Informe de la Auditoría de controles generales al proceso de Gestión de Tecnologías de información

Yadira Velosa
Jose Luis Caycedo
Febrero 24 de 2020

Alcance y Metodología

Evaluar los **controles generales** del proceso de Gestión de Tecnologías de Información, con el fin de verificar la implementación de **buenas practicas** de gestión TIC alineadas a los objetivos estratégicos de la entidad, e **identificar debilidades** de control de los escenarios a evaluar en los criterios de auditoría, mediante la inspección de la **correcta implementación y existencia documentada** y divulgada de las políticas, estándares y procedimientos, para proporcionar confianza de que los objetivos de la función TIC se logren alcanzar con el **uso eficiente de los recursos** disponibles y que los eventos no deseados se prevean, detecten, y corrijan oportunamente.

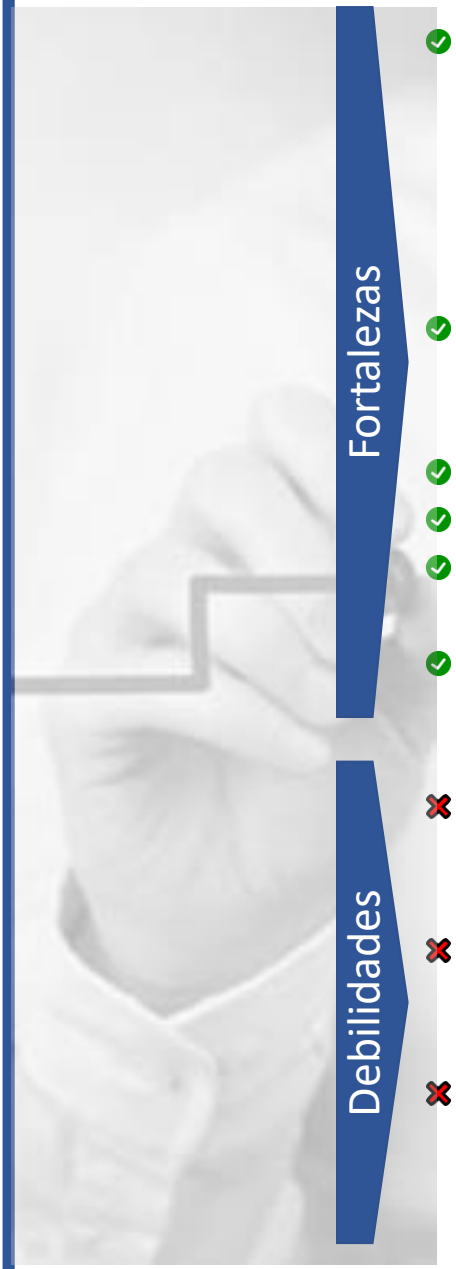
Premisas

- El presente informe corresponde a una auditoría de controles generales de la gestión TIC, no a una auditoría de calidad, por lo tanto se da reconocimiento a los instrumentos construidos por el proceso aunque no sean documentos controlados.
- La auditoria se ejecuta sobre el modelo presente y no sobre el modelo futuro, sin desconocer los elementos de planeación.
- Se presentan observaciones positivas y negativas.
- Para el establecimiento de oportunidades de mejora se usa como referente frameworks de buenas prácticas como COBIT, ITIL, SCRUM y en especial el Manual de Gobierno Digital versión 5 agosto de 2018 – Mintic – DNP.

Metodología Aplicada

- Levantamiento de información mediante **entrevista.**
- **Análisis documental** de políticas, procedimientos, planes y registros asociados a la gestión TIC y a la gestión de seguridad de la información.
- Entrevistas con una muestra de 6 **usuarios finales** de servicios TIC.
- Verificación de controles sobre una muestra de equipos de la red.
- Pruebas básicas de seguridad sobre la red y servicios TIC.

Conclusiones



Fortalezas

- El proceso de Gestión TIC ha estructurado y presentado el Plan Estratégico de Tecnologías de la Información 2019, el cual si bien debe ser optimizado en la vigencia 2020, refleja el **interés** del proceso **por dar cumplimiento a los lineamientos el Marco de Referencia de Arquitectura Empresarial** (MRAE) y de **Gobierno Digital,** para lo cual ha incorporado inversiones orientadas a fortalecer la plataforma tecnológica y vincular contratistas de apoyo para la construcción e implementación de los lineamientos, sin embargo la meta debe ser el Fortalecimiento de la Función TIC **no el cumplimiento documental**.
- Se han implementado algunos **elementos de protección** y gestión de la plataforma tecnológica que si bien deben ser mejorados ofrecen un nivel aceptable de protección de primera capa sobre los activos de información especialmente contra ataques de seguridad perimetral.
- Las herramientas de **backup** a cargo del proceso de Gestión de TI están correctamente configuradas
- La estrategia de alojamiento en nube ofrece la **transferencia efectiva del riesgo de plataforma** a terceros
- Los usuarios de los servicios TIC tienen una **percepción positiva** sobre el servicio de soporte interno, pero manifiestan baja satisfacción con el servicio y la dependencia de conocimiento de terceros de sistemas de información .
- Se destaca el compromiso de la profesional líder del área, quien asume gran parte de las labores operativas, aunque esta situación dificulta su dedicación a actividades estratégicas, de gestión y de revisión detallada de la pertinencia y calidad de los entregables en el marco de la implementación de gobierno digital.

Debilidades

- El proceso de desarrollo de software no cuenta con **metodologías formales de fabrica** que garanticen la atención satisfactoria de los requerimientos del negocio en términos de calidad, alcance, tiempo y costos, además de otorgar a la entidad **conocimiento para la autonomía en el soporte y mantenimiento de los sistemas de información**.
- No se han establecido **procedimientos de gestión de cambios** para activos TIC y sistemas de información, que garanticen equilibrio entre los **recursos invertidos y el valor agregado** a la entidad, además de ser implementados sin **impactos previsibles** y de manera concertada con los interesados.
- Si bien se está adelantado el proceso de identificación y **administración de riesgos** TIC y de seguridad de la información en el marco de implementación del MSPI, este componente debe ser priorizado, ya que no solo ofrece elementos de cumplimiento documental, sino que es la base para determinar la manera de asegurar la plataforma tecnológica y la gestión TIC con controles efectivos y medibles, además de ser la base para la actualización de un **Plan de Continuidad** efectivo

Resultados Resumen

Planeación y Organización

Gestión estratégica → Estructura Organizacional → Administración de Riesgos → Políticas de seguridad

Los procesos y controles se depuran a nivel de buenas prácticas, innovación y el resultado de la medición continua. La plataforma TIC esta asegurada, integrada , es eficiente y se garantiza continuidad. El riesgo esta controlado

Administración de Accesos y Seguridad Lógica

Seguridad de la Red y servicios TIC → Pruebas de seguridad → Gestión de accesos → Seguridad Física

Existen instrumentos de gestión formales y comunicados, que incrementan la posibilidad de detectar fallas. Los activos TIC operan en niveles aceptables

Desarrollo y adquisición de Software Aplicativo

Gestión de desarrollo de software → Gestión de terceros → Administración de requerimientos → Pruebas y Despliegue

Los instrumentos de gestión y control son insuficientes, hay alto grado de dependencia de las personas. La operación es reactiva.

Administración de recursos TIC

Gestión de cambios → Procedimientos e instructivos de operación → Inventarios y mantenimiento de activos TIC → Mesa de Servicio

Los avances no dan cobertura suficiente a la necesidad, los procesos no tienen instrumentos de control formal. La organización esta expuesta a riesgos asociados a las practicas actuales

Resultados por dominio

Planeación y Organización

- Gestión estratégica
- Estructura Organizacional
- Administración de Riesgos
- Políticas de seguridad

Desarrollo y Adquisición de Software Aplicativo

- Gestión de desarrollo de software
- Gestión de terceros
- Administración de requerimientos
- Pruebas y Despliegue

Planeación Estratégica de Tecnología de Información PETI

El PETI debe estar Articulado con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI y su objetivo es garantizar que la planeación de los proyectos y adquisiciones TIC estén alineados con el PEI y que aporten equilibrio entre la inversión TIC y el valor agregado a la entidad mediante el tratamiento de debilidades y amenazas y el aprovechamiento de fortalezas y oportunidades.

Estrategia de TI

Entendimiento interno y externo mediante análisis DOFA y el PEI para la identificación de Proyectos y adquisiciones TIC.

Uso y apropiación

Estrategias para lograr la aceptación, el uso, el entendimiento y la apropiación de la evolución TIC.

Gobierno de TI

Esquema alineado con el MIPG que incluya: Proceso de Gestión de TI, Indicadores de gestión de TI, Instancias de decisión de TI definidas, Roles y responsabilidades de TI y la Estructura organizacional del área de TI.

Gestión de Información

Caracterización detallada de las fuentes de datos y los requisitos de calidad, integración, unicidad y seguridad, junto con los flujos de información interna y externa y el gobierno de los datos.

Servicios Tecnológicos

Establecer la estrategia y procesos de operación y continuidad de la plataforma tecnológica, los servicios de TI y la mesa de servicio.

Sistemas de Información

Caracterización detallada de los sistemas de información para determinar estandarización, integración y escalamiento

Planeación Estratégica de Tecnología de Información PETI

Oportunidades de Mejora Generales

Estrategia de TI

Actualizar el PETI de acuerdo al MRAE y **alinear los proyectos** en términos de planeación, formulación, planes de acción e informes de gestión. **Crear indicadores** confiables y efectivos. Planear con análisis de **esfuerzo**.

Uso y apropiación

En el marco del MSPI diseñar un plan de **gestión del cambio** con base en la evaluación de necesidades. Adelantar un plan de trasferencia de conocimiento (terceros SI, Profesional Líder)

Gobierno de TI

Establecer las directrices para el logro de los objetivos de un Gobierno TI a saber: **inversión** estratégica de TIC, toma de **decisiones centralizada**, gestión integral de **proyectos**, apropiación del **conocimiento** TIC, aplicabilidad efectiva del ciclo PHVA y **sostenibilidad** de la plataforma tecnológica a mediano y largo plazo.

Gestión de Información

Adelantar la caracterización detallada de las fuentes de datos e identificar los requisitos de calidad, integración y unicidad, como base para su aprovechamiento escalable en **inteligencia de negocios**.
Determinar los requisitos de **seguridad** y flujos de información interna y externa. Optimizar el inventario de activos de información.

Servicios Tecnológicos

Adelantar la identificación y tratamiento de los **riesgos TIC conforme al MSPI** y construir, implementar y probar el **Plan de Continuidad** y Recuperación de la entidad.
Diseñar el **modelo de servicio** potenciando la herramienta GLPI.

Sistemas de Información

Documentar en el marco del MSPI la **gestión de cambios** y la administración y control de **proveedores** de sistemas de información para garantizar la estandarización, **integración y escalamiento autónomo**.

Planeación Estratégica de Tecnología de Información PETI

El PETI debe estar Articulado con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI y su objetivo es garantizar que la planeación de los proyectos y adquisiciones TIC estén alineados con el PEI y que aporten equilibrio entre la inversión TIC y el valor agregado a la entidad mediante el tratamiento de debilidades y amenazas y el aprovechamiento de fortalezas y oportunidades.

	Observaciones
Estrategia de TI Entendimiento interno y externo mediante análisis DOFA y el PEI para la identificación de Proyectos y adquisiciones TIC.	El PEI y el PETI no **se encuentra completamente alineados** a través de los lineamientos estratégicos, **los 5 proyectos** declarados **no coinciden** plenamente con la formulación del Plan de Acción, lineamientos de Gobierno Digital y los indicadores de gestión (ciclo PHVA). No se cuenta con los Planes detallados: Plan Estratégico de Tecnologías de la Información PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información, integrados al Plan de Acción Institucional y que incluyan: Proyectos, Metas, Acciones, Productos, Responsables, Cronogramas e indicadores para planeación y medición de la eficacia de su implementación
	A nivel táctico no se aplican **cronogramas** detallados para atender los Planes de Acción, y los tiempos no son calculados con base en un **análisis de esfuerzo** real de las acciones, lo cual puede generar atrasos. Los planes tácticos incorporan los lineamientos de Gobierno Digital.
	En cuanto al seguimiento y control no se encuentran definidos **criterios de aceptación** de entregables como medida para determinar el avance en términos de satisfacción de la necesidad. Aplicables tanto a responsables internos y terceros
Gobierno de TI Esquema alineado con el MIPG que incluya: Proceso de Gestión de TI, Indicadores de gestión de TI, Instancias de decisión de TI definidas, Roles y responsabilidades de TI y la Estructura organizacional del área de TI.	La entidad **no cuenta con una Dirección u Oficina de tecnología de la información y las comunicaciones** como lo establece el Decreto 415 de 2016, cuyo propósito es dejar atrás la concepción de la función tecnológica como soporte y no como habilitador para el desarrollo de las estrategias institucionales y sectoriales. Si bien, el proceso no considera esto un obstáculo, se observa que no esta en operación un gobierno de TI, un líder u Oficial de seguridad de la información (ajeno a sistemas) y la articulación MSPI-SIG
	El proceso **cuenta con un Plan de Adquisiciones anual,** alineado en gran medida con los planes tácticos, pero la gestión de adquisiciones tecnológicas no está articulada a un procedimiento de gestión de cambios que evalúe de manera formal y documentada los impactos de cualquier decisión de inversión, adquisición o modernización tecnológica en la entidad. De igual manera, no hay un procedimiento de gestión de cambios a sistemas de información, para que las adquisiciones garanticen el costo/beneficio y cumplan con criterios de **estandarización, evolución, capacidad de integración, mantenimiento, desempeño, apropiación del conocimiento, riesgo tecnológico, seguridad y sostenibilidad futura**. Se identificaron algunas diferencias entre lo planeado y lo efectivamente adquirido (Compras_2019)
	Se evidencian instrumentos de **seguimiento a los contratos suscritos con terceros** en materia de formalidad contractual y registro de obligaciones para trazabilidad financiera, pero aún no se aplican criterios de aceptación de entregables.
	No se aplican indicadores de gestión TIC y los propuestos en el PETI no están correctamente definidos para ser la base de toma de acciones correctivas sobre la gestión de servicios TIC, no incluye indicadores del MSPI, y no se han establecido las fuentes de información para su calculo.

