TELEANTIOQUIA

COMUNICACIÓN INTERNA

Medellín, 25 de abril de 2022 2022300537

PARA: Luis Felipe Hincapié Uribe
Gerente

DE: Dirección de Control Interno

ASUNTO: Informe Auditoría de Sistemas de Información.

La Dirección de Control Interno, en desarrollo del plan de auditorías, presenta el informe realizado a los Sistemas de Información del canal con alcance al año 2022.

En el mismo, se evaluaron los controles que posee Teleantioquia para el manejo de la seguridad de la información y su salvaguarda.

Se adjunta el informe.

Cordialmente,

HENRY DARÍO MUÑOZ MONTOYA

Copia: Document; Comité de Gerencia.

Proyectó: Henry Darío Muñoz Montoya – Andersson Benítez Arboleda
Radicó: Nelcy Gómez Arismendy

Auditoría N° 02		
Fecha		
Día	Mes	Año
15	03	2022

AUDITORÍA A LOS SISTEMAS DE INFORMACIÓN DEL CANAL TELEANTIOQUIA	
Representante de la Auditoría:	Henry Darío Muñoz Montoya
Auditor	Andersson Benítez Arboleda Henry Darío Muñoz Montoya
Objetivo General	Analizar los sistemas de información que operan en el canal Teleantioquia.
Objetivos Específicos	-Elaborar cuestionario para revisión del proceso. -Visitas de verificación. -Entrevistar a los operadores de los sistemas de información -Comprobar la veracidad de la información suministrada por los operadores del proceso.
Alcance	Procesos de los sistemas de información del canal
Fecha de apertura:	Marzo 15 de 2022
Fecha de cierre:	Abril 22 de 2022

ASPECTOS GENERALES

INTRODUCCIÓN

La oficina de Control Interno constituye un apoyo al logro de los objetivos y metas institucionales, ayuda a la protección de sus recursos y fomenta la eficacia y efectividad de cada una de las actividades que se realizan en las diferentes dependencias de la Entidad.

Cumpliendo con la ley y en desarrollo de las funciones señaladas en el artículo 9 de la ley 87 de 1993 y del rol que deben desempeñar las oficinas de Control Interno, además de las normas referidas a los fines de ésta Oficina y en especial del estatuto anticorrupción (ley 1474 de 2011), pretende dirigir éste trabajo hacia el cumplimiento en la realización de Auditorías a los procesos que se ejecutan buscando el cumplimiento de los objetivos institucionales.

Los sistemas de información son elementos fundamentales en todas las entidades, para el adecuado control de sus procedimientos, actividades, tareas, sirven de apoyo para que los funcionarios, ejecuten sus actividades de manera más ágil, segura y eficiente.

LA ENTIDAD

La Sociedad Televisión de Antioquia Limitada, TELEANTIOQUIA, es una sociedad conformada como entidad pública, organizada como empresa industrial y comercial de Estado, constituida como sociedad de responsabilidad limitada, entidad descentralizada indirecta del orden departamental, mediante la Resolución 08 del 2 de junio de 1995, elevada a la escritura pública 3187 del 9 de agosto de 1995, de la Notaría Primera del Círculo de Medellín. Hace parte de la Rama Ejecutiva, con autorización legal para la prestación de servicios de telecomunicaciones e información mediante la transmisión de audio y video de conformidad con la Ley 1341 de 2009.

Misión

Somos la televisión pública regional que inspira, integra y proyecta a los antioqueños, mediante la prestación de servicios audiovisuales que contribuyen a la sostenibilidad de la organización y la satisfacción de nuestros clientes, accionistas y colaboradores.

Visión

Ser una empresa líder en servicios de comunicación audiovisual con capacidad para competir a nivel regional con productos innovadores que satisfagan las necesidades de los clientes.

