INFORME DEFINITIVO EVALUACIÓN INDEPENDIENTE PROCEDIMIENTO GESTIÓN DE LOS SERVICIOS DE TI. 2021

DIANA CAROLINA TORRES GARCÍA
Contralora General de Medellín

DIEGO MAURICIO ECHEVERRI ARANGO
Jefe de Oficina de Control Interno

CARLOS ALBERTO GUERRA ACOSTA
Profesional Universitario 2

OFICINA DE CONTROL INTERNO

MEDELLÍN, DICIEMBRE DE 2021

TABLA DE CONTENIDO

Pág.

1. INTRODUCCION

Uno de los asuntos que más preocupa a las empresas hoy en día es la ciberseguridad. La gran dependencia de los negocios de la tecnología, las redes y las comunicaciones han puesto como prioridad la seguridad para poder garantizar la continuidad del negocio.

La auditoría de seguridad informática es la herramienta principal para poder conocer el estado de seguridad en que se encuentra una empresa en relación con sus sistemas informáticos, de comunicación y acceso a internet. Estas auditorías permiten mejorar los sistemas e incrementar la seguridad, siendo fundamentales para poder garantizar el funcionamiento del negocio y proteger la integridad de la información que manejan.

Es así que una auditoría de seguridad no es solo responsabilidad de grandes empresas y corporaciones. Hoy en día cualquier tipo de empresa depende de elementos y dispositivos tecnológicos para poder realizar sus procesos de negocio, por lo que es necesario que se evalúe de forma periódica su seguridad.

Es por esto que la Oficina de Control Interno de la Contraloría General de Medellín, en cumplimiento de las funciones asignadas en la Ley 87 de 1993 y en virtud del rol de evaluación y seguimiento asignado a través del artículo 17 del Decreto 648 del 2017, realiza el presente informe de evaluación a la gestión Licenciamiento de Software de propósito general, asignación de claves de acceso y contraseñas y a la Evaluación del nivel de seguridad de la información en la Contraloría General de Medellín, con corte al 30 de diciembre de 2021, teniendo en consideración los lineamientos del Departamento Administrativo de la Función Pública DAFP en el marco del Modelo Integrado de Planeación y Gestión MIPG y la Guía para la Gestión del Riesgo y el diseño de controles versión 5 de 2020.

Para el desarrollo de la presente evaluación, se realizó el estudio del Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI) vigente de la C.G. de Medellín, Modelo de Seguridad y Privacidad de la Información, procedimientos SIGI que se encontraron pertinentes, Guías del MinTic para el modelo de seguridad y Norma ISO 27001 - Gestión de la seguridad de la información, y su Anexo A., así como la documentación propia de la Entidad, entre otras.

Por último, al final del informe se presentan consolidadas las conclusiones del trabajo realizado y una conclusión general, con la que se busca que en la Entidad se fortalezca en materia de seguridad de la información.

2. NORMATIVIDAD RELACIONADA

La Contraloría General de Medellín en cumplimiento del proceso de Control interno y que reza que es aquel proceso que se ejerce internamente en las organizaciones y es impulsado por las directivas, administradores y demás personal que está vinculado a ella, el cual posee la suficiente ética y moral, así como formación académica, que le amerite credibilidad a sus hallazgos y conclusiones y tiene como propósito lograr el cumplimiento de los objetivos institucionales, en pro del aseguramiento de los resultados institucionales y del mejoramiento continuo de la entidad, estableció el siguiente marco legal para esta Auditoria

Marco Legal:

- Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI) vigente de la C.G. de Medellín.
- Modelo de Seguridad y Privacidad de la Información.
- Procedimientos SIGI que sean pertinentes.
- Guías del MinTic para el modelo de seguridad.
- Norma ISO 27001 - Gestión de la seguridad de la información, y su Anexo A.
- Decreto 1474 de 2017 – Dirección de Gobierno Digital.
- Ley 80 de 1993 Por la cual se expide el Estatuto General de Contratación de la Administración Pública.
- Decreto 1008 del 14 de junio de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- Ley 603 de 2000, llamada en algunos casos como ley de licencias de Software (o Ley para cumplimiento de las licencias de Software).
- El artículo 29 de la Ley 23 de 1982.
- Ley 44 de 1993 derechos de autor.

3. OBJETIVOS DE LA EVALUACION

3.1 OBJETIVO GENERAL

Evaluar las políticas, programas y controles que tengan como finalidad preservar la confidencialidad, integridad, disponibilidad y privacidad de la información de dos de los procesos de la Dirección de Desarrollo Tecnológico de la Contraloría General de Medellín, basados en buenas prácticas internacionales y lineamientos del Modelo de Seguridad y Privacidad de la Información.

3.2 OBJETIVOS ESPECIFICOS

- Evaluar los procedimientos para asignación de claves de acceso, modificaciones, cancelaciones, entre otros y sus posibles vulnerabilidades.
- Realizar seguimiento a la implementación de controles de seguridad informática como son un sistema de control de amenazas Malware.
- Evaluar el nivel de seguridad de la información en la Entidad, analizando en este caso los procesos o temas como la seguridad de la información y los derechos de autor y comprobando si sus políticas de seguridad se cumplen**.**
- Evaluar el acceso al directorio activo, igualmente la generación de contraseñas seguras y la asignación de privilegios o vulnerabilidades producidas por los usuarios.

4. ALCANCE

La auditoría a la gestión del proceso de Seguridad de la Información se encuentra dentro del marco del procedimiento SC05-C01 Gestión de Seguridad de la Información, asociado a la gestión de riesgos de seguridad digital, así como el cumplimiento de políticas de seguridad y privacidad de la información, para nuestro caso en particular la enfocaremos a evaluar los procedimientos para asignación de claves de acceso, realizar seguimiento a la implementación de controles de seguridad informática (Malware) y evaluar si se cumple los derechos de autor del software de propósito general, los cuales tendrán como vigencia el período comprendido entre enero y diciembre de la vigencia 2021. No obstante, se podrán incorporar hechos adicionales que se evidencien en la auditoria y que estén por fuera del periodo definido en el alcance, hechos que quedarán habilitados para la evaluación que se adelante. En los casos que sea necesario ampliar información, se tomaran muestras de soportes o transacciones de otras vigencias.

Es de anotar que para esta Auditoria se tomaran como temas relevantes la seguridad de la información y los derechos de autor.

5. METODOLOGIA

La evaluación incluye: planificación, ejecución y comunicación de resultados del seguimiento realizado a los objetivos enunciados en este documento para el año 2021.

Cada etapa de la auditoría se llevará a cabo de acuerdo a la evaluación de la información aportada por los dueños del proceso de la Dirección de Desarrollo Tecnológico de la Entidad y con el personal de la misma área, mediante entrevistas y ejecución de pruebas de los equipos o estaciones de trabajo para determinar la legalidad del licenciamiento.