Planeación Estratégica de Tecnología de Información PETI

	Observaciones
Servicios Tecnológicos Establecer la estrategia y procesos de operación y continuidad de la plataforma tecnológica y la mesa de servicio.	El PETI incluye una **descripción general** de la plataforma tecnológica en cuanto a hardware, software y telecomunicaciones, y hace alusión al documento "*Inventario SisINFO y Aplicativos LBogotá.xlsx*", sin embargo adolece de un diagrama de infraestructura, la caracterización de servicios tecnológicos y perfil de accesos, y análisis proyectivo de su capacidad para satisfacer las necesidades de las áreas.
	El documento **no incluye la estructura de modelo de servicios tecnológicos** y mesa de ayuda con Acuerdos de Niveles de Servicio y articulación de terceros responsables de soporte a servicios TIC. Debe incluirse el inventario de terceros prestadores de servicios TIC.
	No referencia el **Plan de Continuidad** con las estrategias de contingencia y recuperación para cada uno de los servicios tecnológicos. No incluye los avances del año 2019 como resultado de los contratos 63-2018 y 31-2019 para la contingencia de los sistemas en la Nube de Oracle, ni el Manual para la elaboración del Plan de Continuidad del contrato 048, ni la adquisición de la herramienta de monitoreo del 072
Gestión de Información Caracterización detallada de los sistemas de información para determinar estandarización, integración y escalamiento	La entidad ha adelantado acciones para **publicación de datos abiertos y servicios al ciudadano,** y cuenta con un sistema único que soporta los procesos administrativos, financieros y misionales, lo cual disminuye los requisitos de integración.
	En cuanto explotación de la información, **ha adelantado la implementación de Oracle BI**, inicialmente para la unidad de apuestas, pero puede ser extensivo a las demás áreas misionales y de apoyo administrativo y financiero.
	El inventario de activos de información aún no incluye las **fuentes de información** (bases de datos y documentos) identificando cada elemento, proceso al que corresponde, responsable de la información, la caracterización de criticidad (Confidencialidad, Integridad y Disponibilidad), ni el análisis de requisitos de calidad de los datos y seguridad (criptografía y anonimización de datos).
Uso y apropiación Estrategias para lograr la aceptación, el uso, el entendimiento y la apropiación de la evolución TIC	En el contrato 48-2019 se adelantaron algunos **talleres de concientización y sensibilización** en seguridad de la información. La Líder TIC envía regularmente tips de seguridad acerca de los cuales los usuarios entrevistados manifiestan tener recordación, pero no se adelantan análisis de necesidades de conocimiento con base en la mesa de servicio, ni se adelantan encuestas de satisfacción y requisitos.
	El dominio no se encuentra desarrollado incluyendo: estrategia de uso y apropiación de proyectos y servicios de TI a los usuarios de la entidad, estrategias de fortalecimiento de competencias del personal a cargo de la función TIC, planes de gestión del cambio basados en sensibilización, apropiación y la integración del MSPI, control 7.2.2 **Concienciación y capacitación sobre la seguridad de la información.**
Sistemas de Información Caracterización detallada de los sistemas de información para determinar estandarización, integración y escalamiento	El "*Inventario SisINFO y Aplicativos LBogotá.xlsx*", incluye el listado de sistemas de información, pero el PETI no contempla todas las condiciones de adquisición, desarrollo, integración, interoperabilidad, mantenimiento, relación con terceros y requisitos de seguridad. El **inventario de sistemas de información** debe incluir todos aquellos utilizados y autorizados por la entidad, con su debido soporte de licenciamiento y/o propiedad intelectual(propios, de terceros, adquiridos o software libre autorizado). Existen para SIGA y el ERP.

Planeación Estratégica de Tecnología de Información PETI

Recomendaciones

Actualizar el PETI 2020 atendiendo las fases y dominios del MRAE. Optimizar la identificación de proyectos alineados con el PEI y con Gobierno Digital, pero también propios orientados a la mejora y continuidad de la plataforma tecnológica y la gestión TIC.

- Actualizar: Diagrama de infraestructura, catalogo de servicios TIC, inventario de activos (sistemas de información, documentos y categorización), Plan de uso y apropiación, Plan de MSPI, Plan de tratamiento de riesgos, Plan de Continuidad y Modelo de Servicios propios y con terceros.
- Para el dominio de Gestión de información, adelantar el **levantamiento de fuentes y requisitos de explotación de datos** como insumo para el fortalecimiento del componente de BI de Oracle. Identificar la información que debe ser protegida (dominio 10 del MSPI).
- Garantizar la alineación entre PEI, PETI, Planes de Acción, cronogramas, indicadores, Plan de adquisiciones y Plan de Mejoramiento (PHVA)
- Ajustar el documento de Gestión y Gobernabilidad TI, así como el A 6.1.1 Propuestas Funciones Segurinfo Lotería, conforme a los lineamientos de Gobierno Digital y en especial Clausulas 5 y 7 y dominio A6 del MSPI. Asignar las funciones y ubicación organizacional del Oficial de Seguridad.

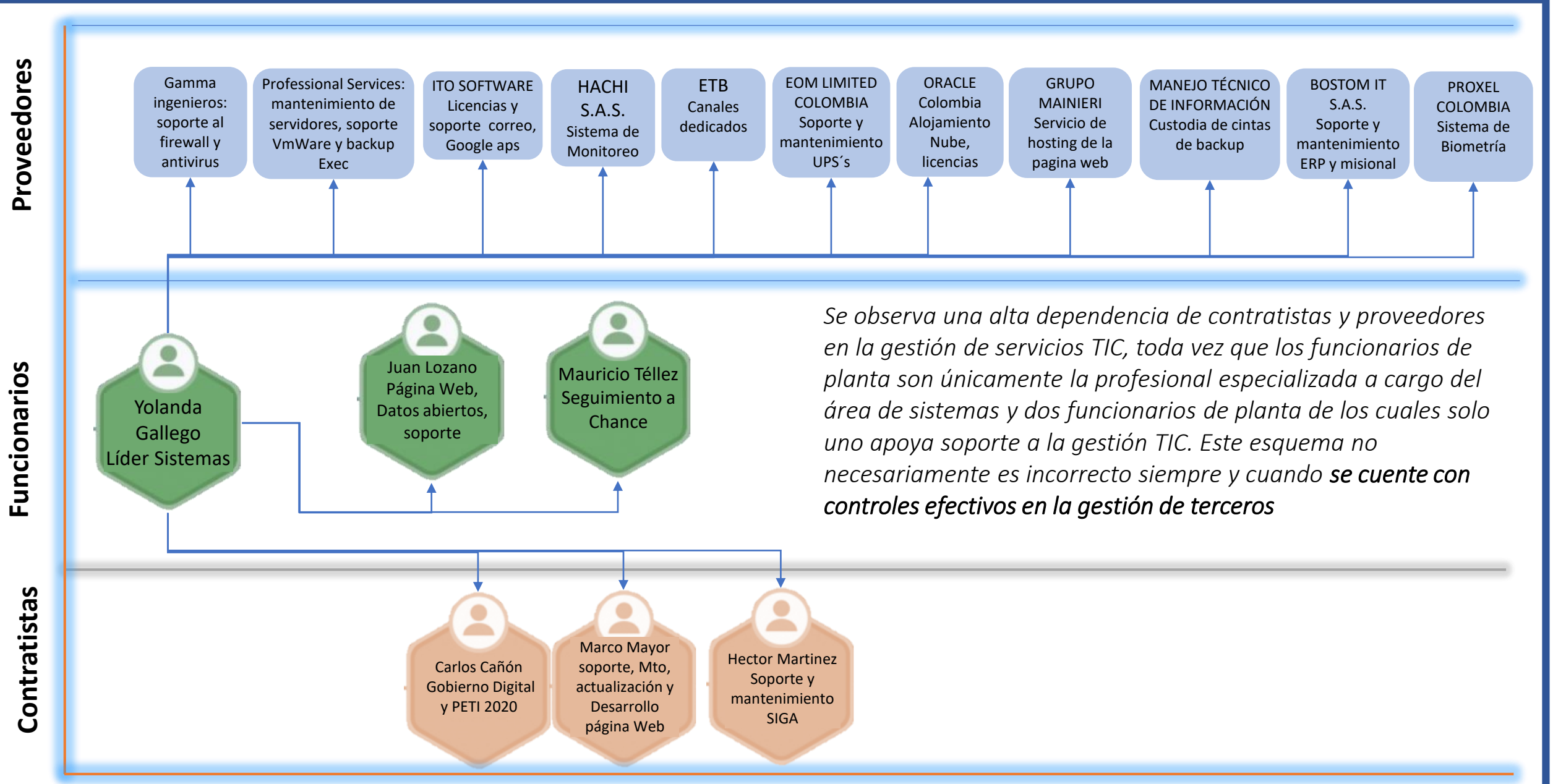
Con relación a los Planes de acción y cronogramas para Control acciones y/o proyectos se recomienda:

- **Establecer las fechas y responsables con base en un análisis de estimación de esfuerzo** vs la capacidad de trabajo instalada, para identificar necesidades de recurso humano, establecer fechas viables de cumplimiento y ponderar las actividades de acuerdo con el esfuerzo requerido.
- Asignar tareas de manera individual con el fin de **medir cumplimiento y productividad por recurso**.
- **Priorizar las tareas** de acuerdo con: requisitos regulatorios, valor misional, valor para la plataforma tecnológica (DOFA), innovación TIC.
- **Establecer criterios de aceptación** de los entregables para garantizar que el resultado obtenido realmente cumple con la mejor práctica.
- **Calcular los avances de acuerdo al nivel de cumplimiento** de los entregables con los criterios establecidos. Si es posible hacer revisión de pares.

Incorporar en el PETI **indicadores de cumplimiento, productividad y calidad en los servicios TIC y proyectos**. Para los **indicadores del MSPI** diseñar indicadores que midan la implementación de los controles, no cumplimiento de actividades. Antes de formular el cálculo de indicadores se recomienda incluir en GLPI, los equipos del dominio y los requerimientos de desarrollo y de soporte **atendido por terceros** y disponer fuentes de datos confiables y suficientes. Usar los resultados como insumo para tomar acciones correctivas oportunas e identificar riesgos
Para el caso de desarrollo de software interno o contratado con terceros **usar el conteo de defectos** en las pruebas y niveles de tolerancia.

Construir el **Plan de Continuidad y recuperación** de la entidad de manera articulada con la gestión de riesgos que se ha decidido tratar mediante aceptación. El plan debe incluir las estrategias de contingencia y de recuperación por cada activo critico y bajo criterios de tiempos máximos de salida de operación de los procesos de la entidad, debe tener responsables y protocolos de pruebas y de actuar. Incluir los avances y el monitoreo en la identificación preventiva de eventos .
Ejecutar las **pruebas integrales al Plan** y documentar los resultados, contemplar los lineamientos de MSI control 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Estructura Organizacional TIC



Se observa una alta dependencia de contratistas y proveedores en la gestión de servicios TIC, toda vez que los funcionarios de planta son únicamente la profesional especializada a cargo del área de sistemas y dos funcionarios de planta de los cuales solo uno apoya soporte a la gestión TIC. Este esquema no necesariamente es incorrecto siempre y cuando ***se cuente con controles efectivos en la gestión de terceros***

Estructura Organizacional TIC – Desarrollo Software

Observaciones

Se destaca la labor del proceso que pese a los pocos recursos ha generado una **percepción favorable entre los usuarios entrevistados**, el compromiso con el mejoramiento de la plataforma y la contratación de apoyo **para atender la implementación de Gobierno Digital**.
Para los proveedores existen controles de confidencialidad, Acuerdos de Niveles de Servicio y **anexos técnicos** que describen las condiciones del objeto contratado. Para herramientas criticas como Firewall y Antivirus se incluyen obligaciones de **trasferencia de conocimiento hacia la Lotería de Bogotá**.
Las compras TIC están centralizadas, y se llevan instrumentos de seguimiento a entregables de los contratos, pero no se aplican criterios de aceptación.

La Lotería de Bogotá cuenta con los registros de derechos de uso del sistema de información SIGA emitidos por la Alcaldia de Bogotá, al igual que con el registro de derechos de autor del sistema Administrativo y Financiero a nombre de la entidad, pero no del componente Misional.

Para los contratistas no se incluyen obligaciones asociadas a **criterios de aceptación** de entregables, gestión documentada de **cambios**, **metodologías** de desarrollo de software, Acuerdos de Niveles de Servicio y **garantía** de producto.

La líder de sistemas tiene a su cargo no solo las actividades de gestión sino también la mayoría de tareas operativas y de administración de los servicios TIC. Esto **limita su disponibilidad** para atender la planeación estratégica, seguimiento e implementación de instrumentos de gestión de los servicios TIC.

No se llevan procesos de **trasferencia de conocimiento** para mitigar el riesgo de afectaciones a la operación por ausencias temporales o permanentes de los recursos actuales. Se observa dependencia de conocimiento, especialmente de la líder y los contratistas de desarrollo de software.

Los contratos que implican desarrollo no incluyen la **cesión de derechos patrimoniales** a favor de la Lotería de Bogotá, ni cláusulas de responsabilidad sobre daños a código fuente y confidencialidad de base de datos, pese a que tienen acceso a los ambientes productivos y control sobre fuentes.

Los desarrolladores tienen copias de las bases de datos en sus equipos personales y hacen **impactos directos en ambientes productivos** sin que exista un documento RFC para dar trazabilidad a los cambios y aportar conocimiento a la Lotería sobre las modificaciones al producto.

Los contratos de desarrollo no exigen la aplicación de una **metodología formal de desarrollo de software ni la entrega de los siguientes tipos de instrumentos** que aportan conocimiento y permiten controlar el equilibrio entre el producto, calidad e inversión realizada (dominio 14 MSPI):

- Formatos de especificación de requerimientos con estimación de esfuerzo y condiciones de auditoría, seguridad, parametrización y diseños gráficos
- Documentación de diseño técnico y arquitectura por capas, Políticas de desarrollo de software y documentación de código.
- Documentación de producto: manuales de usuario, de administración e instalación.
- Entrega del soporte a la mesa de ayuda.