Como entidad pública, es una empresa industrial y comercial del Estado, entidad descentralizada indirecta perteneciente al orden departamental, cuya creación fue autorizada por los Decretos Nacionales 3100 y 3101 de 1984, siendo transformada al orden departamental en ejercicio de las facultades conferidas a la Junta Administradora Regional a través del numeral 3° del artículo 37 de la Ley 182 de 1995.

ASPECTOS PRELIMINARES

ANOTACIONES INICIALES

- Planeación de la auditoría: estudio y conocimiento del proceso, recolección de la información de la dependencia a auditar (área de tecnologías).
- Verificación del cumplimiento de los planes de mejoramiento.
- Aplicación de cuestionario y entrevistas con los funcionarios del área de tecnologías y otros funcionarios del canal.
- Verificación del inventario del área de tecnologías.
- Procesamiento de la información.
- Elaboración del informe final.

PROCEDIMIENTO

- Notificación de inicio de la auditoría a la Directora de Producción y Tecnologías.
- Solicitud de información referente al proceso.
- Verificación de los expedientes contractuales.
- Visitas de verificación
- Entrevistas a funcionarios.

HERRAMIENTAS Y DOCUMENTOS

- Cuestionario
- Entrevista
- Expedientes contractuales
- Listado de inventario de equipos de cómputo.
- Documentos soporte a las repuestas del cuestionario
- Document
- Herramientas ofimáticas

DESARROLLO

La auditoría se desarrolló de acuerdo al plan de auditoria por parte de la oficina de control interno, en esta se pretende verificar que los sistemas de información del canal tengan una buena administración, además de evaluar los controles que se poseen para la salva guarda de la información.

- **CUESTIONARIO PARA REVISIÓN DEL PROCESO**

Para el desarrollo de la auditoria a los Sistemas de Información, se elaboró el siguiente cuestionario, para ser diligenciado por el Coordinador del área de Tecnologías, con el objeto de conocer el estado actual de los sistemas de información de la Entidad.

Con el cuestionario, se busca conocer la arquitectura tecnológica que tiene el canal, conocer el proceso, con sus manuales, procedimientos, inventario de equipos y recursos, que tiene el área de tecnologías.

Cuestionario

Proceso Sistemas de Información - Adquirir y mantener la arquitectura tecnológica			
Objetivo de Control	**Evaluación del Nuevo Hardware y Mantenimientos**		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿Se cuenta con un inventario de todos los equipos que tiene la Entidad?			
¿Con Cuanta Frecuencia se revisa el inventario?			
¿Se posee de bitácoras de fallas detectadas en los equipos?			
Características de la bitácora (señales las opciones)			
¿La bitácora es registrada por personal especializado			
¿Señala fecha de detección de la falla?			
¿Señala fecha de corrección de la falla y revisión de que el equipo funcione?			
¿Se poseen registros individuales de los equipos?			
¿La bitácora hace referencia a hojas de servicio, en donde se detalla la falla y las causas que la originaron, así como las refacciones utilizadas?			
¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?			
¿Se cuenta con un servicio de mantenimiento para todos los equipos?			
¿Con Cuanta Frecuencia se realiza mantenimiento a los equipos?			
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?			
¿Se tiene criterios de evaluación para determinar el rendimiento de los equipos de cómputo a adquirir y así elegir el mejor?			
Documentos Probatorios Presentados			

Proceso Sistemas de Información - Administración de Instalaciones			
Objetivo de Control	**Escolta de visitantes**		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿Las instalaciones (aulas, cubículos y oficinas), fueron diseñadas o adaptadas, específicamente para funcionar como un centro de cómputo?			
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?			
¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?			
¿Existen lugares de acceso restringido?			
¿Se cuenta con sistemas de seguridad, para impedir el paso a lugares de acceso restringido?			
¿Se cuenta con sistemas de emergencia, como son detectores de humo, alarmas u otro tipo de Sensores?			
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tiene establecidas rutas de evacuación?			
¿Se tiene medios adecuados para extinción de fuego en el centro de cómputo?			