6. REFERENCIA RESPUESTA DEL AUDITADO

La Dirección de Desarrollo Tecnológico objeto de esta auditoría, dio respuesta a la información solicitada en comunicación radicada bajo el No 1520 – 202100010153 radicado el 26/11/2021, en el cual expresa lo siguiente:

De acuerdo con la solicitud de información referente al radicado 202100009835, sobre la Evaluación Independiente a los Servicios de Tecnología de la Información, le remito las respectivas respuestas y se necesitan ampliación al respecto estaremos disponibles.

1. Controles, Políticas y Procedimientos de Seguridad:

La Dirección de Desarrollo Tecnológico está inmersa al proceso Gestión de Recursos e Infraestructura, dentro de este proceso está definido el procedimiento de Gestión de los Servicios TI, el cual tiene por objetivo “Prestar los servicios de tecnologías de la información y las comunicaciones –TIC, para el óptimo funcionamiento de la Entidad, mediante actividades de gestión y servicios de Outsourcing.”. Como condición inicial de este procedimiento se presenta el manual de políticas de operación, donde se definen los lineamientos a seguir en materia de Política de Gobierno Digital y Modelo de Seguridad y Privacidad de la Información.

La Dirección de desarrollo tecnológico cuenta con las políticas de uso de servicios informáticos; estas políticas definen los objetivos buscados por la dependencia de cara a los servicios de TI prestados a los usuarios con los ítems definidos en el catálogo de servicios de TI. Con los objetivos claros el equipo técnico de la Dirección de Desarrollo Tecnológico define los elementos de software y hardware necesarios para sostener la operatividad de la institución.

Cada elemento de Hardware y software presenta mecanismos para ejecutar su labor y coherente con cada elemento y su tecnología se tienen los elementos de seguridad que los acompañan y definen las mejores prácticas posibles dentro del ámbito tecnológico adquirido.

En el ámbito administrativo lo que se define como procedimientos, en el ámbito tecnológico está enmarcado sobre los elementos de configuración definidos por

el fabricante de un hardware o software a través de manuales o esquemas de implementación para obtener los mejores resultados con las prácticas más adecuadas posibles.

Con estas implementaciones técnicas se definen los controles que en el ámbito tecnológico están enmarcadas en configuraciones o parametrizaciones sobre los elementos de hardware o software, que para este contexto se enfocaran en el ámbito de la seguridad.

Definido nuestro contexto operacional, pasamos a enumerar los controles implementados por la Dirección de Desarrollo Tecnológico:

- **Control Segmentación de subredes**

Este permite tener ocultas las redes de otras redes, evitando que tráfico sospechoso pueda afectar o buscar servicios con debilidades en elementos de hardware o software.

- **Control de Navegación de entrada desde el internet**

Este permite que los servicios publicados reciban la navegación adecuada desde internet, permitiendo que los sistemas firewall de la CGM solo reciban tráfico desde ciertos puntos, para este tipo de control se tienen definidas listas negras que permiten que según los boletines emitidos por la csirt podamos restringir el tráfico recibido de ciertas IP, de igual forma minimizando el área de ataques de seguridad posibles se tienen restricciones para recibir tráfico de países que son monitoreados por las firmas de seguridad internacionales(ej. Check Point Software Technologies) como emisores de ataques de seguridad por ciberdelincuentes.

- **Control de tráfico desde internet aislado en DMZ**

Se cuenta con el aislamiento de los servidores que están publicados a internet a través de un esquema de infraestructura que determina una zona desmilitarizada de red donde los servidores no se comunican con los demás equipos de la CGM, evitando que un posible atacante llegue a los servicios principales de TI. Esto es una práctica recomendada por los mejores esquemas de seguridad del mundo.

- **Control de tráfico encriptado**

  A través de la utilización de certificados de seguridad SSL se mantiene segura la comunicación a través de internet para el tráfico de los servicios publicados por la entidad.

- **Control de Navegación de Salida hacia Internet por usuarios**

  Este permite a través de reglas y políticas de los equipos firewall tener control del tráfico de salidas a través de solicitudes de usuarios, limitando el mismo a categorías permitidas y que son de necesidad de la CGM para el cumplimiento de sus labores organizacionales.

- **Control de Navegación de salida hacia internet por aplicaciones**

  Este permite a través de reglas y políticas de los equipos firewall tener control del tráfico de salidas a través de solicitudes de aplicaciones, limitando el mismo a categorías permitidas y que son de necesidad de la CGM para el cumplimiento de sus labores organizacionales

- **Control de seguimiento a posibles ataques de red**

  Este permite que a través funcionalidades IPS, SSL/TLS inspection Malware y Zero-day protection, analizar todo el tráfico de red para determinar posibles riesgos de seguridad y bloquear cualquier posible amenaza, con actualizaciones constantes a través de canales seguros.

- **Control de acceso a internet por servidores**

  Se limita el acceso a internet a los servidores que realmente necesitan la explotación de algún servicio del internet, bloqueando específicamente los que no deben tener ningún tipo de exposición de internet.

- **Control de aseguramiento de servidores a través de la Tecnología WAF**

  Protección de trafico de servidores con reglas específicas de firewall para la revisión antivirus de uploads a los servidores, bloqueo de clientes con mala

reputación, sql injection attacks, xss attaks, applications attacks, protocol enforcement, scanner detection, data leakage.

- **Control Protección avanzada contra amenazas**

  Advanced Threat Protection (ATP) puede ayudar a detectar rápidamente clientes infectados o comprometidos dentro de la red y generar una alerta o eliminar el tráfico de esos clientes. En este artículo se explica cómo configurar ATP.

- **Control de puertos publicados a la Internet**

  Este busca tener controlados los puertos que son publicados a través del firewall y que puedan ser factores de debilidades de seguridad para CGM, y que pueden convertirse en factores de ataques para ciberdelincuentes externos a la organización.

- **Control de Ping y Tracert desde la Internet**
  Minimizando las posibilidades de que herramientas tecnológicas puedan escanear los puertos y servicios publicados a la internet.

- **Control de navegación por perfiles de seguridad**
  Asignados según lo establecido en las políticas de servicios TI, se tienen perfiles de navegación por usuario, de acuerdo a sus perfiles de funciones establecidos por la entidad.

- **Control de instalación de aplicaciones**
  Se tiene establecido por GPO bloqueo para la instalación de cualquier aplicación sobre los equipos de cómputo de la CGM sin la utilización de un usuario administrativo.

- **Control de Antivirus sobre los equipos de cómputo**
  Se tiene instalado un antivirus de última generación, con tecnología Intercept X, para prevenir riesgos de Malware, antivirus, ransonware, entre otros.