No se obtuvo evidencia de la existencia de documentación técnica del sistema de información Administrativo/financiero/misional (arquitectura, diseño, desarrollo, documentación de código, etc.) que permitan a la entidad apropiarse del conocimiento del sistema frente al riesgo de ausencia temporal o permanente de Luis Davila, quien de acuerdo a las entrevistas con los usuarios finales es la única persona en capacidad de hacer cambios al sistema.

Estructura Organizacional y Desarrollo de Software

Recomendaciones

- Formalizar un Plan de **Transferencia de Conocimiento hacia la Lotería de Bogotá**, que incluya: elaboración de los instructivos y procedimientos, capacitación y rotación de funciones temporal, entre colaboradores principales y de contingencia y entre contratistas y los colaboradores. Evaluar resultados.
- De ser posible, incluir en los contratos, cláusulas que obliguen al contratista a:
  - Realizar un empalme y dar capacitación de sus resultados al finalizar la prestación de servicios.
  - **Criterios de aceptación de entregables**; documentos, servicios y productos y condiciones mínimas de documentación técnica de acuerdo a cada caso: adquisición de software comercial, desarrollo por encargo a terceros o desarrollo interno.
  - **Cesiones de derechos patrimoniales** a favor de la entidad para el caso de desarrollos de software.
  - Especificaciones de la **documentación técnica mínima** a entregar en desarrollo de software y la metodología que debe ser aplicada.
  - Obligaciones de **seguridad de la información** en desarrollo de software para protección del código fuente contra hurtos y ataques informáticos.
  - Condiciones de **soporte sobre el producto y ANS** durante la vigencia del contrato.
  - Condiciones de **garantía** sobre el producto al finalizar el contrato y por un termino de entre 6 y 12 meses.
- Exigir a los contratistas de desarrollo de software entrega de los documentos de arquitectura, diseño, desarrollo y despliegue, con criterios de aceptación que permitan a la entidad autonomía en mantenimiento y soporte. SI APLICA. Solicitar el registro en derechos de autor del componente misional del ERP.
- Adoptar una **metodología para la adquisición y desarrollo** de sistemas de información que incluya como mínimo los siguientes instrumentos de control;
  - Documentos de **requisitos de la adquisición RFP**, formatos de **especificación** de requerimientos para desarrollos internos y contratados con terceros, Procedimientos de protocolo de **pruebas** (**funcionales y técnicas**) y gestión de **defectos** y Procedimientos de aceptación y **despliegue** en ambientes.

  En ningún caso los desarrolladores deben hacer despliegues autónomos a ambientes productivos, esta tareas debe estar **a cargo de sistemas con RFC.**
- En el marco de implementación MSPI adelantar el procedimiento de **gestión de cambios** que permita llevar trazabilidad y control sobre los cambios impactados a la plataforma tecnológica y por los desarrolladores. Incluir registros de cambios y medias de seguridad para mitigar las fallas en uso productivo
- En el marco del proyecto de implementación de la **mesa de ayuda incluir los requerimientos de desarrollo** como una tipología de solicitud, registrar las especificaciones, asignar responsable y usar la funcionalidad de documentos anexos para llevar la base documental de cada desarrollo. En el marco del contrato 65 de 2019, solicitar al contratista la documentación, implementación en GLPI y capacitación a usuarios de un Modelo de servicio integral que incluya servicios internos y con terceros.
- Fortalecer el conocimiento en los criterios de calidad de los instrumentos de implementación de Gobierno Digital, con el fin de que las contrataciones de apoyo a su implementación no se limiten a documentos y realmente aporten valor a la entidad en fortalecimiento de la gestión TIC y la gestión de riesgos

Riesgos y Contingencias

Observaciones

La entidad ha publicado la Política de administración del riesgo **(Pol_Administracion_Riesgo_2019.pdf),** y el formato de registro "**Matriz de Riesgo 2019.xls**", que otorgan los lineamientos para la administración de riesgos en identificación, análisis, valoración, monitoreo y seguimiento. Contemplan los riesgos tecnológicos, pero no su relación directa con el nivel de criticidad de los activos de información y la condiciones especiales para su tratamiento en términos de Planes de contingencia, recuperación y continuidad, como lo establecen los lineamientos del MSPI en articulación con el MIPG

El documento Metodología Gestión Riesgo Segurinfo LBOG.docx, incluye un **modelo de valoración** que no coincide por lo establecido en la Política de Administración de riesgo de la entidad, y referencia al documento "Tratamiento del Riesgo Lotería de Bogota.xlsx", que si bien identifica 33 riesgos de seguridad de la información relacionados con los controles ISO27001:2013, no establece acciones y no cumple con el **formato** establecido por la entidad.

En el contrato 48-2019, se entrego el documento "Manual de Continuidad del Negocio Final.docx", el cual incluye la temática de riesgos, pero **no coincide** con el documento Metodología Gestión Riesgo Segurinfo LBOG.docx en cuanto a: identificación de amenazas, identificación de vulnerabilidades y el modelo de valoración del riesgo y controles, además no hace **referencia a los Planes de Continuidad**, por materialización en activos críticos.

Aunque no hay un plan de continuidad y recuperación documentado, formalizado, implementado y probado, el proceso de gestión TIC ha adelantado las siguientes acciones: ambiente contingente en la Nube de Oracle para sistema ERP/Misional, pruebas de continuidad del ambiente, instructivo para contingencia en nube (FormatoDocumentacion-DRP-LoteriaBogota.pdf), manual para construir el Plan, solución de monitoreo de la infraestructura tecnológica (contrato 72-2019), canales contingentes y UPS. La implementación de **alojamientos en nube es favorable** al trasladar el riesgo a terceros.

Se cuenta con la herramienta **Veritas Backup Exec**, correctamente configurada y programados los trabajos que generan los backup para la NAS, máquinas virtuales, directorio activo y bases de datos con RMAN de Oracle. Se lleva control de las cintas magnéticas para almacenamiento externo amparado por contrato. **Faltan backup de** servidores físicos, de las configuraciones de switches, Access Point y NAS, en caso de daños se tendría que volver a configurar y pruebas de contingencia por **falla en directorio activo**.

Si bien el procedimiento PRO202-211-8 GESTION_BACKUP.pdf se llevan de manera correcta, aún no se encuentra debidamente desarrollados los **procedimiento y formatos** del dominio 12.3 del MSPI para la planeación, registro de novedades y pruebas de restauración.

El proceso de Gestión TIC solo ha incluido **dos riesgos** que son **insuficientes** para dar cobertura a las diferentes amenazas en materia de tecnología y seguridad de la información, no esta alineado a MSPI y las acciones no incluyen la implementación de los controles y la verificación de su eficacia, pese a que el presupuesto 2020 contempla el rubro: "SGSI, ANALISIS DE VULNERABILIDADES, IPV6".

No se lleva un control documental de las evidencias de los avances en las **acciones de tratamiento de los riesgos** y actualización del riesgo remanente luego de la implementación de controles. Esto no desconoce las acciones adelantadas tal como los ambientes de prueba para el sistema ERP/Misional

Pese a la alta dependencia de terceros y a las observaciones presentadas en el informe, no se han incluido **riesgos relacionados con terceros** y proveedores en desarrollo del dominio 15 del MSPI.

Riesgos y Contingencias

Recomendaciones

- En la implementación del MSPI **unificar la Metodología de administración de riesgo** para todo el sistema integrado de gestión, agregando o anexando lo que corresponda a la identificación y tratamiento de riesgos TIC alineado con los activos de información de la entidad y los Planes de Continuidad. Corregir las inconsistencias de los documentos del contrato 048 antes de su formalización.
- Se recomienda adelantar el ejercicio de identificación de **riesgos de seguridad de la información orientado a activos críticos** que en caso de materialización de amenazas afectan la continuidad de la operación y/o la disponibilidad, integridad y resguardo de la información.
  Tener en cuenta que los riesgos deben contemplar también los diferentes aspectos de la gestión TIC para garantizar que los controles de la norma han sido incorporados en los riesgos. Tal es el caso de los riesgos relacionados con la relación con terceros y dependencia de conocimiento que no necesariamente se originan en activos tecnológicos, sino en debilidades contractuales o de control.
- En el marco de la implementación del MSPI depurar las acciones y controles de acuerdo con las configuraciones de dichos controles en la plataforma TIC. Incluir evidencia de la implementación y **eficacia de los controles**.
- Adelantar los documentos de procedimientos de copias de respaldo por cada tipo de activo objeto de backup.
  Incluir en la documentación del proceso registros de **Planeación de copias de respaldo, de novedades de procesos y de restauraciones** aleatorias en cumplimiento del objetivo de control 12.3 del MSPI, de igual manera garantizar que los instructivos por herramienta y ambiente sean suficientemente claros para ser guía de operación en ausencia del responsable actual. Reforzar la **capacitación** a los usuarios sobre las políticas de Backup.
- Construir el **Plan de Continuidad** y recuperación incluyendo las estrategias de contingencia y de recuperación por **cada activo servicio crítico** y bajo criterios de tiempos máximos de salida de operación de los procesos de la entidad. Debe tener **responsables y protocolos** de pruebas y de actuar.
  Una vez adelantado el Plan de Continuidad, ejecutar las pruebas integrales al Plan y documentar los resultados
- Incluir en la programación de copias de respaldo el Backup de las bases de datos y las imágenes de los servidores físicos, y de las configuraciones de los elementos activos de red como NAS, Access Point, firewall y switches
- Llevar control de las novedades de los procesos, especialmente sobre los **fallidos o alertados**. Incluir acciones correctivas en los procedimientos.

Políticas de Seguridad – Implementación MSPI

Observaciones

La entidad cuenta con una **política general de seguridad de la información,** publicada con la Resolución 022 del 24 de febrero de 2011, que si bien requiere actualizaciones al MSPI, resulta más completa que el documento "A 5 POLÍTICAS.docx" del contrato 48-2019. La resolución hace referencia a la creación del "Comité de sistemas de seguridad de la información" mediante resolución de Gerencia 31 de 19-2-2009, pero no se celebra periódicamente.

El documento "A 5 POLÍTICAS.docx" se acompaña de algunos documentos que si bien declaran la política general por dominio del MSPI, adolecen de los procedimientos, formatos e instructivos necesarios para dar aplicabilidad e implementar los controles de la norma, ya que estos son los instrumentos tanto para la implementación tecnológica de los controles como para su articulación con el Sistema de Gestión Integral.

Se evidencia avance en los procesos de **sensibilización al usuario final** en materia de seguridad de la información. Los usuarios entrevistados manifiestan haber recibido una charla al respecto, y tienen recordación de tips por correo, pero no tienen claridad en las políticas ni su publicación.

Se ha logrado un avance en el levantamiento manual y no en GLPI, de **activos de información de hardware y software**, lo cual genera carga operativa. El inventario no incluye conjuntos de datos y archivos confidencial en tránsito interno y con terceros, ni la **clasificación** de seguridad de la información y la categorización de **criticidad** para la operación, lo que es la base para gestión de riesgos e identificación de activos para el Plan de Continuidad.

El contrato 65-2019, no precisa los entregables puntuales para las políticas, con el riesgo de **obtener documentos generales** como en el contrato 048-2019 y no la totalidad requerida para Gobierno Digital y en particular el MSPI. Incluye el inventario de activos tipo hardware y software sin archivos.

No se ha adelantado la Herramienta de Diagnostico de Seguridad y Privacidad de la Información de Mintic, y **no se cuenta con una declaración de aplicabilidad**, que relacione para cada control los documentos que deben construirse para dar cumplimiento a la aplicabilidad de la entidad. No se han levantado las matrices de funciones Vs perfiles de acceso a los servicios TIC como insumo para la implementación de la gestión de accesos del dominio 9 del MSPI

No se ha adelantado el levantamiento de **documentos comunes del SIG con el MSPI**, para garantizar que se evoluciona hacia un Sistema Integrado de Gestión que contempla los lineamientos, políticas, procedimientos, formatos e instructivos comunes entre ISO9001:2015 y MSPI con base en ISO 27001:2013. Este levantamiento es insumo para elaborar la declaración de aplicabilidad y determinar que documentos comunes deben ser ajustados.

Las políticas declaradas en los documentos, aún **no se reflejan completamente en la plataforma tecnológica**, en las inspecciones de seguridad realizadas por el auditor se identificaron debilidades de seguridad que deben ser subsanadas en el desarrollo del MSPI.

Se observa que no se ha adelantado una **estimación de esfuerzo** para determinar si un solo recurso es suficiente para la implementación documental y tecnológica del **MSPI** en los plazos establecidos. De igual manera no se ha definido la posición del Oficial de Seguridad a futuro en la estructura organizacional, ya que una vez implementado el sistema, el oficial asume labores de inspección, seguimiento y auditoría, por lo tanto, debe tener carácter independente y objetivo con respecto a la Función TIC.

Políticas de Seguridad – Implementación MSPI

Recomendaciones

✓ Continuar la implementación del modelo MSPI en 4 frentes paralelos:

- Levantamiento y planeación de los documentos **comunes** en el sistema integrado de gestión y la planeación de la salida escalonada de documentos de acuerdo al avance en implementación.
- La elaboración del marco documental de políticas, procedimientos, instructivos y formatos en la **declaración de aplicabilidad**. Tener en cuenta que la implementación de los dominios no se realiza por orden de la norma, sino de acuerdo a los esfuerzos de su implementación, sensibilización y puesta en operación real. Vale aclarar que la declaración de aplicabilidad debe incluir claramente las justificaciones y soportes para la exclusión de controles.
- Un programa de programa de concientización, educación y **capacitación** sobre la seguridad de la información (control 7.2.2 ISO 27002:2013). Junto a un plan de gestión del cambio asociado a las restricciones de las políticas y los nuevos procedimientos.
- **Implementación** de los controles de seguridad de la información en la plataforma TIC de manera incremental.