¿Se cuenta con una iluminación adecuada y con iluminación de emergencia es caso de presentarse una?			
¿Se tiene sistemas de seguridad para evitar que se sustraiga equipo en las instalaciones?			
¿Son funcionales los muebles instalados dentro del centro de cómputo: Cintoteca, Discoteca, archiveros, mesas de trabajo, etc?			
¿Se tiene un lugar asignado para papelería y utensilios de trabajo?			
¿Existen prohibiciones de fumar, consumir bebidas y alimentos?			
¿Se cuenta con suficientes carteles en lugares visibles que recuerden estas prohibiciones?			
¿Con cuanta frecuencia se limpian las instalaciones?			
¿Con cuanta frecuencia se limpian los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)?			
Documentos Probatorios Presentados			

Proceso Sistemas de Información - Administración de Instalaciones			
Objetivo de Control	**Suministro Ininterrumpido de energía**		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿Se cuenta con instalación con tierra física a todos los equipos?			
¿La instalación eléctrica se realizó específicamente para el centro de cómputo?			
¿Se cuenta con otra instalación dentro del centro de cómputo, diferente de la que alimenta a los equipos de cómputo?			
¿La acometida llega a un tablero de distribución?			
El tablero de distribución está en la sala, visible y accesible?			
¿El tablero considera espacio para futuras ampliaciones de hasta un 30% (considerando que se dispone de espacio físico para la instalación de más equipos?			
¿La instalación es independiente para el centro de cómputo?			
¿Se cuenta con interruptores generales?			
¿Se cuenta con interruptores de emergencia en serie al interruptor general?			
¿Se cuenta con interruptores por secciones o aulas?			
¿Se tienen los interruptores rotulados adecuadamente?			
¿Se tiene protecciones contra corto circuito?			
¿Se tiene implementado algún tipo de equipo de energía auxiliar?			
¿Se cuenta con planta de emergencia?			
¿Qué porcentaje de lámparas están conectadas a la planta de emergencia (recomendable el 25%)?			
Documentos Probatorios Presentados			

Proceso Sistemas de Información - Protección contra factores ambientales			
Objetivo de Control	**Seguridad Física**		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿Se tiene lugares de acceso restringido?			
¿Se poseen mecanismos de seguridad para el acceso a estos lugares?			
¿A este mecanismo de seguridad se le han detectado debilidades?			
¿Tienen medidas implementadas ante la falla del sistema de seguridad?			
¿Con cuanta frecuencia se actualizan las claves o credenciales de acceso?			
¿Se tiene un registro de las personas que ingresan a las instalaciones?			
Documentos Probatorios Presentados			

El cuestionario se realizó para conocer como está conformado el centro de cómputo, si cumple con protocolos de seguridad y observar si se tiene inventario de equipos.

De acuerdo a las respuestas del cuestionario anterior, se realizan las siguientes observaciones:

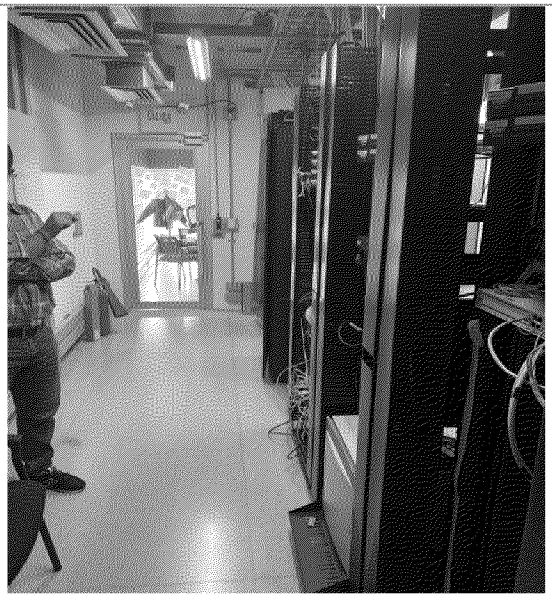
- No se observó en los documentos soporte entregados por el funcionario que diligenció el cuestionario, ni en el inventario recibido por el equipo auditor, información necesaria como características del equipo, ubicación del equipo, software instalado, entre otros. Esta información contribuye a tener un mayor control de los equipos de cómputo, disminuyendo los riesgos operativos de uso, riesgos de pérdida, seguridad de la información y daños, entre otros.