- **Control de Antivirus sobre los equipos servidores**
  Se tiene instalado un antivirus de última generación, con tecnología Intercept X, para prevenir riesgos de Malware, antivirus, ransonware, entre otros. Contando enfáticamente con vigilancia de procesos de servidor y de intrusiones, garantizando el mayor rendimiento posible del servidor.

- **Control de seguimiento a amenazas por informes de la CSIRT**
  Se mantiene constante seguimiento a los boletines de seguridad emitidos por la scirt, informando de las amenazas de seguridad detectadas a nivel nacional y que pueden afectar a las entidades y usuarios.

- **Control de archivos ejecutados en servidores.**
  Implementación de listas negras de bloqueo para extensiones de archivos en servidores de documentos, en la medida de lo posible es una buena práctica para prevenir el ataque ransonware.

- **Control de acceso de usuario**
  Este control se configura con la asignación de un usuario único a cada funcionario, acompañado de un mecanismo de Password para acceder a los recursos de TI habilitados para el perfil de usuario determinado.

- **Control de Cambios de Password**
  Se cuenta con GPO de control de cambio de Password, para garantizar la implementación de un esquema que garantice la rotación de los password de forma que no sean fácilmente identificables

- **Control de cambios a cuentas Administrativas**
  Se cuenta con GPO que permiten cambiar periódicamente los password de las cuentas administradoras locales de los equipos de cómputo de la CGM.

- **Control de doble autenticación en los elementos de gestión Perimetral y antivirus**
  Mediante la utilización de doble factor de autentificación se tiene protección de las consolas administrativas de los Firewalls y Antivirus.

- **Control de la política de prevención de perdida de datos**
  A través del sistema antivirus se tiene implementado el registro y seguimiento a política de prevención de perdida de datos. a prevención de pérdida de datos (DLP) controla la pérdida accidental de datos. DLP le permite monitorear y restringir la transferencia de archivos que contienen datos confidenciales. Por ejemplo, puede evitar que un usuario envíe un archivo que contiene datos confidenciales a casa mediante correo electrónico basado en web.

- **Control de Alta disponibilidad para equipos de seguridad perimetral**
  Se cuenta con un esquema de alta disponibilidad para los equipos firewall de garantiza en gran medida el funcionamiento del servicio en caso de fallas, ya sean de índole físico, lógico o por posibles interferencias de seguridad.

- **Control de remitentes seguros de Email**
  Se implementaron listas de seguridad de remitentes seguros en listas blancas y negras bajo la tecnología de seguridad de Microsoft 365.

- **Control de correo spam**
  Se tiene a disposición de la entidad la tecnología de protección contra spam que brinda Microsoft 365, enmarcada en una gran colección de verificaciones de seguridad sobre la fiabilidad de remitentes seguros.

- **Control de protección antivirus para el correo electrónico**
  Se cuenta con el servicio de antivirus de Microsoft 365 para la verificación de todos los archivos enviados o recibidos por correo electrónico.

- **Control de acceso al correo electrónico de Microsoft 365 con doble autenticación**
  Se cuenta con el servicio de doble autenticación de Microsoft 365 para validar la autenticidad del usuario mediante la utilización del correo electrónico secundario registrado o el celular del mismo, previa validación.

- **Control de prevención de ataques de ciberseguridad medida honeypot**
  Se tienen implementados plantillas de honeypot para ser desplegadas en

caso de un ataque cibernético que vulnere los esquemas de seguridad implementados, dichos honeypot tienen como función desviar los objetivos de los atacantes, atrayéndolos a servicios vulnerables en una red aislada del resto de la red corporativa, evitando el acceso a los servicios principales de la CGM.

- **Control de aplicaciones a través de firewall**
  Visibilidad y control completos sobre todas las aplicaciones de su red con tecnología de escaneado profundo y control de aplicaciones sincronizado que permite identificar todas las aplicaciones que actualmente no están siendo identificadas en la red. Bloqueo de descarga de aplicaciones para prevención de su instalación.

- **Control de aplicaciones a través del antivirus**
  Establecimiento de políticas de control de aplicaciones para prevenir la descarga y acceso USB u otro físico de programas prohibidos para su instalación en los equipos de cómputo de la CGM.

- **Control de Plugins exploradores WEB.**
  Se tiene configurados GPO que permiten la administración de los exploradores WEB y en este sentido se bloquea la instalación de plugins peligrosos o que puedan generar algún riesgo de seguridad.

- **Control de elementos Ejecutados en USB o medios extraíbles**
  Se tienen bloqueos a nivel de GPO y del sistema antivirus para prevenir la ejecución de software malicioso de cualquier tipo desde las USB o medios extraíbles que dispongan los equipos de cómputo.

2. Inventario de licencias de Software de propósito general y que están en uso, con que cuenta la Entidad para estaciones de trabajo.

¿Con cuántos equipos cuenta la entidad?

Con respecto a este numeral, que lo relacionado con el inventario oficial de los equipos de cómputo, responsable, ubicación y placa que identifica a los mismos,

es competencia de la Dirección de Recursos Físicos y Financieros, quien es la responsable de velar porque cada uno de estos bienes esté bajo la responsabilidad de los funcionarios de la Contraloría General de Medellín.

¿El software instalado en estos equipos se encuentra debidamente licenciado?

Todo el software instalado en los equipos de cómputo de la Contraloría General de Medellín cuenta con su respectiva licencia.

- ¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?

Para acceder a los recursos informáticos de la Red de datos de la Contraloría General de Medellín, los usuarios requieren de una identificación única e intransferible, la cual consiste en un nombre de usuario y una contraseña; a este nombre de usuario se le asocian los privilegios o permisos que tendrá en la operación del sistema, de tal manera, que ninguno de los usuarios tiene permiso para instalar programas o aplicativos en los computadores; solamente desde las cuentas con privilegios de administrador se pueden realizar estas acciones. Sólo el personal de Desarrollo Tecnológico está autorizado para utilizar las cuentas con privilegios de administrador y realizar las configuraciones de los equipos e instalar el software en los mismos, según lo establecido según las políticas de uso de servicios informáticos.

Se cuenta además con:

- **Control de instalación de aplicaciones**
  Se tiene establecido por GPO bloqueo para la instalación de cualquier aplicación sobre los equipos de cómputo de la CGM sin la utilización de un usuario administrativo.

- **Control de Plugins exploradores WEB.**
  Se tiene configurados GPO que permiten la administración de los exploradores WEB y en este sentido se bloquea la instalación de plugins peligrosos o que puedan generar algún riesgo de seguridad.

- **Control de aplicaciones a través del antivirus**
  Establecimiento de políticas de control de aplicaciones para prevenir la descarga y acceso USB u otro físico de programas prohibidos para su instalación en los equipos de cómputo de la CGM.