Se recomienda adelantar una inspección de **análisis de vulnerabilidades** antes de la planeación para determinar criticidad y prioridad y nuevamente una vez finalizada la implementación para verificar su eficacia.

Es importante garantizar que los documentos de Gobierno Digital y MSPI tiene **articulación entre ellos** y que los instrumentos de registro y control se basen en lo posible en herramientas automáticas y no en formatos de Excel que generen mayor carga operativa

✓ Adelantar un **análisis de esfuerzo** de la implementación documental y técnica del MSPI para determinar si se requiere mayor apoyo.

Definir el **rol y ubicación organizacional del Oficial de Seguridad** de la Información una vez implementado el Modelo.

✓ Complementar el inventario de sistemas de información incluyendo **todos los sistemas en uso** estén o no alojados en la plataforma de la entidad, incluir igualmente sistemas autorizados de uso libre. Incluir en el inventario el soporte de la legalidad de uso del sistema de información. Estos elementos son insumo para el inventario de activos y para el desarrollo del dominio 18 del MSPI **Cumplimiento**

✓ Una vez implementada la **herramienta GLPI, generar los listados de activos** de información enlazados a dominio y articular estos resultados con el inventario de activos de información tipo hardware, software y comunicaciones. Iniciar la identificación de los activos tipo información, esto es datos e información en medios físicos o electrónicos. Determinar la caracterización de confidencialidad y de criticidad y requisitos de criptografía y anonimización.

✓ Levantar las matrices de **funciones Vs perfiles** de acceso a los servicios TIC como insumo para la implementación de la gestión de accesos del dominio 9 del MSPI

Resultados por dominio

Administración de Accesos, Seguridad Lógica y Física

Administración de Accesos y Seguridad Lógica

Seguridad de la Red y servicios TIC → Pruebas de seguridad → Gestión de accesos → Seguridad Física

Administración de Accesos, Seguridad Lógica y Física

Observaciones Elementos de Protección de Red:

Se cuenta con elementos **adecuados de protección de red** que garantizan una correcta seguridad perimetral: Firewalls y protección de antivirus en los equipo de usuario, los Access Point para el acceso a través de la red inalámbrica están correctamente configurados.

Se tienen correctamente configuradas en el **firewall** las interfaces, DMZ' para Gelsa, objetos y rutas de red, también están configuradas reglas, control de aplicaciones, filtros de contenido de Internet y controles de navegación por grupos de usuarios,

Se tienen configuradas correctamente **VPN's** para accesos remotos con sus respectivos controles a usuarios, el control de uso del ancho de banda, detección y bloqueo de amenazas externas. La red inalámbrica se encuentra correctamente aislada de la red local (LAN).

No se cuenta con un **diagrama de red** completo que permita visualizar todos los componentes que conforman la red y cómo interactúan, incluidos enrutadores, dispositivos, switches, firewalls, etc. Debe incluirse en el PETI dominio de servicios tecnológicos.

La configuración de la de **red de área local** (LAN) no es correcta, ya que permite realizar escaneos y descubrimientos de todos los elementos y equipos de la infraestructura TIC de la Lotería de Bogotá, incluyendo servidores, impresoras, unidades de almacenamiento en red, etc.

El firewall y el antivirus **no se sincronizan**, por lo cual no es posible detectar ataques internos a la red, y por ende no se bloquean herramientas de Hacking (captura de paquetes, contraseñas, detección de recursos sin protección, etc.) que se pudieran ejecutar en cualquier equipo conectado a la red, ya sea de funcionarios o de terceros. Tampoco se tiene configurado el sistema de **alertas por correo**.

La configuración de red y la asignación automática de direcciones de red (DHCP) **no restringen la conexión al dominio a direcciones no conocidas** de tarjetas de red y no se cuenta con protección o separación sobre la información de las direcciones IP's de puertas de enlace, servidores DHCP y DNS

No se están ejecutando las **acciones correctivas reportadas por la herramienta de auditoria** de seguridad de fabrica del firewall, las cuales están enfocadas a mantener la configuración del firewall con los estándares de seguridad adecuado y a reportar errores en la configuración implementada. Tampoco se han aplicado las **actualizaciones del firmware**, importantes para incluir nuevas características de protección y mejoras en la seguridad.

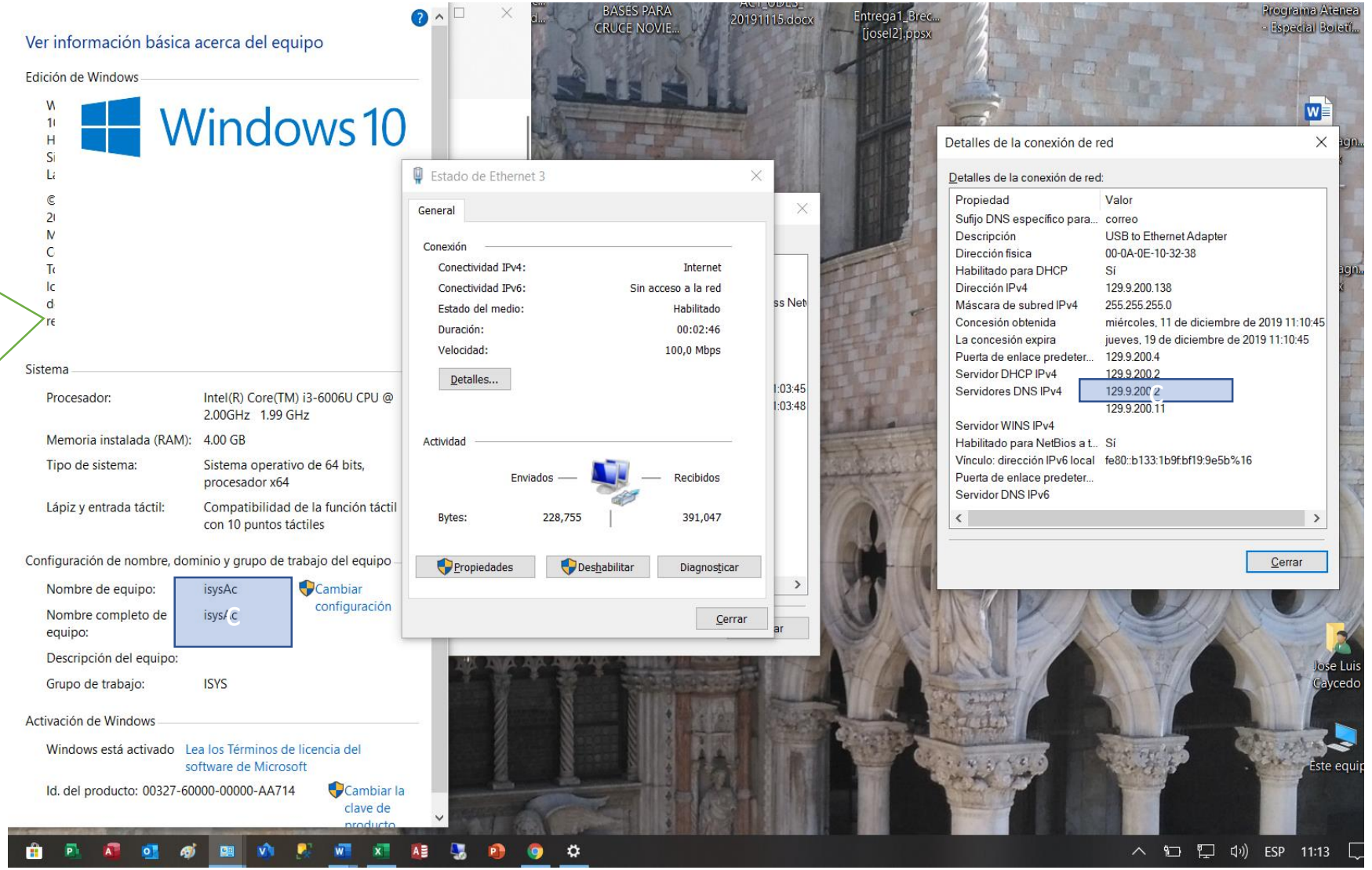
No existen **procedimientos formales para el monitoreo**, ni indicadores definidos y/o seguimientos acciones de mejora que se deban implementar basados en los informes de control generados en las consolas del firewall y antivirus. Ni tampoco procedimientos para el cambio periódico de contraseñas de administrador de dispositivos de red como impresoras, escáneres, unidades de Almacenamiento en red, etc.

La configuración del cliente de antivirus y firewall, permite la descarga y ejecución de herramientas de **captura de contraseñas**, escaneo de red y otros utilizados para generar ataques, considerados como software peligroso.

Se evidencia el uso de aplicaciones de **alto riesgo** que se permiten y/o se bloquean por grupos y están relacionadas con almacenamiento y accesos remotos (AnyDesk, TeamViewer, Remote Desktop, WeTransfer, etc.), algunas sin licencia de uso y de intentos de acceso a sitios reconocidos como propagadores de Virus.

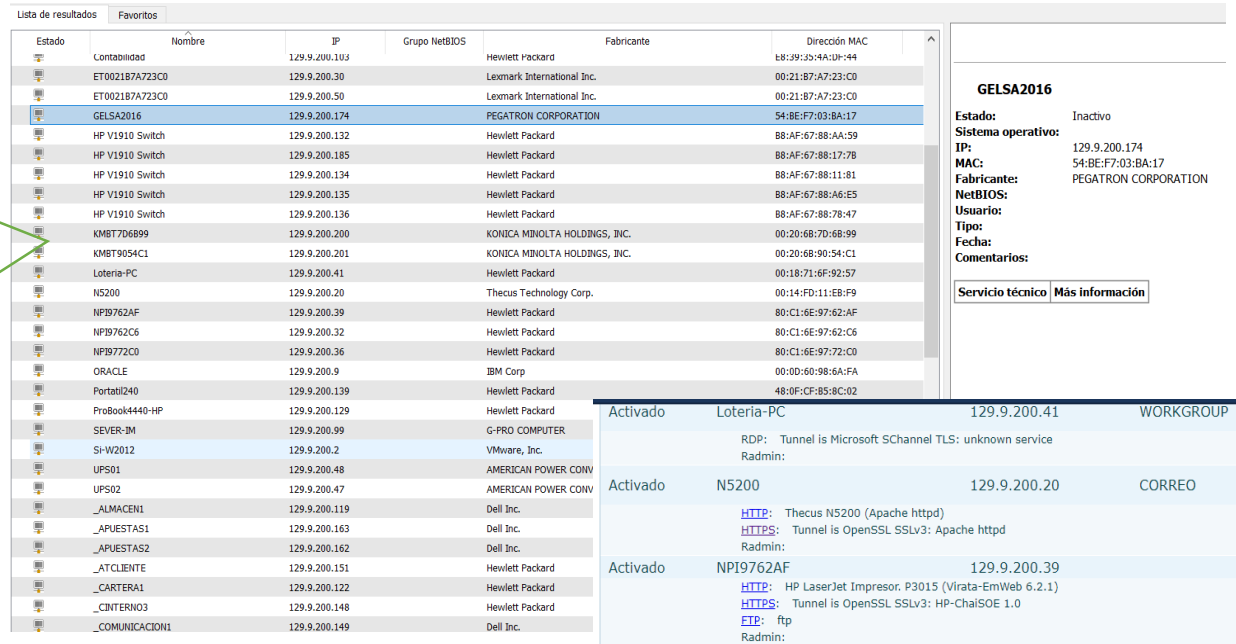
Administración de Accesos, Seguridad Lógica y Física

Al conectar el equipo del auditor con un cable propio a la red LAN, le asigna automáticamente una dirección dentro del rango de los equipos y servidores de la Lotería de Bogotá. Lo que permite descubrir hacia donde dirigir un posible ataque.



Administración de Accesos, Seguridad Lógica y Física

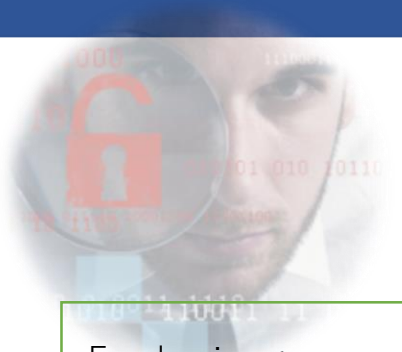
Permite realizar escaneos de red para obtener los datos de los equipos y elementos conectados, sus direcciones y características.



Permite ejecutar procesos para identificar los servicios y puertos que tienen disponibles los equipos en la red, obteniendo información para conectarse a servicios y aprovechar los puertos de manera no autorizada.