Se sugiere realizar inventario de control de todos los equipos de cómputo mínimo cada tres meses, con el objetivo de tener un control de los mismos.

- **VISITAS DE VERIFICACIÓN**

En compañía del jefe del área de tecnologías, se realiza visita al centro de cómputo del canal y al CER "Control Equipment Room", encontrando lo siguiente:

Foto Centro de Computo del canal



Evidencia fotográfica, visita de verificación auditora

Observaciones:

- El centro de cómputo cuenta con una cámara de vigilancia, donde se puede observar el personal que ingresa, dejando registro gráfico.

- Cuenta con perfiles de acceso, donde sólo personal autorizado puede ingresar al centro de cómputo.

- Se evidencia un control para el acceso a este espacio, el cual cumple con las características de seguridad física.

Se realiza visita al Rack del cuarto piso que contiene, Swicth, Hub y cableado. Encontrando lo siguiente:

Foto cuarto Rack cuarto piso

Evidencia fotográfica, visita de verificación auditora

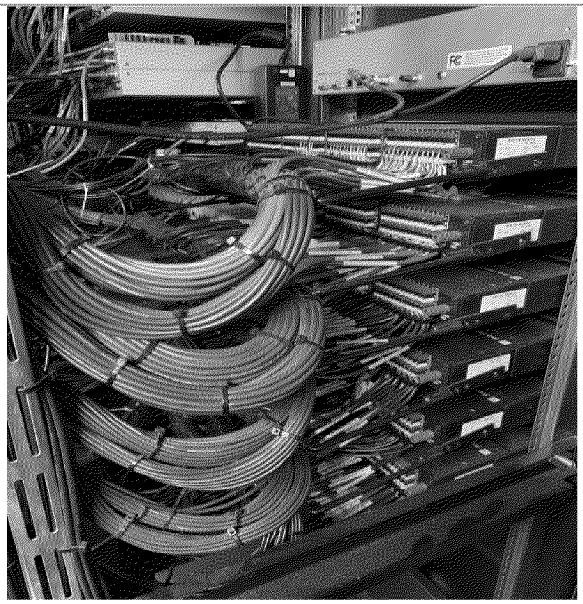
Observaciones:

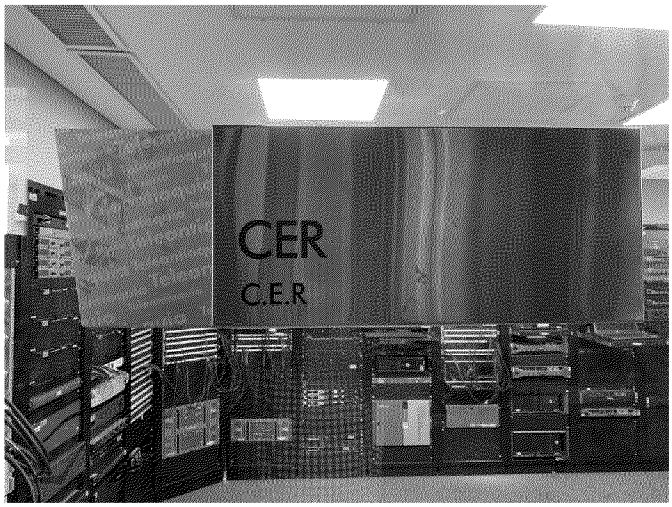
- Cada piso del canal, cuenta con un rack, allí se encuentran los diferentes Switch y Hub, como arquitectura tecnológica diseñada para el canal, se evidencia una buena arquitectura y seguridad en dichos cuartos, solo personal autorizado puede ingresar a estos lugares.

- Se evidencia que el rack del cuarto piso posee adecuados controles de acceso.