- **Control de aplicaciones a través de firewall**
  Visibilidad y control completos sobre todas las aplicaciones de su red con tecnología de escaneado profundo y control de aplicaciones sincronizado que permite identificar todas las aplicaciones que actualmente no están siendo identificadas en la red. Bloqueo de descarga de aplicaciones para prevención de su instalación.

- **Aplicación de Control de inventario de software**
  Se realiza seguimiento a las aplicaciones instaladas en los equipos de la CGM a través del system center configuration manager.

- **Control de elementos Ejecutados en USB o medios extraíbles**
  Se tienen bloqueos a nivel de GPO y del sistema antivirus para prevenir la ejecución de software malicioso de cualquier tipo desde las USB o medios extraíbles que dispongan los equipos de cómputo.

  - ¿Cuál es el destino final que se le da al software dado de baja?

  Según lo establecido en las Políticas operacionales de la CGM en su numeral 40:

  "*Para dar de baja a un bien del inventario el Director Administrativo de la Dirección de Recursos Físicos y Financieros, presenta al Comité Técnico de*

Inventarios (COTEIN) el listado de los bienes no útiles, inservibles y en desuso, con el respectivo concepto técnico, para que se autorice la su baja y disposición final."

Y en concordancia con la resolución 618 del 21 de diciembre del 2020, es función del COTEIN:

"*Aprobar y recomendar la baja de las licencias y los software, previa Determinación técnica de la Dirección Administrativa de desarrollo Tecnológico de la Entidad sobre su obsolescencia o vencimiento de las mismas*"

Por lo anterior, el destino final que se da al software dado de baja es aprobado por el COTEIN y no es correspondencia de la Dirección de Desarrollo Tecnológico

3. Documento del Plan Estratégico de las Tecnologías de la Información (PETI) de la Entidad. Se anexa documento.

4. Documento de Planes de continuidad con que cuenta la Entidad en materia de informática.

Se cuenta con el PLAN DE CONTINUIDAD DEL NEGOCIO DE LOS SERVICIOS TI –2021; este documento es de consulta exclusiva de los funcionarios adscritos a la Dirección de Desarrollo Tecnológico, está disponible para la consulta en dicha oficina por los funcionarios de la auditoria, no es posible la entrega de una copia del mismo ya que es un documento de reserva sensible que contiene la información de toda la infraestructura tecnológica de la entidad y por lo tanto es un alto riesgo de seguridad publicar o divulgar esta información por cualquier medio.

5. Información sobre las herramientas o software que utiliza la Entidad para el manejo y tratamiento de amenazas de Malware (nombre, descripción y funcionalidad).

Nombre: Sophos Intercep X endpoint

Descripción: Sophos Intercept X es la mejor protección para endpoints del mundo. Detiene las ciber amenazas más recientes con una combinación de IA con Deep Learning, funciones antiransomware, prevención de exploits y otras técnicas.

Funciones

Detenga las amenazas desconocidas
La IA con Deep Learning de Intercept X destaca en la detección y el bloqueo de malware incluso si es desconocido. Lo consigue examinando detenidamente los atributos de los archivos de cientos de millones de muestras para identificar amenazas sin necesidad de firmas.

Bloquee el ransomware
Intercept X incluye funciones antiransomware avanzadas que detectan y bloquean los procesos de cifrado malicioso utilizados en los ataques de ransomware. Los archivos que se han cifrado se revierten a un estado seguro, lo que minimiza cualquier impacto en la productividad empresarial.

- **Impida los exploits**
  La tecnología antiexploits detiene las técnicas de explotación de las que se sirven los atacantes para infiltrarse en dispositivos, robar credenciales y distribuir malware. Al detener las técnicas usadas en toda la cadena de ataque, Intercept X mantiene protegida su empresa frente a los ataques sin archivos y los exploits de día cero.

- **Defensas por capas**
  Además de una moderna y potente funcionalidad, Intercept X también utiliza técnicas tradicionales probadas. Algunos ejemplos de estas funciones incluyen el bloqueo de aplicaciones, el control web, la prevención de pérdidas de datos y la detección de malware basada en firmas. Esta combinación de

técnicas modernas y tradicionales reduce la superficie de ataque y ofrece una defensa en profundidad óptima.

- **Seguridad Sincronizada**
  Las soluciones de Sophos funcionan mejor de forma conjunta. Por ejemplo, Intercept X y Sophos Firewall comparten datos para aislar automáticamente los dispositivos comprometidos al tiempo que se realiza la limpieza, y luego restablecen el acceso a la red una vez neutralizada la amenaza. Todo ello sin necesidad de que intervenga ningún administrador.

- **Detección y respuesta para endpoints (EDR)**
  Sophos EDR, diseñado para administradores de TI y especialistas en ciberseguridad, responde preguntas críticas sobre la búsqueda de amenazas y las operaciones de TI. Por ejemplo, identifica dispositivos con problemas de rendimiento o procesos sospechosos que intentan

  conectarse en puertos no estándar y después accede de forma remota al dispositivo para tomar medidas correctivas.

- **Managed Threat Response (MTR)**
  Servicio de búsqueda, detección y respuesta a amenazas 24/7/365 prestado por un equipo de expertos de Sophos. Los analistas de Sophos responden a posibles amenazas, buscan indicadores de peligro y proporcionan análisis detallados sobre los eventos que incluyen lo que ha ocurrido, dónde, cuándo, cómo y por qué

- **Detección y respuesta ampliadas (XDR)**
  Vaya más allá de los endpoints y servidores, y sírvase del firewall, el correo electrónico y otras fuentes de datos*. Obtenga una visión holística de la posición de ciberseguridad de su empresa con la capacidad de profundizar en detalles granulares. Por ejemplo, entienda los problemas de red de sus oficinas y qué aplicaciones los están provocando

- **Nombre: Sophos Firewall**

  Descripción: Sophos Firewall ofrece la mejor protección para detener al instante los ataques e infiltraciones más recientes antes de que entren en su red.

Funciones

- **Inspección detallada de paquetes**
  El motor de inspección detallada de paquetes (DPI) de Xstream ofrece análisis del tráfico de alto rendimiento para IPS, AV, protección web y control de aplicaciones en un único motor de transmisión. Escaneado antivirus de doble motor basado en proxy

- **Tráfico cifrado**
  La inspección TLS 1.3 de Xstream con un rendimiento, visibilidad, herramientas de políticas e inteligencia integrada líderes en el sector elimina un enorme punto ciego en su protección.

- **Protección con ML y de día cero**
  Sophos Firewall se sirve de la tecnología de Machine Learning líder del sector (con el respaldo de SophosLabs Intelix) para identificar al instante el ransomware y las amenazas desconocidas más recientes antes de que entren en su red.