Activado	Loteria-PC	129.9.200.41	WORKGROUP	Hewlett Packard	00:18:71:6F:92:57	2019-12-11 14:37:45 UTC-05:00
	RDP: Tunnel is Microsoft SChannel TLS: unknown service Radmin:					
Activado	N5200	129.9.200.20	CORREO	Thecus Technology Corp.	00:14:FD:11:EB:F9	2019-12-11 14:30:38 UTC-05:00
	HTTP: Thecus N5200 (Apache httpd) HTTPS: Tunnel is OpenSSL SSLv3: Apache httpd Radmin:					
Activado	NPI9762AF	129.9.200.39		Hewlett Packard	80:C1:6E:97:62:AF	
	HTTP: HP LaserJet Impresor. P3015 (Virata-EmWeb 6.2.1) HTTPS: Tunnel is OpenSSL SSLv3: HP-ChaiSOE 1.0 FTP: ftp Radmin:					
Activado	NPI9762C6	129.9.200.32		Hewlett Packard	80:C1:6E:97:62:C6	
	HTTP: Virata-EmWeb 6.2.1 HTTPS: Tunnel is OpenSSL SSLv3: HP-ChaiSOE 1.0 FTP: ftp Radmin:					
Activado	NPI9772C0	129.9.200.36		Hewlett Packard	80:C1:6E:97:72:C0	
	HTTP: HP LaserJet Impresor. P3015 (Virata-EmWeb 6.2.1) HTTPS: Tunnel is OpenSSL SSLv3: HP-ChaiSOE 1.0 FTP: ftp Radmin:					
Activado	ORACLE	129.9.200.9	CORREO	IBM Corp	00:0D:60:98:6A:FA	2019-12-11 13:05:16 UTC-05:00
	HTTP: 401 Unauthorized (Oracle XDB httpd 9.2.0.6.0 - 64bit Production) Radmin:					
Inactivo	Portatil240	129.9.200.139		Hewlett Packard	48:0F:CF:B5:8C:02	
	Radmin:					
Activado	ProBook4440-HP	129.9.200.129	WORKGROUP	Hewlett Packard	B4:B5:2F:73:A3:B8	2019-12-11 14:30:11 UTC-05:00
	Radmin:					
Activado	SEVER-IM	129.9.200.99	CORREO	G-PRO COMPUTER	00:0F:FE:C0:A2:C5	2019-12-11 14:32:06 UTC-05:00
	HTTP: Access forbidden! (Apache httpd 2.2.14) HTTPS: Tunnel is OpenSSL SSLv3: Apache httpd 2.2.14 FTP: ? RDP: Tunnel is Microsoft SChannel TLS: unknown service Radmin:					
Activado	Si-W2012	129.9.200.2	CORREO	VMware, Inc.	00:50:56:A7:50:D3	2019-12-11 14:33:03 UTC-05:00
	HTTP: 403 - Prohibido: acceso denegado. (Microsoft IIS httpd 8.0) RDP: Tunnel is Microsoft SChannel TLS: unknown service					

Administración de Accesos, Seguridad Lógica y Física



En la imagen se muestran los intentos de navegación en sitios altamente peligrosos por ser propagadores de virus. Estos casos deben ser investigados debido a que pueden ser ya virus en dispositivos que hacen intentos de ingreso a los sitios.

Top Websites by Bandwidth

Website	Traffic Out	Traffic In
skype.com		5.3 MB
googlezip.net		443.1 KB
cdn.push.house		34.8 KB
xvideos-cdn.com		34.8 KB
eporner.com		26.5 KB
downloadastro.com		24.2 KB
kompoz.me		23.2 KB
youtrannytube.com		19.2 KB
fuckandcdn.com		15.7 KB
imperiodefamosas.com		15.0 KB

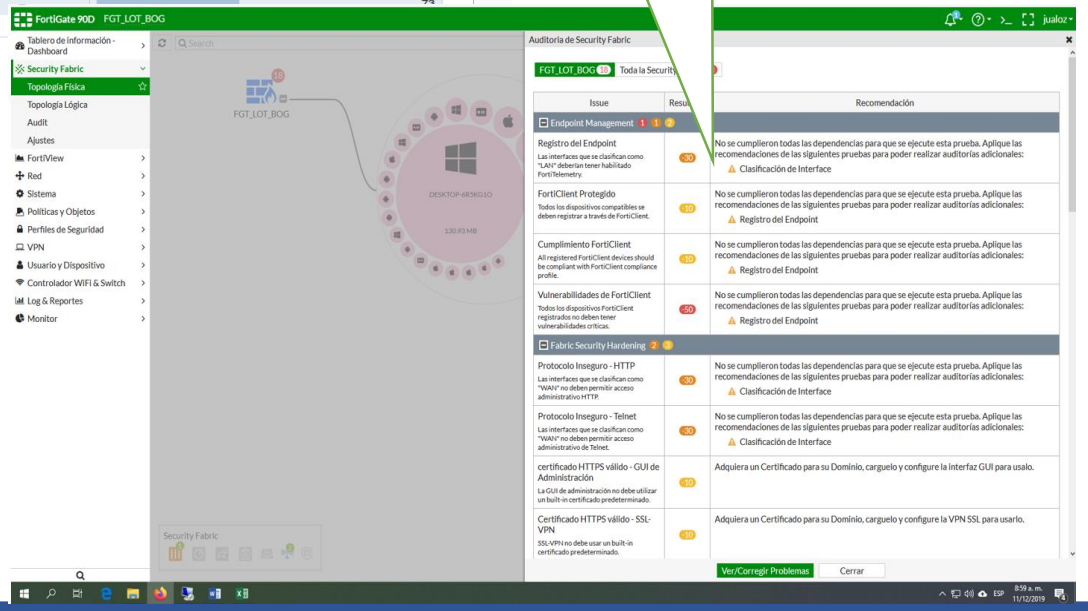
Top Blocked Websites

Website	Requests
skype.com	1.0 K
googlezip.net	140
eporner.com	9
xvideos-cdn.com	9
cdn.push.house	6
kompoz.me	6
fuckandcdn.com	4
imperiodefamosas.com	4
downloadastro.com	3
sheshaft.com	3

Top Users by Blocked Requests

User(or IP)	Hostname(MAC)	Requests
MAUTEL	129.9.200.90	155
192.168.9.11	20:32:6c:6f:99:44	111
YOLGAL	129.9.200.157	103
192.168.9.6	Android	73
ANDPIN	129.9.200.140	

Se encontraron 18 alarmas de auditoria de seguridad de Fabrica del firewall, sin atender.



LOSVIRUS

NOTICIAS | VIRUS | SOFTWARE | ARCHIVOS | PREGUNTA

ADWARE | RANSOMWARE | HACKER DE NAVEGADOR | VIRUS DE MAC | TROYANOS

¿Has visitado páginas porno? ¡Estás infectado! (El top de los sitios más peligrosos)

por Olivia Morelli - 2015-11-16

- *xvideos*. ¿Ver vídeos sexy es tu mejor modo de entretenimiento? Cuidado con el dominio xvideos, el cual ha estado infectando a sus visitantes con ransomware. De acuerdo con ellos, han sido engañados y han descargado esta amenaza en sus ordenadores tras hacer click en alguna publicidad desleal que promueven un sexy chat llamado Sex Messenger. De hecho, es el mismo messenger del que hablamos en Hamster.

Administración de Accesos, Seguridad Lógica y Física

Observaciones Pruebas de Seguridad Internas y Externas:

Se tiene como protección de **antivirus** el Kaspersky Security Center en el servidor de antivirus y Kaspersky Endpoint Security con licencia para 60 equipos de cómputo de la Lotería de Bogotá.

Se **controlan las instalaciones y desinstalaciones** de software por usuario administrador, se encuentran configuradas las directivas de contraseña en el directorio activo y especificados los permisos para compartir recursos en red, además del bloqueo por inactividad.

Al conectarse a la **WIFI** de la Lotería de Bogotá **no es posible obtener** información de las direcciones IP del servidor DHCP, DNS y WINS. Esta ofrece la protección necesaria para evitar ataques desde la red inalámbrica hacia equipos de funcionarios y/o servidores.

Se evidencio la posibilidad de **descargar aplicativos** gratuitos en versión **portable** (no requiere instalación),para escaneo de red identificación de objetivos, captura de contraseñas y análisis de vulnerabilidades, los cuales en su versión portable fueron utilizados por el auditor para encontrar, capturar contraseñas e identificar todos los equipos y puertos expuesto en la red local de la Lotería de Bogotá.

Se pueden **conectar equipos personales** a puntos de red sin restricciones, esto permitió al auditor ejecutar herramientas de **hacking** desde su equipo para planificar ataques.

En los escaneos realizados se encontraron elementos de red como impresoras, carpetas compartidas **sin protección adecuada** de contraseñas y con contraseñas por defecto para el usuario administrador, lo que permite realizar cambios sobre permisos de usuarios o cambiar configuraciones para obtener información de los archivos de usuario y o de los documentos que se escanean o imprimen en los equipos en red pertenecientes a la Lotería de Bogota.

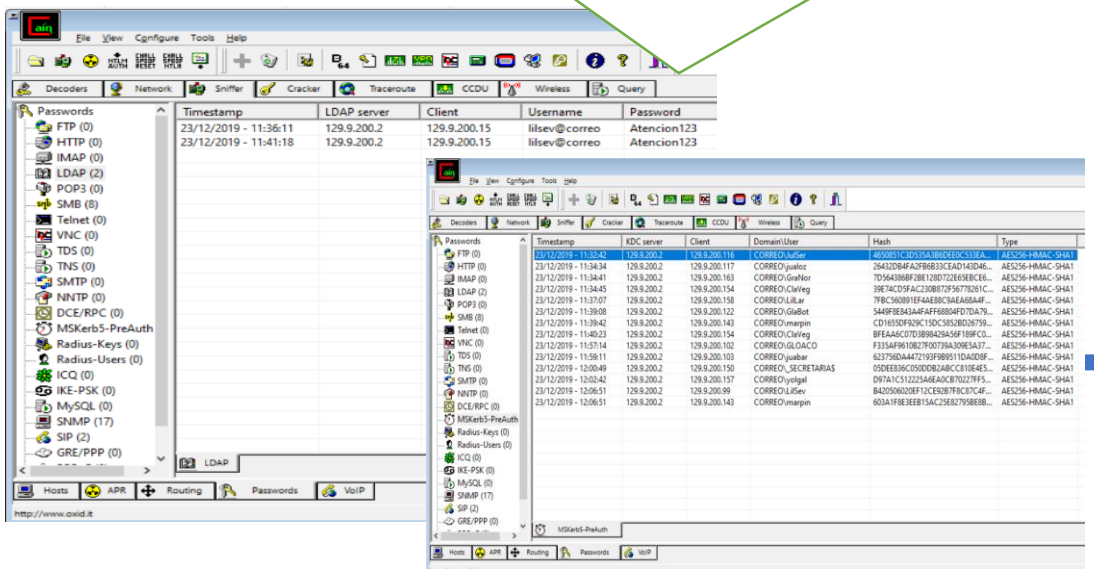
El auditor logro ejecutar desde su equipo el software Cain (sniffer) usado por los **hackers para descifrar y capturar todo el tráfico** de red, incluyendo usuarios y contraseñas de los servicios de red y sistemas de información. En la ejecución de uno de estos ataques se capturo la actividad en toda la red durante 10 minutos, obteniendo contraseñas de usuario sin cifrado, con las cuales el auditor logro conectarse remotamente a algunos equipos y servidores **suplantando a usuarios** de funcionarios de la Lotería de Bogotá.

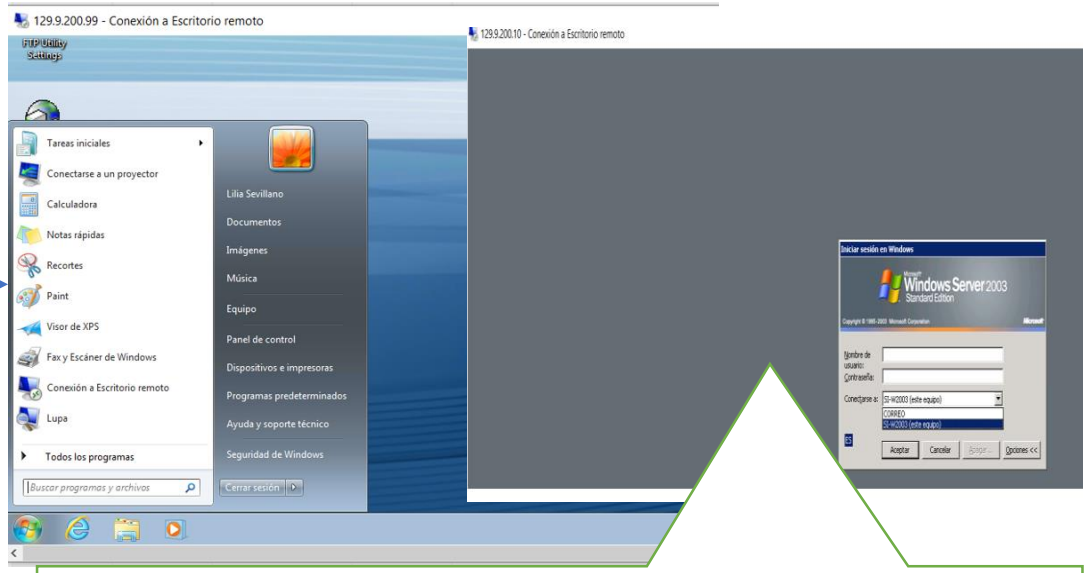
La subred sobre la cual están los teléfonos IP de la Lotería de Bogotá también permite escaneos. Al ejecutarlos se encontró que en todos los teléfonos, el ingreso a la pagina de configuración tiene la contraseña de fabrica por defecto *Admin* y por ende pueden ser manipulados para realizar posibles capturas de llamadas y obtener información.

En la pruebas externas realizadas al portal web (https://loteriadebogota.com) se encontró una vulnerabilidad de riesgo medio: *Cookies http* a la falta del indicador *HttpOnly* que permite al navegador acceder a la cookie desde los scripts del lado del cliente. Además de tres vulnerabilidades de riesgo bajo. Lo que puede ser usado para capturar información para obtener acceso autorizado a una sesión web de un usuario.