Se realiza visita al CER evidenciando lo siguiente:

Fotos CER "Control Equipment Room"





Evidencia fotográfica, visita de verificación auditora

Observaciones:

- El CER, se encuentra organizado y bien estructurado, evidenciando un adecuado mantenimiento de orden y limpieza de dicho lugar, lo que evidencia el cuidado de los bienes del canal.

- Los elementos que se encuentran en el CER, corresponden a los que deben de estar en estos cuartos de control.

- No se observan riesgos que puedan afectar directamente los equipos en este cuarto, como, por ejemplo, cables pelados, conexiones sueltas, elementos que generen incendio, daño o corto circuito.

Foto Puerta CER

Evidencia fotográfica, visita de verificación auditora

Observaciones:

- Al momento de la visita se encuentra que la puerta de acceso del CER "Control Equipment Room", no cumple su función, no cierra por completo, lo que puede generar una vulnerabilidad de acceso a dicha oficina, generando riesgos de seguridad de la información, riesgos a los equipos o actos mal intencionados.

ENTREVISTAS A LOS OPERADORES DE LOS SISTEMAS DE INFORMACIÓN

- Se pregunta a los operadores de los sistemas de información, sobre las políticas de seguridad de la información que tiene el canal, si bien existe un documento, estas no se han aprobado y formalizado con todo el personal, lo que genera una falta de control, pues existe una vulnerabilidad de la información, ya que no existen copias de seguridad en los equipos de cómputo de cada funcionario; esto a nivel de usuario final.

- Se indaga por documentos que soporten los roles y responsabilidades del personal del área de tecnologías, estas van ligadas al documento de políticas de seguridad de la información, se evidencia que no existen, por lo que se hace necesario, elaborarlo, formalizarlo y socializarlo.

- El área de Tecnologías, cuenta con un correo como mesa de ayuda, para la solución de incidentes por parte de los usuarios finales y así dar solución a inconvenientes informáticos. El correo al que deben copiar los usuarios es: mesadeayuda@teleantioquia.com.co. No existe un procedimiento definido para esto, normalmente los usuarios llaman a las extensiones del área de Tecnologías y no utilizan el correo.

- Se realiza un recorrido para revisar la red de datos con que cuenta el canal. Se observa una buena marcación, identificación de los switch, hub y cableado. Los enrutadores y AP "Acces Point" que tiene el canal, cuentan con una configuración, donde a la red, solo puede acceder personal autorizado y la navegación es restringida.

- Al momento de esta auditoría, se evidencia que la navegación de internet no tiene restricciones en algunos puestos de trabajo, lo que genera una vulnerabilidad para el filtro de información, además de la generación de virus o códigos maliciosos, que pueden causar daños a la red del canal.

- Se indaga por las pólizas que tiene el canal para la cobertura de los equipos de cómputo, esta tiene vigencia hasta las 24 horas del día 30-06-2022, dando cobertura a estos.

- Si bien en las políticas de seguridad de la información que posee el canal, se informa que cada usuario es responsable de su información y que por ende debe realizar copias de seguridad, se hace necesaria una aclaración, pues la oficina de tecnologías debe acompañar en este proceso a los usuarios finales, pues indagando con personal del canal, comunican que no saben cómo hacerlo o si saben hacerlo lo hacen en dispositivos o disco duros propios y no del canal, lo que genera vulnerabilidad en la información, pues esta puede ser filtrada y utilizada para otros fines. También podría presentarse propagación de virus y pérdida de información sensible para el canal.

- Con relación a los licenciamientos, se evidencia que el canal, tiene sus equipos de cómputo debidamente licenciados, además de sus servidores; si bien tiene licencias Windows 10 y de office 2016, se debe estar más a la vanguardia de la información, donde se utiliza la nube como respaldo y no almacenarla dentro de los equipos de cómputo, evitando así vulnerabilidad en los respaldos de información y sistemas obsoletos.