- **Espacios seguros en la nube**
  El análisis de archivos dinámico de día cero de Sophos utiliza la tecnología de espacio seguro en la nube next-gen con Deep Learning y la mejor tecnología de Intercept X para ofrecer a su empresa la mejor protección contra amenazas de día cero, como el ransomware y los ataques dirigidos más recientes vía phishing, spam o descargas web.

- **Protección web**
  El motor de protección web de Sophos cuenta con el respaldo de SophosLabs e incluye innovadoras tecnologías necesarias para identificar y bloquear las últimas amenazas web.

- **Seguridad sincronizada**
  Nuestro revolucionario Security Heartbeat vincula su endpoint administrado por Sophos con su firewall para compartir el estado de seguridad y otra información valiosa, lo que posibilita una respuesta coordinada y automatizada para aislar amenazas y evitar la propagación lateral.

- **Protección avanzada contra amenazas**
  Sophos Firewall proporciona una protección contra amenazas avanzadas que identifica al instante bots y otras amenazas avanzadas al tiempo que defiende su red de los sofisticados ataques modernos.

- **Identidad del usuario**
  Las políticas basadas en la identidad del usuario y el análisis de riesgo de usuarios le proporcionan la información y la capacidad para recuperar el control de sus usuarios antes de que se conviertan en una grave amenaza para la red.

- **Control de aplicaciones**
  Visibilidad y control completos sobre todas las aplicaciones de su red con tecnología de escaneado profundo y control de aplicaciones sincronizado que permite identificar todas las aplicaciones que actualmente no están siendo identificadas en la red.

- **Control web**
  Visibilidad y control completos sobre todo el tráfico web con herramientas de aplicación flexibles que funcionan según sus necesidades, con opciones de cumplimiento para actividad, cuotas, programaciones y conformado de tráfico según usuarios y grupos.

- **Correo electrónico y datos**
  Proteja el correo electrónico contra el spam, el phishing y la fuga de datos con nuestra exclusiva protección todo en uno que combina cifrado de correo electrónico basado en políticas con DLP y antispam.

➢ **Nombre: Microsoft 365 Defender**

Descripción: Microsoft Defender para Office 365 es un servicio de filtrado de correo electrónico basado en la nube que ayuda a proteger su organización contra amenazas avanzadas para el correo electrónico y las herramientas de colaboración, como phishing, compromiso de correo electrónico empresarial y ataques de malware. Defender for Office 365 también proporciona capacidades de investigación, búsqueda y corrección para ayudar a los equipos de seguridad a identificar, priorizar, investigar y responder de manera eficaz a las amenazas.

Funciones

- Directivas de seguridad preestablecidas y analizador de configuración.
- Archivos adjuntos seguros
- Caja fuerte Datos adjuntos en Teams
- Vínculos seguros
- Documentos seguros
- Vínculos seguros en Teams
- Protección para SharePoint, OneDrive y Microsoft Teams
- Directivas contra phishing
- Protección avanzada para correo interno
- Rastreadores de amenazas
- Investigación de amenazas (investigación avanzada de amenazas)

Entre las tecnologías se incluyen:

- correo no deseado

- suplantación de identidad
- malware
- correo masivo
- inteligencia contra la suplantación de identidad
- detección de suplantación
- Cuarentena del administrador

- Entregas de usuarios y administradores de Falsos positivos y Falsos negativos
- Permitir/bloquear direcciones URL y archivos
- Informes

6. Plan o programas de socialización de políticas y procedimientos que en materia de seguridad tiene la Entidad y medios de divulgación que ha empleado para las mismas.

Las políticas y procedimientos en materia de seguridad se han sensibilizado a través de los boletines y carteleras electrónicas, donde se plasman los mensajes y se tiene una programación que se le remite a la Oficina Asesora de Comunicaciones, además a los funcionarios que ingresan a la Entidad se las da una inducción sobre las políticas de los servicios informáticos, la cual se incluye los cuidados y limitaciones de las claves de acceso, sistemas de información, los perfiles que tienen asignados. Se anexan las campañas de sensibilización, los cuales han sido publicados en los boletines que se encuentran en la intranet.

7. Presupuesto asignado a la seguridad, teniendo en cuenta los objetivos trazados para esta Auditoria.

La Contraloría General de Medellín no cuenta con sub segmentación del presupuesto asignado por dependencias por temas específicos, sin embargo, podemos que la inversión directa en elementos de seguridad TI para el año 2021 tiene un valor de $186.000.000.00.

8. Asignación presupuestal a la Dirección de Desarrollo Tecnológico en la

vigencia 2021 para el desarrollo de proyectos informáticos.

El presupuesto asignado para la Vigencia 2021 a la Dirección de Desarrollo Tecnológico fue de $968, 600,000.00

9. Bitácora de Incidentes de Seguridad de la Información (si existe).

La Bitácora por definición es un cuaderno que permite llevar un registro escrito de diversas acciones y su comportamiento es generalmente cronológico.

En este sentido a la luz del contexto que nos atañe, que son las tecnologías de la información, las bitácoras son el símil de los LOGS de aplicaciones o eventos del sistema. En este sentido las herramientas de seguridad mencionados anteriormente cuentan con todos los elementos necesarios para generar los informes de los LOGS correspondientes.

Como es de anotarse que, aunque se presenten elementos detectados en los LOGS, no se presentaron materialización de riesgos de seguridad en concordancia con los controles implementados.

10. Información estadística que permita medir el grado de satisfacción de las partes interesadas en la seguridad (Si existe).

No existe dentro de nuestro procedimiento o políticas el esquema para esta medición; este elemento es subjetivo he inversamente satisfactorio a los elementos de seguridad implementados. Los usuarios perciben la seguridad como un bloqueo innecesario y en un sentido más real de la expectativa humana, como no se ha materializado una amenaza real a la seguridad de la información de la CGM precisamente por los controles implementados por la Dirección de Desarrollo Tecnológico, nuestros usuarios no tienen la experiencia de lo que significa que un riesgo de seguridad se materialice y se pierda gran cantidad de información o toda la información, lo que hace que no se perciba el trabajo de seguridad en sí. En realidad, desde un punto de vista técnico esta medición de satisfacción no aporta nada a la realidad de la seguridad.

7. RESULTADOS DE LA EVALUACIÓN

Con este informe de auditoría de seguridad se pretende presentar de forma clara y concisa los temas seleccionados para esta Auditoria y los resultados obtenidos y las medidas correctoras necesarias en ciberseguridad a aplicar.

Con el informe de la auditoría la Contraloría General de Medellín podrá conocer cuál es el estado de procedimientos para asignación de claves de acceso, y sus posibles vulnerabilidades, así como de sus políticas de seguridad, sistema de control de amenazas Malware, derechos de autor del software de propósito general y contraseñas seguras y la asignación de privilegios, con lo cual podrá tomarse las decisiones oportunas para mejorarlas e incrementar su nivel de seguridad.

