual de licencias | La entidad tiene el documento donde especifica los perfiles |
| Cual es el procedimiento para realizar el cambio de cableado estructurado de un servidor de misión critica | **X** |  |  | Manual de la política de seguridad para las tecnologías de la información y las comunicaciones | La empresa cuenta con la infraestructura y estándares adecuados para realizar un sistema |

**Aplicaciones web**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PREGUNTAS** | **CONFORMIDAD** | | | **DOCUMENTOS**  **CONSULTADOS** | **OBSERVACIONE**  **S** |
| Muéstreme la documentación para el seguimiento de actualización de la pagina web | **C X** | **NC** | **O** | Manual de seguridad | La empresa lleva a cabo un  documento donde anota el seguimiento de actualizacion |
| Muéstreme el certificado de seguridad de la información |  |  | **X** | Manual de documentación Itil. | La empresa no cuenta con el documento |
| Muéstreme el documento donde está el gestor de permisos de archivos | **X** |  |  | Manual de permisos | La entidad tiene un Plan que permite la protección de la información ante la posible pérdida, destrucción, robo y  otras amenazas |
| Muéstreme si la información sensible esta encriptado | **X** |  |  | Manual de seguridad | La entidad tiene el documento donde especifica los perfiles |
| Muéstreme la documentación para el proceso de copias de seguridad. | **X** |  |  | 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 |

# Reporte de Auditoria

**FECHA** Junio 1 2018

**AREA AUDITADA** Tecnologías de la Información

**PERSONA AUDITADA** Erika maría Pérez Orozco

**CARGO** Líder de Desarrollo

**AUDITORES** Natalia Isaza Serrano

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 a cargo del Sr Andrés Felipe Arboleda Abad no cuentan con ningún plan de contingencia contra ataques de elevación de privilegios | El área de tecnología de la información no ha solicitado un plan de contingencia.  La empresa no ha contado con un experto en seguridad para remediar este problema y asesorar a los empleados.  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 1 2018 | Erika maría Pérez Orozco |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 a cargo del Erika Maria Perez, se encontró en los sistemas operativos vulnerabilidad en el comando Sudo de Linux que podría permitir a usuarios locales con permisos para ejecutar, Sudo obtener permisos de root. se requiere incumpliendo con el requisito 9.3 de la norma NTC/ISO 27001:2013 | La vulnerabilidad podrá permitir a un usuario local de la empresa con permisos para ejecutar comandos a través de Sudo elevar sus privilegios a root. | Delegar personal para que este pendiente de esta vulnerabilidad a dar solucion  Instalar y actualizar software. | Junio 1 2018 | Erika maría Pérez Orozco |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 a, que 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. | 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 1 2018 | Erika maría Pérez Orozco |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 a cargo del Sr Andrés Felipe Arboleda Abad 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 1 2018 | Erika maría Pérez Orozco |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 evidencio que en la página web de la empresa dvwa.com tiene una vulnerabilidad Cross Site Request Forgery (CSRF) esto atrae a actividades maliciosas en nombre del empleados y usuarios logueado. NTC/ISO 27001:2013 que  habla sobre prevenir o reducir ataques, proporcionando una pagina segura | La empresa nunca ha implementado protocolo se seguridad para evitar ataques.  La empresa no posee una aplicación web que este protegida hacia ataques csrf, este ataque podría sacar información importante de la empresa.  El empleado atenta a proteger su información de la web. Poniendo a cargo un ingeniero que cubra estas vulnerabilidades | Implementar en  todas las  Comunicaciones a partes externas de la empresa  Colocar a cargo un ingeniero que esté atento y de solución a este problema  Capacitar a los empleados en tema de seguridad de la información. | Junio 1 2018 | Erika maría Pérez Orozco |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| **6** |  | X | Se evidencio que en la página web tiene dos vulnerabilidades en la parte de los tokens que son: Vulnerabilidades debido a debilidades en el algoritmo de generación de los tokens.  Vulnerabilidades debido al manejo no correcto de los tokens. Esto puede generar ataques por medio de las cookies almacenadas en los navegadores web NTC/ISO 27001:2013 que  habla sobre prevenir o reducir ataques, proporcionando una página segura | La empresa no asesorada sobre las desventajas que podría tener dejar cookies permanentes en los n  La empresa no posee una aplicación web que este protegida hacia ataques por medio de cookies  El empleado debe asesorar a sus usuario y darles a conocer los riesgos que pueden tener las cookies permanentes | Sin darse cuenta, los usuarios manejan muchas sesiones a la vez, como por ejemplo, cuando utilizan las redes sociales o los correos electrónicos y puedes robar sus cookies almacenadas en el navegador  Capacitar a los empleados en tema de seguridad de la información. | Junio 1 2018 | Erika maría Pérez Orozco |  |  |

# Conclusiones

A través de este trabajo 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.

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