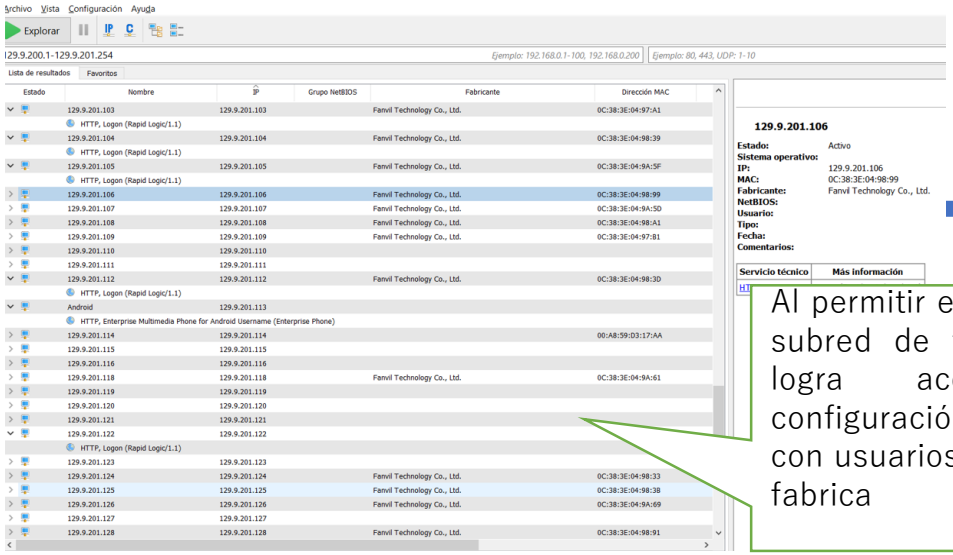
Administración de Accesos, Seguridad Lógica y Física

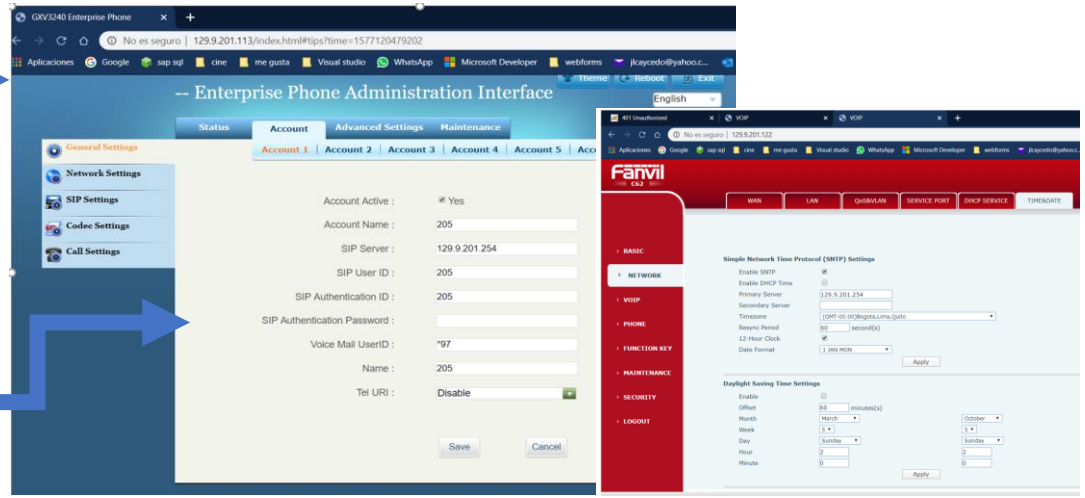
El firewall no bloquea la ejecución de software de captura de paquetes de red (sniffers). El auditor logro capturar usuarios y contraseñas desde su equipo con esta herramienta.





Con la información capturada ingresa desde su equipo a servidores con el acceso remoto habilitado, identificados en los escaneos



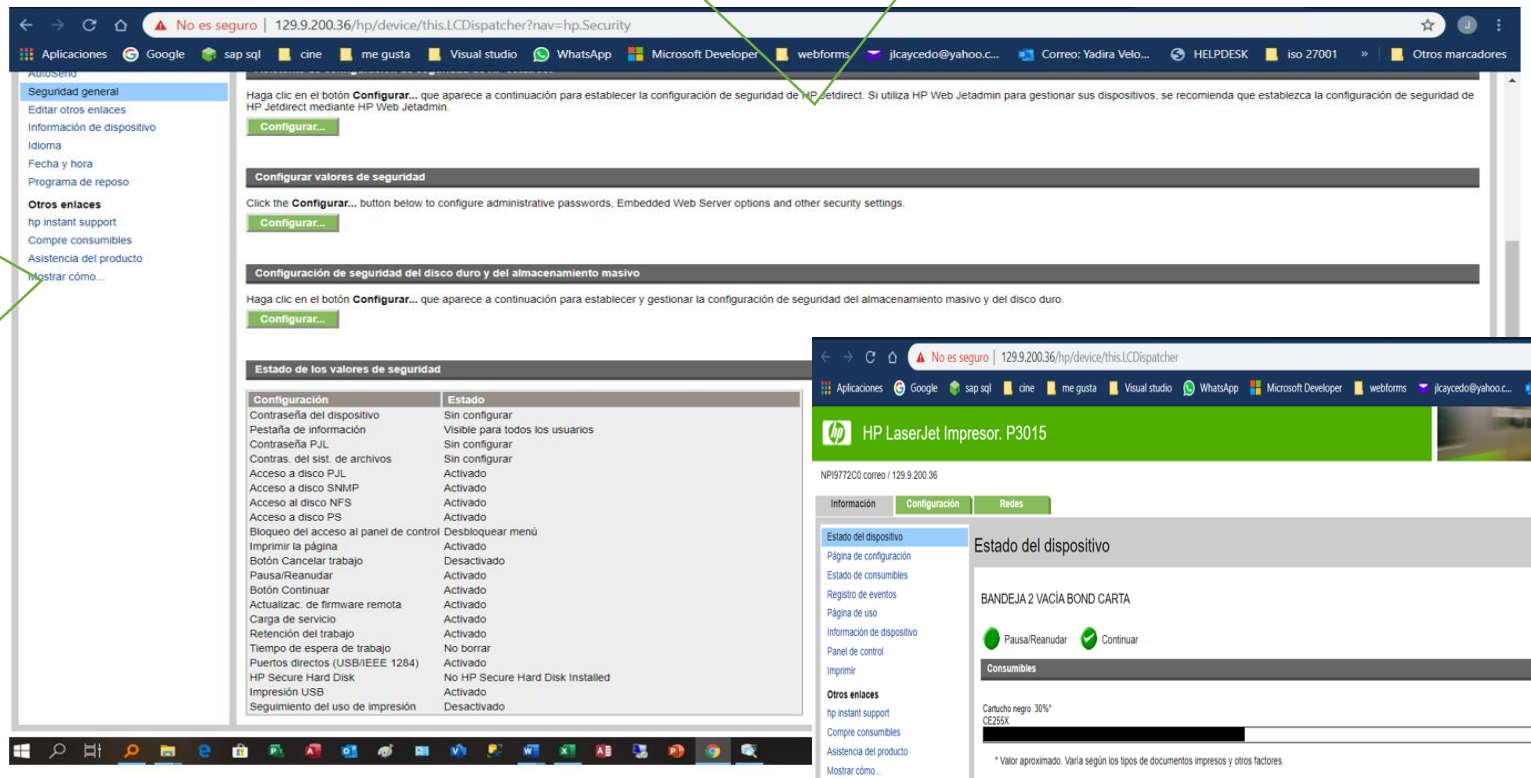


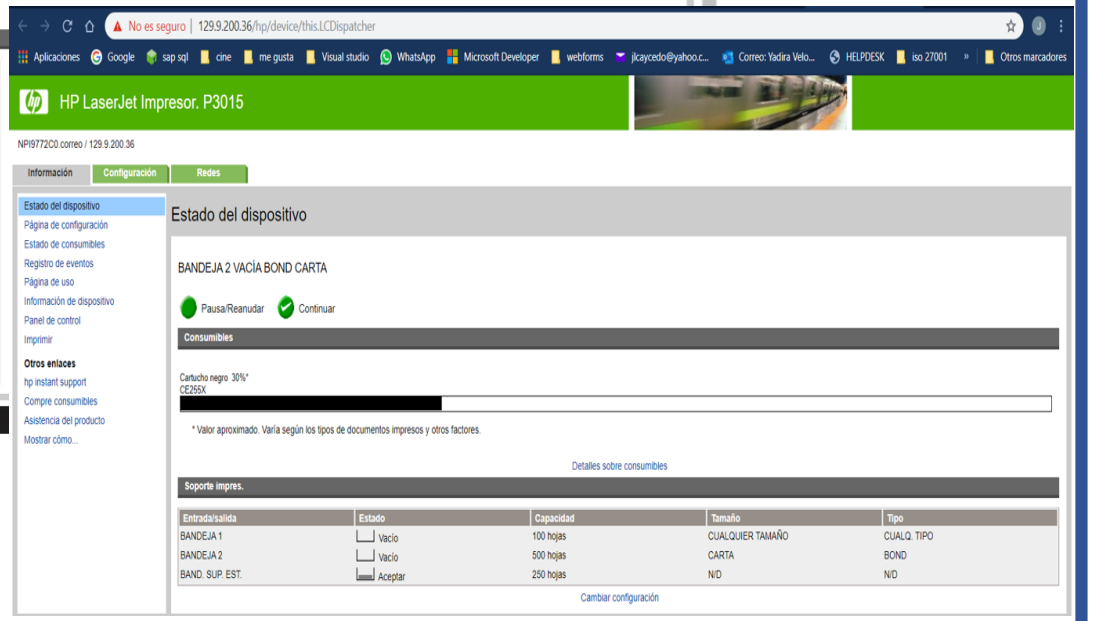
Al permitir escaneos sobre la subred de teléfonos IP, Se logra acceso a la configuración de teléfonos con usuarios y contraseña de fabrica

Administración de Accesos, Seguridad Lógica y Física

Luego de obtener la información de Equipos, servicios y puertos, se accede a cada uno de los objetivos identificados y se intenta ingresar para verificar si tienen protección, y si la protección no es la que viene configurada de fabrica para los equipos.

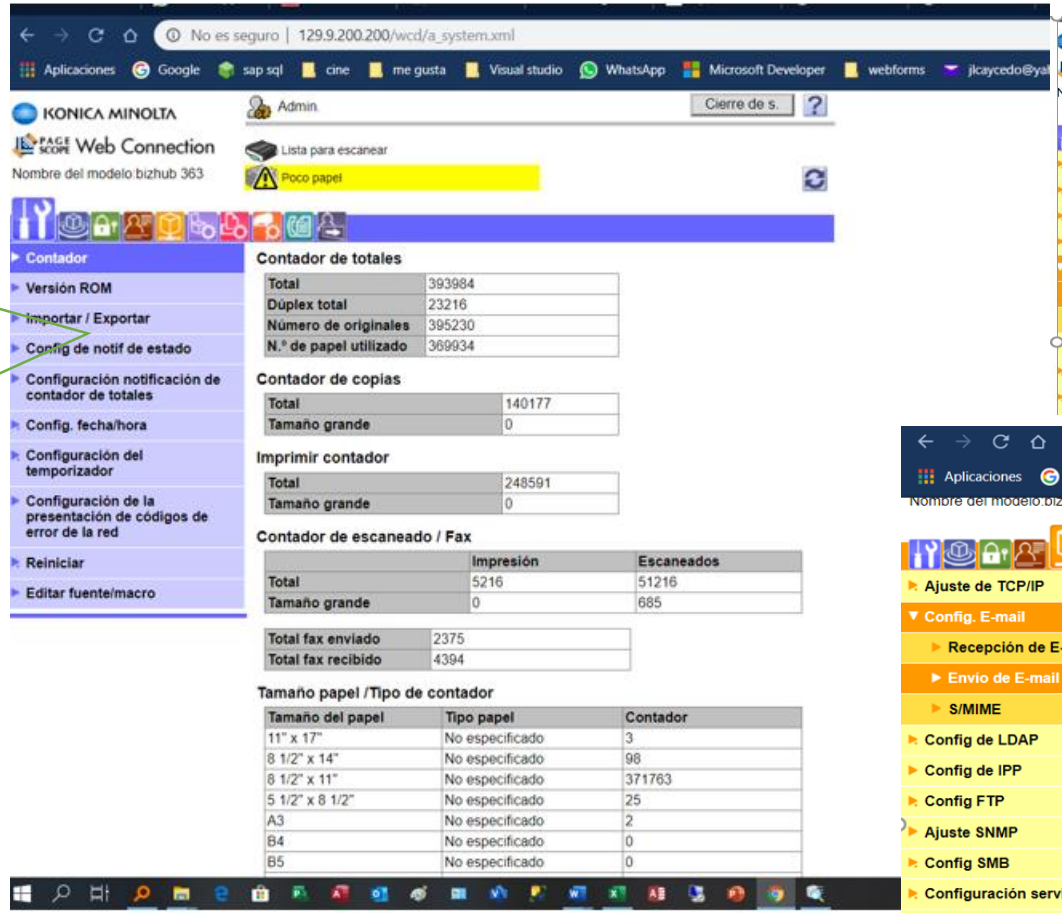
La imagen muestra la impresora: *HP LASER JET P3015,* que se encuentra sin protección de contraseña para cambios de configuración, es importante tener en cuenta que al tener acceso a la configuración de las impresoras es posible ejecutar scripts (conjunto de instrucciones autoejecutables), que permitirían tener copias de los documentos que se imprimen y/o enviar la copia automáticamente a un correo o unidad de almacenamiento.

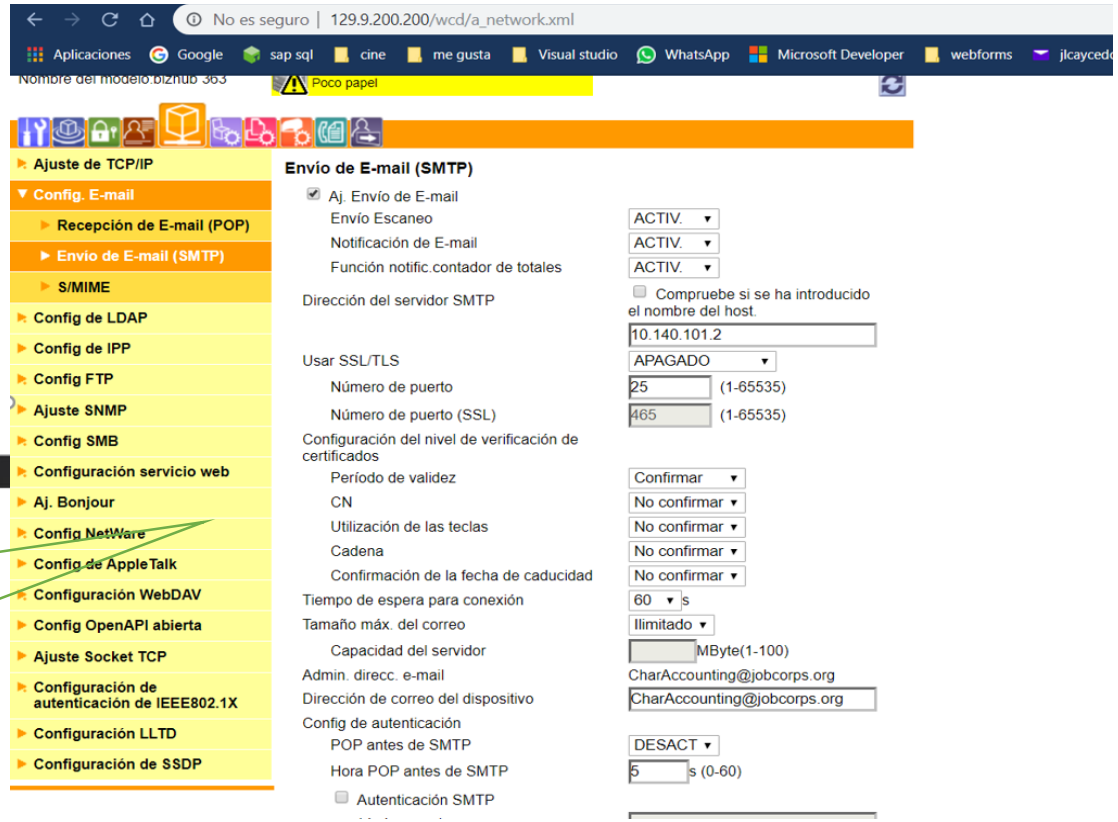




Administración de Accesos, Seguridad Lógica y Física

El auditor logro ingresar a la configuración de los escaners con el usuario administrador que tiene la contraseña de fabrica: 12345678.