Este informe de auditoría de ciberseguridad incluirá las actuaciones recomendadas si las hay para el mejoramiento de los puntos críticos (con alto riesgo) que se han encontrado, para poder eliminar el riesgo asociado. Con las auditorías de seguridad se pretende contribuir a un sistema más seguro y ágil a la hora de reaccionar ante cualquier amenaza externa o incidente interno en materia de seguridad.

Para efectos de dar cumplimiento a los objetivos propuesto en la evaluación, se evaluaron los siguientes procedimientos que se detallan a continuación:

7.1 Evaluar los procedimientos para asignación de claves de acceso, modificaciones, cancelaciones, entre otros y sus posibles vulnerabilidades y evaluar el acceso al directorio activo, igualmente la generación de contraseñas seguras y la asignación de privilegios o vulnerabilidades producidas por los usuarios.

Vulnerabilidades producidas por contraseñas

Con el trabajo en casa, el teletrabajo y el cloud computing la gestión de contraseñas se ha convertido en uno de los puntos más importantes en ciberseguridad. Para acceder a las plataformas de trabajo de las entidades es necesario utilizar un usuario y contraseña. Utilizar contraseñas poco seguras genera vulnerabilidades en los sistemas, pues si son fácilmente descifrables pueden generar incursiones de terceros no autorizados que pueden robar, modificar o eliminar información, cambiar configuraciones si disponen de los privilegios apropiados, o incluso apagar equipos.
La generación de contraseñas seguras es una de las claves para incrementar el nivel de ciberseguridad de las empresas.

Todavía hoy, muchos usuarios y trabajadores anotan sus contraseñas en una libreta o utilizan contraseñas poco seguras (1234 sigue siendo la más utilizada). Un hacker puede descubrir una contraseña poco segura en segundos, y conocer el grado de vulnerabilidad de estas nos ayudará a mejorar su seguridad.

Es así como tras la realización de esta auditoría podremos ser conscientes del grado de vulnerabilidad de nuestra Entidad a los posibles ataques. Este informe, además, cuenta con la enumeración de las medidas a llevar a cabo para mejorar la protección de los sistemas de la Entidad.

Así mismo, la auditoría narra algunos de los diferentes controles implementados por la Dirección de Desarrollo Tecnológico en caso de ataques. En ellos, se especifica qué hacer en caso de que nuestra Entidad sea atacada y qué pasos se van a seguir.

“Para acceder a los recursos informáticos de la Red de datos de la Contraloría General de Medellín, los usuarios requieren de una identificación única e intransferible, la cual consiste en un nombre de usuario y una contraseña; a este nombre de usuario se le asocian los privilegios o permisos que tendrá en la operación del sistema, de tal manera, que ninguno de los usuarios tiene permiso para instalar programas o aplicativos en los computadores; solamente desde las cuentas con privilegios de administrador se pueden realizar estas acciones. Sólo el personal de Desarrollo Tecnológico está autorizado para utilizar las cuentas con privilegios de administrador y realizar las configuraciones de los equipos e instalar el software en los mismos, según lo establecido según las políticas de uso de servicios informáticos.”

Vulnerabilidades producidas por los usuarios

Una de las principales causas de los ataques informáticos está relacionada con un uso incorrecto o negligente por parte de un usuario. Una mala asignación de privilegios o permisos puede hacer que un usuario tenga acceso a opciones de administración o configuración para las que no está preparado, cometiendo errores que suponen una amenaza para la empresa.

El error humano es otra causa de riesgos en ciberseguridad. El usuario siempre tiene el riesgo de cometer un error que pueda generar una vulnerabilidad que suponga una amenaza informática. Por eso en ciberseguridad se tiende

a automatizar procesos críticos para minimizar o eliminar el factor de riesgo del error humano.

Las malas prácticas o la falta de formación en ciberseguridad también generan vulnerabilidades, como la apertura de archivos de dudosa procedencia, engaños por publicidad falsa, apertura de correos fraudulentos y similares. Estas acciones son una amenaza que pueden causar ataques como el *phishing* (suplantación de identidad) o similares.

Ejemplos de Controles establecidos por la dirección de Desarrollo tecnológico en este tema son los siguientes:

Control de seguimiento a posibles ataques de red

Este permite que a través funcionalidades IPS, SSL/TLS inspection Malware y Zero-day protection, analizar todo el tráfico de red para determinar posibles riesgos de seguridad y bloquear cualquier posible amenaza, con actualizaciones constantes a través de canales seguros.

Control de Antivirus sobre los equipos de computo

Se tiene instalado un antivirus de última generación, con tecnología Intercept X, para prevenir riesgos de Malware, antivirus, ransonware, entre otros.

Control de Navegación de entrada desde el internet

Este permite que los servicios publicados reciban la navegación adecuada desde internet, permitiendo que los sistemas firewall de la CGM solo reciban tráfico desde ciertos puntos, para este tipo de control se tienen definidas listas negras que permiten que según los boletines emitidos por la csirt podamos restringir el tráfico recibido de ciertas IP, de igual forma minimizando el área de ataques de seguridad posibles se tienen restricciones para recibir tráfico de países que son monitoreados por las firmas de seguridad internacionales(ej. Check Point Software Technologies) como emisores de ataques de seguridad por ciberdelincuentes.

Control de Navegación de salida hacia internet por aplicaciones

Este permite a través de reglas y políticas de los equipos firewall tener control del tráfico de salidas a través de solicitudes de aplicaciones, limitando el mismo a categorías permitidas y que son de necesidad de la CGM para el cumplimiento de sus labores organizacionales.

Control Protección avanzada contra amenazas

Advanced Threat Protection (ATP) puede ayudar a detectar rápidamente clientes infectados o comprometidos dentro de la red y generar una alerta o eliminar el tráfico de esos clientes. En este artículo se explica cómo configurar ATP.

Control de Antivirus sobre los equipos servidores

Se tiene instalado un antivirus de última generación, con tecnología Intercept X, para prevenir riesgos de Malware, antivirus, ransonware, entre otros. Contando enfáticamente con vigilancia de procesos de servidor y de intrusiones, garantizando el mayor rendimiento posible del servidor.

Control de acceso de usuario

Este control se configura con la asignación de un usuario único a cada funcionario, acompañado de un mecanismo de Password para acceder a los recursos de TI habilitados para el perfil de usuario determinado.

Control de Cambios de Password

Se cuenta con GPO de control de cambio de Password, para garantizar la implementación de un esquema que garantice la rotación de los password de forma que no sean fácilmente identificables

Control de cambios a cuentas Administrativas

Se cuenta con GPO que permiten cambiar periódicamente los password de las cuentas administradoras locales de los equipos de cómputo de la CGM.”