- Se pregunta por el programa de mantenimientos a los equipos de cómputo de los usuarios finales, donde comunican que todo se resuelve según la falla y sea reportado por el usuario. Si bien al realizar la llamada por el usuario, el área de tecnologías resuelve los inconvenientes, se debe generar un cronograma de mantenimientos preventivos, no obstante, los equipos nuevos tienen garantías, motivo por el cual, se debe vigilar por parte del área de tecnologías, que se hagan estos mantenimientos para evitar errores en los equipos.

- Se evidencia un cortafuego activo, llamado FORTINET. Cada equipo de cómputo cuenta con un antivirus, que protege contra ataques informáticos, salvaguardando la información del canal.

CONCLUSIONES

- ✓ Si bien existe un inventario de los equipos de cómputo del canal, debe ser más amplia la información que en él se relaciona, teniendo en cuenta la relevancia de la misma, por ejemplo: mantenimientos preventivos realizados, ubicación, software instalado, permisos de cada equipo, entre otros. Se recomienda tener una hoja de vida por cada equipo con esta información y actualizarla cuando sea necesario.

- ✓ Se sugiere realizar el inventario de control de los equipos de cómputo mínimo cada tres meses, con el fin de evitar riesgos de daños, hurto, pérdidas, generando así mayor control de estos activos.

- ✓ Existe muy buen control al acceso del centro de cómputo y al CER “Control Equipment Room”, pues solo personal autorizado puede ingresar a estos lugares, se debe corregir el imán de la puerta de acceso al CER, para que este cierre por completo y no exista riesgo de accesos no autorizados a un lugar tan neurálgico del canal.

- ✓ Se debe de revisar, actualizar, aprobar y socializar la Política de Seguridad y Privacidad de la información, así mismo como el Plan de Seguridad y Privacidad de la Información y el Plan Estratégico de Tecnologías de la Información de acuerdo a los lineamientos establecidos por la guía G.ES.06 del Departamento Administrativo de la Función Pública y el modelo de seguridad y privacidad de la información del Ministerio de las Tecnologías de la Información y Comunicaciones.

- ✓ Se deben evidenciar en la Política de Seguridad y Privacidad de la Información, los roles y responsabilidades del personal de acuerdo a su alcance, así mismo debe quedar documentada esta información en los diferentes procedimientos del área de Tecnologías.

- ✓ Se debe crear un cronograma de mantenimientos preventivos, de los equipos de cómputo con los que cuenta el canal, para así evitar riesgos de pérdida de información, además de tener equipos más confiables y funcionales.

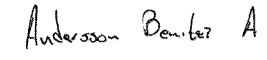
- ✓ Se sugiere definir los perfiles de acceso a las diferentes páginas comerciales como WhatsApp Web, correos electrónicos, entre otros, para evitar riesgos de vulnerabilidad a los sistemas de información.

- ✓ El canal debe estar a la vanguardia de la información y tener sistemas de información acordes al core de negocio, para tener un mayor control de los backups a los equipos de cómputo de los usuarios. Se sugiere tener licencias de Office 365, que cuenta con un sistema en la nube para el respaldo de la información, así en caso de un robo de equipo o problema informático, la información se pueda recuperar y restaurar.

PLAN DE MEJORAMIENTO

Se sugiere realizar plan de mejoramiento de las conclusiones de este informe y enviarlo a la oficina de Control Interno, antes de finalizar el primer semestre del año 2022, al correo henry.munoz@teleantioquia.com.co y abenitez@teleantioquia.com.co

FIRMAS

Nombre completo	Responsabilidad	Firma
Henry Darío Muñoz Montoya	Director de Control Interno	
Andersson Benítez Arboleda	Auditor de apoyo	

Copia: *Document Teleantioquia, Página Web, Comité de Gerencia, Dirección de Innovación y Contenidos, Dirección de Control interno, Profesional de Control Interno.*
Proyectó: *Henry Darío Muñoz Montoya – Andersson Benítez Arboleda*
Radicó: *Nelcy del Socorro Gómez Arismendy*