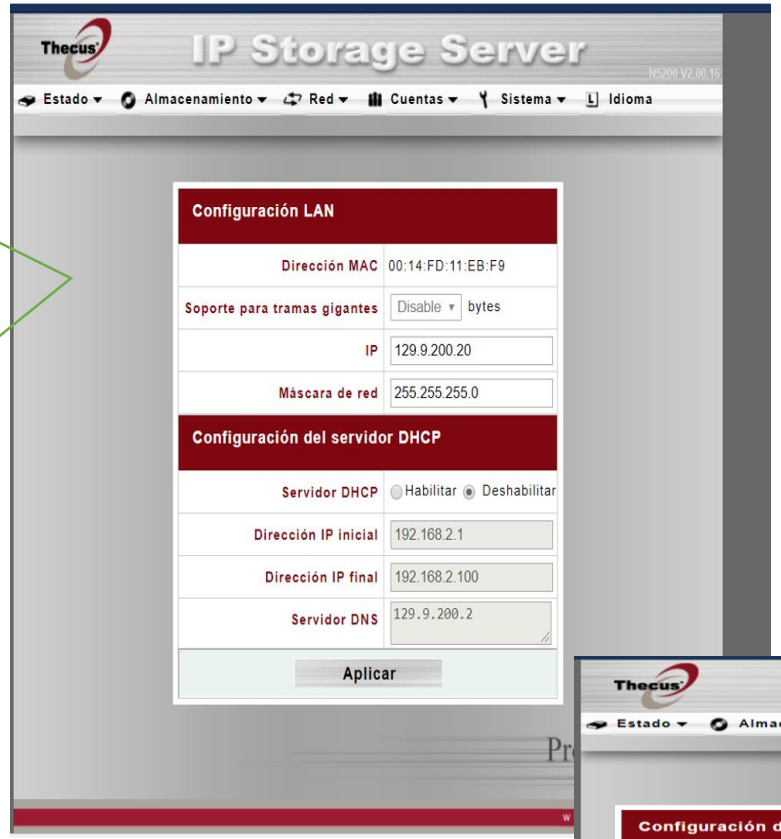


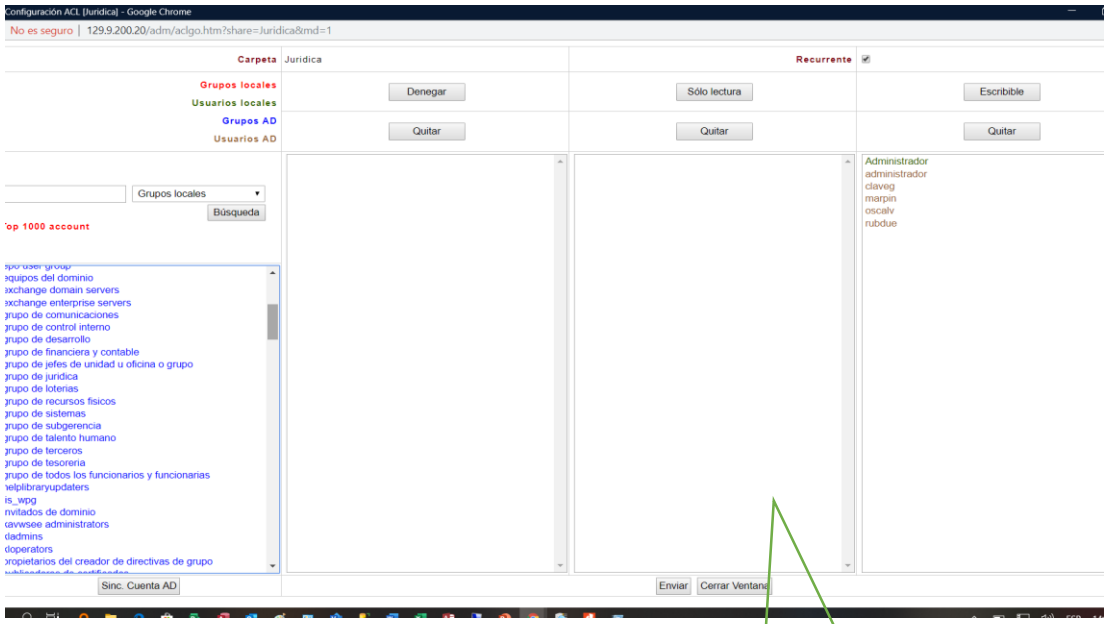


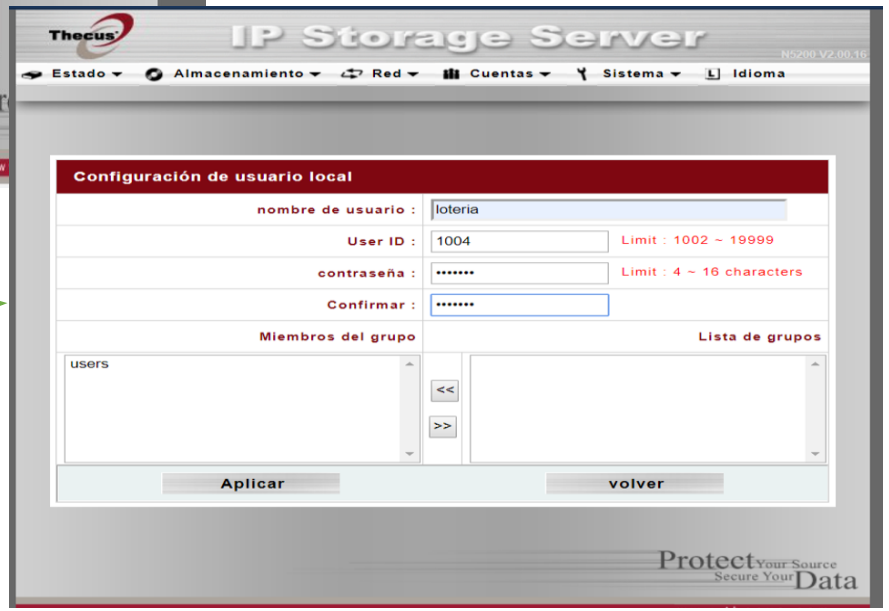
Un posible atacante podría configurar el dispositivo para enviar una copia de lo escaneado a un correo o unidad de almacenamiento controlada por él.

Administración de Accesos, Seguridad Lógica y Física

El auditor logro ingresar como usuario administrador a la configuración de la NAS (Unidad de Almacenamiento) donde se guardan todos los documentos de los usuarios de la Lotería de Bogotá por área y que es de donde se generan las copias de seguridad de los documentos y archivos de la entidad.







Al ser usuario administrador tiene control sobre todo lo que se almacena en estas unidades y puede cambiar o dar permisos a usuarios no autorizados o crear un usuario no perteneciente al dominio para tener acceso no controlado, ni autorizado. También podría modificar configuración para eliminar información. En la imagen se muestra la creación de un usuario: *loteria,* generado por el auditor como evidencia.

En la imagen se muestra los permisos de usuario sobre el repositorio de archivos del área Jurídica en la NAS, como evidencia de que el auditor podría cambiarlos o adicionar el usuario que creo para obtener acceso a este recurso.

Administración de Accesos, Seguridad Lógica y Física

Observaciones Gestión de Accesos :

La Lotería de Bogotá cuenta con un **controlador de dominio** Windows Server 2012 en el cual están configurados correctamente: el directorio activo y la creación de las unidades organizativas por cada área funcional para el control de acceso de equipos y usuarios a la red local.

Para la gestión de **asignación de usuarios y contraseñas** se creo el formato: "Solicitud de asignación de usuario", en el cual se definen los perfiles de accesos, servicios y aplicaciones para el nuevo usuario. El área crea el usuario de dominio asignándole una contraseña temporal y marcando la opción de cambio obligatorio de contraseña al siguiente inicio de sesión en los sistemas que lo permiten.

Se lleva un correcto control sobre el retiro temporal o permanente de usuarios y se deshabilitan sus cuentas respectivas.

En cuanto a las **políticas de dominio** se tienen correctamente configuradas: Política predeterminada de controladores de dominio, la política predetermina del domino, fondo de escritorio y una para el Bloqueo de PC's. las directivas de contraseña se tienen con longitud mínima de 8 caracteres, vigencia de 45 días, 3 contraseñas recordadas, se exige complejidad y se tiene configuradas correctamente las directivas de Kerberos, a los usuarios se le alerta automáticamente el cambio obligatorio de contraseña con 5 días de anticipación.

La gestión de **contraseñas de administradores** de las bases de datos Oracle la maneja únicamente la profesional encargada del área. La Gestión de accesos en el aplicativo de gestión documental SIGA está integrado con LDAP a los usuarios del dominio. En el aplicativo administrativo y financiero hay un módulo de seguridad, desde el cual se define los perfiles de acceso y permisos a los usuarios.

El aplicativo para la gestión de apuestas permanentes en línea y tiempo real: "*Chanseguro*" cuenta con un módulo de administración para la **gestión de privilegios**, se tiene un usuario administrador (*weblogic*) y un usuario de consulta, los permisos están definidos para los tipos de usuario y se puede consultar el log de acciones realizadas por cada usuario.

No están configuradas correctamente las plantillas administrativas para reemplazar el nombre de usuarios **administradores locales** en las estaciones de trabajo por otro y así evitar ataques locales con este usuario, ni tampoco para deshabilitar el **usuario invitado** de Windows automáticamente y deshabilitar la identidad de usuario anónimo.

No se tiene configurado el umbral de **bloqueo de cuenta** por intentos de inicio de sesión fallidos, lo cual debe incluirse como control de seguridad contra intentos de acceso no autorizados. Además, no se tiene un procedimiento formal para el cambio periódico de las contraseñas de los usuarios administradores locales en los PC's. ni una matriz de usuarios vs perfiles de acceso global, que permita realizar seguimientos a la configuración actual de todos los usuarios en los sistemas de información.

Para el correo corporativo y para el sistema administrativo y financiero no se tiene la opción de configurar el **cambio de contraseña** periódico lo cual expone la seguridad de los mismos, ya que la clave podría ser capturada y decodificada para obtener accesos no permitidos o suplantación de identidad. Para el sistema administrativo y financiero, si bien existe un menú de auditoria, solo tiene la función de auditoria financiera. No existe un módulo para realizar seguimiento al log de transacciones y seguimientos a las acciones de los usuarios.

Administración de Accesos, Seguridad Lógica y Física

Observaciones Seguridad de Pc's y Correos:

Únicamente los usuarios administradores pueden detener los servicios de Windows y realizar actualizaciones.

Sin la contraseña de administrador, no se permite editar las directivas de grupo para cambio de políticas locales, ni cambiar las propiedades de las conexiones de red.

No se permite cambiar la configuración de los recursos compartidos, la navegación en sitios de alta peligrosidad estándar está bloqueada por el firewall. La instalación/desinstalación de software se tiene restringida a usuarios administradores..

En todos los equipos examinados no se tienen configurados bloqueos para el panel de control, el editor del registro de Windows, la ejecución de comandos: *CMD* y *Power Shell*, las cuales se deben bloquear para usuarios no administradores, ya que son comúnmente utilizadas por atacantes y/o software malicioso para ejecutar scripts (archivo de ordenes o instrucciones) que violan la seguridad y permiten programar accesos remotos no permitidos, además en los PC's, se permite la inactivación de cliente del antivirus.

Los PC's permiten el almacenamiento de credenciales tanto web como Windows, lo que permite descubrir contraseñas de usuarios para diferentes servicios fácilmente.

El auditor logro obtener contraseñas de usuarios de la Lotería de Bogotá por diferentes métodos, con las que obtuvo acceso a los diferentes aplicativos y servicios de TI de la entidad, Capturando los usuarios y contraseñas de ingreso a los aplicativos, correos, oficina virtual de la SHD, función pública, Dian, linio, usuarios de dominio, *pasivocol*, entre otros.