Es de anotar que en la realización de esta Auditoria se determinó la existencia de los anteriores controles y algunos otros que coadyuvan al establecimiento de una buena seguridad en la Entidad, acorde con la privacidad de la información y las Leyes que para este tipo de entidades rige.

En conclusión, en lo referente a esta materia la Contraloría General de Medellín, cuenta con suficientes controles y procedimientos para asignación de claves de acceso y de generación de contraseñas seguras y la asignación de privilegios, los cuales aportan en alto grado a minimizar las vulnerabilidades producidas por los

usuarios y otros actores que intervienen en este proceso de mantener la ciberseguridad en la Entidad.

7.2 Realizar seguimiento a la implementación de controles de seguridad informática como son un sistema de control de amenazas Malware.

La dependencia de las tecnologías de la información por parte de las Entidades ha generado una alta preocupación por la ciberseguridad.

Las vulnerabilidades y amenazas informáticas son un riesgo para los sistemas y la información de la Entidad, sobre todo en el entorno actual, altamente digitalizado y dependiente de los servicios TI.

Para poder tomar las medidas adecuadas para proteger los recursos tecnológicos y la información de la empresa es necesario conocer cuáles son las principales amenazas y vulnerabilidades que ponen en riesgo la seguridad de la empresa en la red.

VULNERABILIDADES

Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un "*agujero*" que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para poder entrar en los mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento.

Las vulnerabilidades son una de las principales causas por las que una empresa puede sufrir un ataque informático contra sus sistemas. Por eso siempre es recomendable actualizar a las últimas versiones, las aplicaciones informáticas, sistemas de protección y sistemas operativos, pues esas actualizaciones contienen muchas correcciones sobre vulnerabilidades descubiertas.

AMENAZA INFORMATICA

Se entiende como amenaza informática toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas).

Son muchas las vulnerabilidades y amenazas informáticas a las que pude estar expuesta la Entidad en la actualidad. Por eso la inversión en ciberseguridad y sistema de protección se debe potenciar cada vez más.

A continuación, veremos una de las principales amenazas y que está enmarcado como uno de nuestros objetivos específicos:

AMENAZAS DE MALWARE

Los programas maliciosos son una de las mayores ciberamenazas a las que se pude exponer la Entidad. Dentro del malware existen distintos tipos de amenazas, siendo las principales.

Virus: Los virus informáticos son un software que se instala en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento. Para que un virus infecte un sistema es necesaria la intervención de un usuario con o sin intención.

Gusanos: Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en un espacio corto de tiempo.

Troyanos: Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.

Ransomware: El ransomware se ha convertido en el malware más temido en la actualidad por las empresas. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins).

Keyloggers: Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares.

Es así como la Entidad ha establecido políticas e implementado controles que coadyuvan al establecimiento de una mejor protección de los sistemas de la empresa y el fortalecimiento de la seguridad en sus puntos críticos, ejemplo de estas son:

- Control Protección Avanzada Contra Amenazas.
- Control de antivirus sobre los equipos de cómputo.
- Control de antivirus sobre los equipos servidores.
- Control de seguimiento a amenazas por informes de la CSIRT.
- Control de correo SPAM.

Dicho lo anterior y analizando las respuestas dadas por la Dirección de Desarrollo tecnológico con respecto a este tema, podemos deducir que la Entidad cuenta con las herramientas adecuadas para la prevención **AMENAZAS DE MALWARE** y ha implementado controles tendientes a minimizar dichas amenazas**,** acordes a la importancia de la información que se maneja y a la seguridad que debe contemplar este tipo de Entidades.

Respecto a la gestión de medidas preventivas ante los eventos detectados por las herramientas de monitoreo de **MALWARE**: Durante las sesiones de auditoría y la verificación de las alarmas y eventos de seguridad reportados por la Dirección de Desarrollo Tecnológico (Sophos Central Protection) del proveedor GMS Grupo Microsistemas Colombia S.A.S, de acuerdo a los eventos se identificaron registros de seguridad ocasionados por la presencia y eliminación de un Malware (software malicioso) encontrados en equipos de cómputo de usuarios. Al revisar en detalle dichos eventos, se pudo identificar que el malware detectado por el sistema de antivirus provenía de diferentes medios entre esos extraíble, que al parecer se encontraba infectado y estaba siendo conectado por el usuario del equipo de cómputo. Si bien se observó que la solución de antivirus y antimalware se encuentra detectando y eliminando las amenazas, en concordancia con los parámetros establecidos y una base de datos de virus actualizada, no se identificó que los especialistas de mesa de ayuda o el Grupo de Trabajo de la Dirección de Desarrollo Tecnológico hayan advertido a todos los usuario acerca de la presencia de programas maliciosos en sus dispositivos de almacenamiento de información extraíble ni que se hayan tomado las medidas preventivas adecuadas de manera conjunta con el usuario en todos los casos.

Es de anotar que la Dirección de Desarrollo Tecnológico realiza campañas generales para todos los funcionarios, tendientes a minimizar los casos de MALWARE.

Cuando estos se presenten se recomienda socializar con todos los usuarios los eventos que puedan afectar la seguridad de la información de la Contraloría, los correctivos necesarios o procedimientos a seguir con el fin de minimizar la posibilidad de ocurrencia de dichos eventos, igualmente la Dirección de Desarrollo Tecnológico debe establecer un procedimiento escrito para estos casos.

Los ciberdelincuentes no descansan y siempre buscan nuevas formas de atacar, infectar y robar información de las empresas, por lo que la ciberseguridad debe ser una actividad flexible y dinámica que se adapte a las nuevas amenazas. Se debe establecer un procedimiento para llevar a cabo una revisión de ciberseguridad por lo menos cada seis meses.

7.3 Evaluar el nivel de legalidad de las licencias de propósito general en lo concerniente a derechos de autor y comprobando si sus políticas en esta materia se cumplen.

Uno de los asuntos que más preocupa a las empresas hoy en día es la ciberseguridad. La gran dependencia de los negocios de la tecnología, las redes y las comunicaciones han puesto como prioridad la seguridad para poder garantizar la continuidad del negocio.

La auditoría de seguridad informática es la herramienta principal para poder conocer el estado de seguridad en que se encuentra la Entidad, en este caso en lo relacionado con las políticas de seguridad de la información y de derechos de autor.

En la auditoría realizada se tuvo en cuenta examinar y evaluar el sistema de inventario de las licencias de software vigentes, evaluar los controles internos para impedir o detectar Software ilegal que violen la normatividad existente en materia de derechos de autor y determinar como la Contraloría General de Medellín administra el software de propósito general conforme a los procedimientos, normativas y políticas que se tienen en esta materia. La auditoría abarcó el periodo de enero de 2021 a diciembre de 2021.

La Contraloría General de Medellín en el momento de realizar la Auditoria, cuenta con 387 equipos asignados a los funcionarios, de los cuales 189 son propiedad de

la entidad y 198 son de comodato y en bodega existen 44 equipos de los cuales hay 14 nuevos y 30 que fueron reintegrados, los cuales están por evaluar su estado por parte de la Dirección de Desarrollo Tecnológico.

Esta Auditoría Interna encuentra que se llevan a cabo controles de seguridad en varios niveles para minimizar los riesgos. Habría que establecer no obstante la herramienta que posee la Contraloría General de Medellín para distribución del software de propósito general, una muestra aleatoria equivalente al 10% de las 401 estaciones de trabajo equivalente a 40 equipos, de la totalidad con que cuenta la Entidad, para en campo entrar a corroborar el software que pudiera estar ilegal y que entraña riesgos de incumplimiento y seguridad relacionados con los derechos de autor.

Es por esto que se revisó el procedimiento y sus políticas de seguridad en los temas antes mencionados, igualmente se realizó un comparativo entre la herramienta que sirve para instalación de software en la Entidad y el licenciamiento adquirido por la misma, encontrándose que dicho software de propósito general se ajusta a las normas y leyes que en materia de derechos de autor se tienen o aplican en Colombia.

Para determinar la legalidad y veracidad del software instalado en los diferentes equipos, se realizó un trabajo de campo consistente en un recorrido que se hizo con un funcionario de la Dirección de Desarrollo Tecnológico y el equipo auditor por las diferentes dependencias de la Contraloría General de Medellín, pudiéndose constatar que el software existente en los diferentes computadores o estaciones de trabajo obedecen al número de licencias y software de propósito general legalmente adquirido por la Entidad.

Es así como en la Auditoria realizada se pudo determinar que la Entidad para evitar que los usuarios instalen programas o aplicativos cuenta con dos (2) mecanismos de control: 1. Un control automático desde el Directorio Activo que restringe la instalación de software, y 2. Una política de seguridad de la información que fija la responsabilidad del Proceso en la Dirección de Desarrollo Tecnológico frente a la instalación de programas y prohíbe “la descarga, uso, intercambio o instalación” de los mismos por parte de personas no autorizadas. El control automático restringe la instalación de aplicativos por parte de usuarios a partir de la incorporación en el Directorio Activo. De otra parte el Manual de Políticas dispone de varias políticas en

esta materia como el Control de instalación de aplicaciones, Control de aplicaciones a través de firewall e igualmente no se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros y sólo personal designado por la Dirección de Desarrollo tecnológico está autorizado para instalar software en los equipos.

En conclusión, existen políticas lineamientos para la solicitud licencias de software y seguridad de la información. Se observaron controles procedimentales y automáticos para minimizar el riesgo de instalación de software no autorizado.

8. RECOMENDACIONES

La Auditoría Interna identificó posibilidades recomendaciones en algunos aspectos que pueden contribuir a mejor la seguridad, para lo cual la Oficina de Control Interno con base en la auditoría realizada recomienda adelantar las siguientes acciones:

- Es conveniente que la Alta dirección comprometa mayores recursos en materia de seguridad de la información de la Contraloría General de Medellín, e igualmente alineado a esta inversión contratar con entidades externas un estudio de seguridad informática de forma periódica para evaluar el estado de su ciberseguridad y detectar cualquier debilidad o vulnerabilidad que ponga en riesgo sus sistemas e información.

  Realizar dicho estudio no es solo responsabilidad de grandes empresas y Entidades. Hoy en día cualquier tipo de Entidad depende de elementos y dispositivos tecnológicos para poder realizar sus procesos administrativos y misionales, por lo que es necesario que evalúe de forma periódica la seguridad de esta. Las principales ventajas que se conseguiría al realizar una auditoría de seguridad serian**:**

  - Mejora los controles internos de seguridad de la Entidad.
  - Detectar debilidades en los sistemas de seguridad como errores, omisiones o fallos.
  - Identifica posibles actuaciones fraudulentas (acceso a datos no autorizados o robos a nivel interno).
  - Ayuda a eliminar los puntos débiles de la empresa en cuestión de seguridad (webs, correo electrónico o accesos remotos, por ejemplo).
  - Permite controlar los accesos, tanto físicos como virtuales (revisión de privilegios de acceso).
  - Permite mantener sistemas y herramientas actualizadas.

  - La Contraloría debe procurar contar con un equipo dedicado a evaluar los riesgos, mitigar eventos y reaccionar, esta labor debe ser calificada de alta incidencia para la organización y contar con el apoyo de la alta gerencia.

- Fortalecer conocimientos de los funcionarios de la Dirección de Desarrollo tecnológico en metodología de riesgos informáticos y definiciones relacionadas

con amenazas y vulnerabilidades que se deben tener en cuenta a fin de mejorar la supervisión de los controles implementados y en materia de gestión de riesgos de seguridad digital, conocimiento de la Norma ISO27001 y el Modelo Integrado de Planeación y Gestión – MIPG, en lo concerniente a este tema.

- Proveer al equipo de seguridad de herramientas de evaluación de riesgos y prevención de última tecnología y que puedan evolucionar como lo hacen los riesgos para contemplar nuevas amenazas y permitir la reacción oportuna y evitar la pérdida de información.

- Incluir controles documentales para la declaración de aplicabilidad a fin de que se pueda hacer trazabilidad de los cambios del documento, en función de los cambios que se implementen para garantizar la gestión y transmisión de conocimiento enfocado a mejorar los controles de seguridad de la Entidad.

- Cuando estos se presenten se recomienda socializar con todos los usuarios los eventos que puedan afectar la seguridad de la información de la Contraloría, los correctivos necesarios o procedimientos a seguir con el fin de minimizar la posibilidad de ocurrencia de dichos eventos, igualmente la Dirección de Desarrollo Tecnológico debe establecer un procedimiento escrito para estos casos.

9. CONCLUSIÓN

Los riesgos que enfrentan las empresas en el área de TI las obliga a fomentar el trabajo constante de personal especializado en estos temas y dotarlos de las herramientas que permitan detectar y reaccionar ante eventos de seguridad que se materialicen y puedan ocasionar perdida de la información. Riesgos de seguridad de TI que poseen un alto grado de cambio, todos los días se descubren métodos para vulnerar las medidas impuestas por las entidades para proteger la información. Por lo anterior, se vuelve fundamental la protección cibernética enfocada a la prevención.

Es por esto que la necesidad de realizar auditorías de ciberseguridad cada vez es mayor para las empresas. Estudios recientes confirman que un 68% de las organizaciones invertirá mucho más en su ciberseguridad dados los probables ataques que se pueden dar durante esta pandemia.

Globalmente, las conclusiones de esta Auditoría es que existe una garantía razonable de que los controles internos, las políticas y los procesos de gestión de riesgos en materia de lo evaluado en la Entidad funcionan.