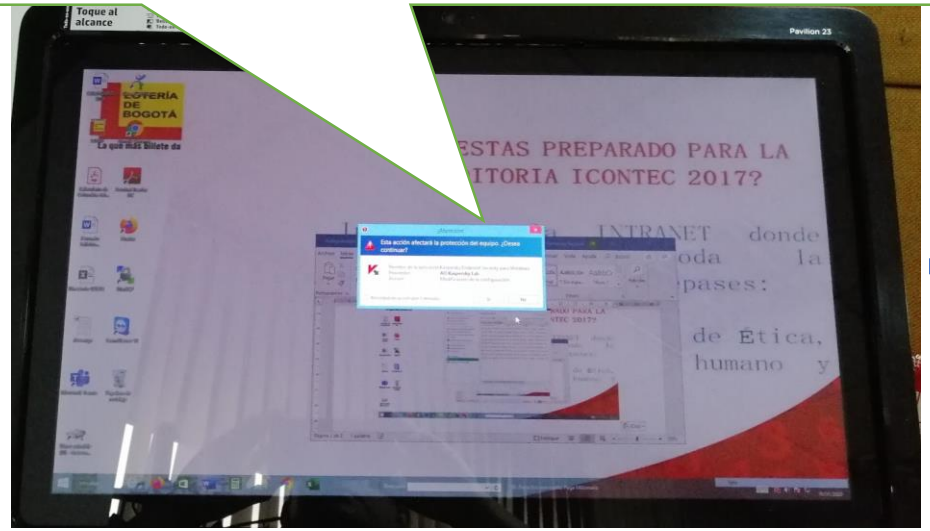
No se tiene ningún tipo de control sobre la conexión de medio extraíbles tales como USB, CD 's o DVD 's, esto permitió al auditor ejecutar varios tipos de software considerado como peligroso y de hackers

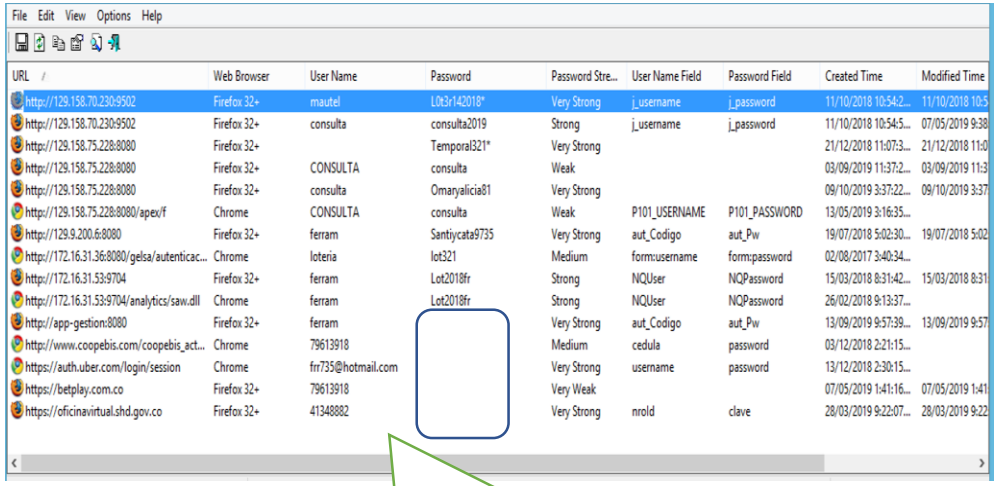
Hay varios PC's de la Lotería de Bogotá que poseen dos tarjetas de red: alámbrica e inalámbrica, en estos equipos no está restringida la conexión a cualquier red WIFI, ya se personal o de pago, lo cual permite que no se tenga la protección de firewall y por ende no se apliquen las restricciones a la navegación en internet y se puedan descargar cualquier tipo de archivo.

Para las cuentas de correo no se tiene configuradas la validación de doble factor para proteger el acceso a cuentas desde equipos no conocidos, con una clave o validación de numero de celular, por ejemplo, en caso de que la contraseña principal se capturada.
Adicionalmente, no se encuentra restringido el uso de correos personales, lo cual es un riesgo de seguridad de ataques tipo Phishing, mediante los cuales pueden entrar a los equipos de red distintos tipos de malware, entre ellos Ramsonware.

Administración de Accesos, Seguridad Lógica y Física

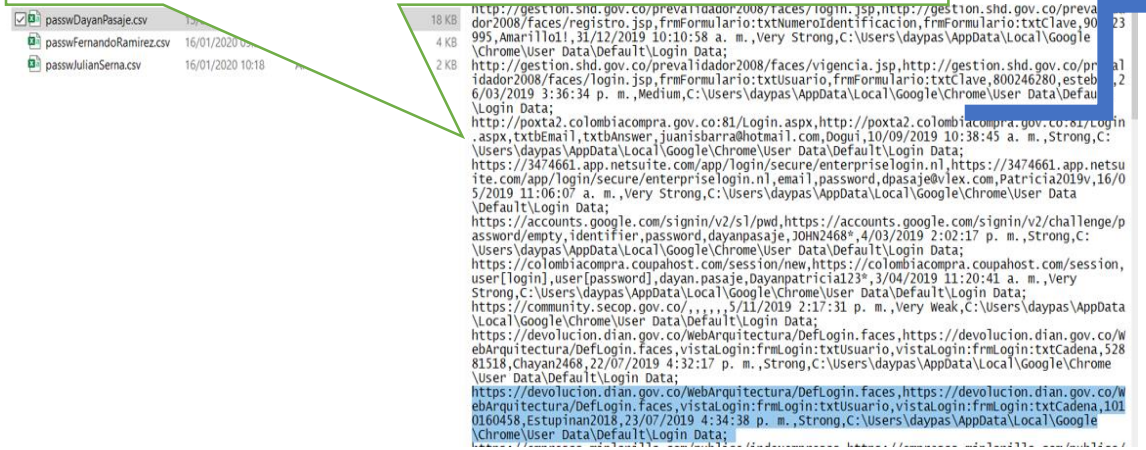
Ya que el firewall no bloquea las descargas y que el antivirus puede deshabilitarse, el auditor descargo archivos considerados “peligros” o virus tipo programas portables con los cuales descifro contraseñas.



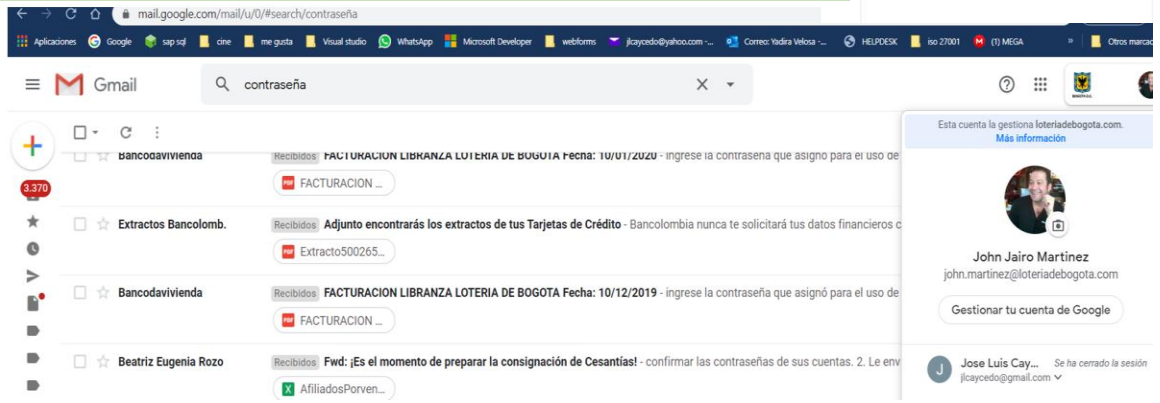


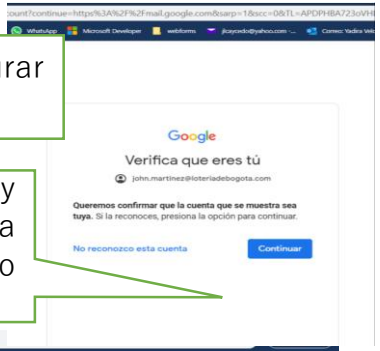
Una vez descargado el programa se logra capturar contraseñas de usuarios.

Al permitir USB ’s y almacenamiento de contraseñas, con solo conectar una USB, se pueden generar archivos planos con información de usuarios y claves.



Una vez realizadas las capturas de usuarios y contraseñas, al no estar configurada en los correos la autenticación de doble factor, se puede suplantar y/o acceder a las cuentas o sistemas del funcionario





Administración de Accesos, Seguridad Lógica y Física

Observaciones Seguridad Física:

Los servidores, equipos de comunicación y demás elementos críticos se encuentran resguardados en centros de cómputo con control de acceso de biométrico solo para los funcionarios del área de TI.

El centro de cómputo tiene instalados correctamente elementos de seguridad física como detección de incendios, refrigeración, control de temperatura.

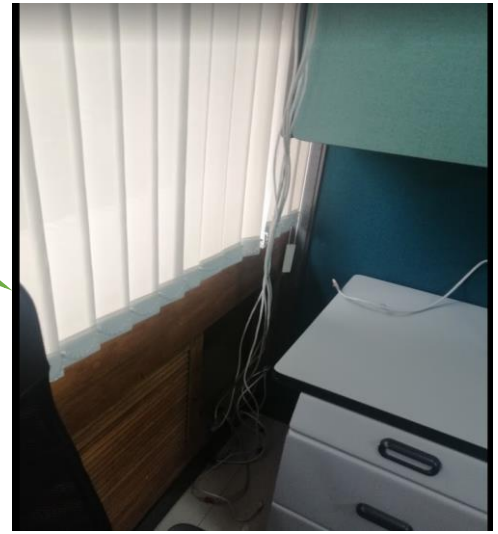
Todo invitado debe anunciarse y registrarse en la entrada al edificio, además relacionar el portátil y su serial.

Se cuenta con canaletas adecuadas para red eléctrica, de voz y de datos en la mayoría de las áreas, sin embargo, en varias oficinas el cableado se encuentra por fuera de las canaletas, colgando del techo falso y cables de conexión de red (patch cords) desatendidos y sin uso, esto permitirá hacer conexiones no permitidas que afecten la seguridad de la red

No se encuentran etiquetados la totalidad de los cables en los racks lo cual dificultaría la identificación de fallas en los puntos y disminuye los tiempos de atención. En algunos racks no se tienen organizados correctamente los cables.

No se cuenta con diagramas en los closets de comunicaciones del centro de cómputo, ni etiquetas, que permitan identificar rápidamente los elementos, equipos y ubicaciones de puntos en los closets de comunicaciones, lo que genera dependencia del conocimiento de los funcionarios del área.

Cables desde el techo y patch cords sin uso.



Cables sin etiquetas.

Administración de Accesos, Seguridad Lógica y Física

Recomendaciones

- Configurar correctamente la LAN para evitar que se realicen escaneos a direcciones IP diferentes a la que corresponde al equipo de acuerdo a su configuración. Crear dos segmentos de red: uno para los servidores y otro para los equipos, para aislar accesos no permitidos a los servidores.
- Actualizar el diagrama de red conforme a los hallazgos del informe, especificando las direcciones IP, equipos, Wifi y demás elementos activos de la red.
- Elaborar instructivos de la configuración y operación del firewall, routers y swtichs, además de un procedimiento para el cambio periódico de las claves de administrador para el Dominio, Routers, Firewalls, bases de datos, etc. De ser posible instalar un software para la administración y almacenamiento seguro de las contraseñas de administración. Integrarlos a los documentos del dominio 12 de MSPI.
- Configurar las políticas de firewall y las políticas de dominio para impedir descargas de archivos ejecutables o de instalación. La restricción se debe generar independientemente del cargo del usuario. Todo archivo ejecutable que se requiera, debe ser autorizado por el área de TI.
- Configurar correctamente todos los computadores para que no se permita cerrar el cliente detener cualquier protección del antivirus. Deshabilitar las tarjetas de red inalámbricas en los PC's que tengan dos tarjetas o solo permitir la conexión a las redes WIFI autorizadas y controladas por la entidad.
- Configurar la red y el DHCP para restringir la conexión al dominio solo a equipos cuya dirección de tarjeta de red (*Mac Address*) este registrada en la lista autorizada.
- Restringir en todos los equipos de escritorio y portátiles los accesos al panel de control en especial al centro de redes y recursos compartidos, a la ejecución de comandos desde el símbolo del sistema de Windows (*CMD*), editor de registro de Windows (*RegEdit*) y del PowerShell. Configurar los navegadores para impedir el almacenamiento de contraseñas en texto plano e impedir la creación de conexiones ODBC.
- Configurar correctamente todos los clientes del antivirus para que no permita ejecución y descargue de archivos considerados como peligrosos, Por ningún motivo exponer información de claves de acceso en archivos sin encriptación ni en correos y/o documentos físicos sin custodia.
- Configurar todas las directivas de seguridad del dominio de acuerdo con las recomendaciones de Microsoft para entornos corporativos y habilitar bloqueo de cuentas por intentos fallidos.
- Revisar los niveles de acceso a la navegación en internet con el fin de garantizar que todos los usuarios tengan privilegios acordes con las funciones de su cargo. Generar un procedimiento de revisión periódica de los informes generados por el antivirus y firewall, tomar acciones correctivas frente a alertas y documentarlas.

Administración de Accesos, Seguridad Lógica y Física

Recomendaciones

Modificar las configuraciones del Firewall y del antivirus para bloquear automáticamente todo tipo de trafico de envenenamiento ARP, para evitar el uso de aplicaciones de captura de paquetes de red (sniffers), Además de generar un procedimiento de revisión periódica a los informes generados por el antivirus y el firewall para tomar acciones correctivas pertinentes frente a alertas.

Realizar un procedimiento de revisión y cambio periódico de las contraseñas de los equipos activos de red tales como: Switches, impresoras, NAS, robots de cintas, etc. y nunca dejar las contraseñas de fábrica de estos dispositivos

De ser posible, frente a la necesidad de renovación o cambio de licenciamiento del firewall y/o antivirus, incluir en los anexos técnicos la sincronización Firewall – Endpoints (clientes de antivirus), para proteger correctamente todo el trafico interno de la red local, y así poder detectar y bloquear automáticamente cualquier anomalía o ataque interno a los equipos y elementos de red.

Cambiar todas las contraseñas de cualquier servicio expuesto sobre la red, de los teléfonos IP y ocultarlos para que no sea posible su visualización por parte de cualquier usuario sin autenticación en dominio.

Implementar medidas automáticas o manuales para el cambio periódico de contraseña en todos los servicios Tic y sistemas de información atendiendo el dominio 9 de MSPI. No permitir el uso de correos electrónicos personales, a menos que se demuestre su necesidad para cumplir las funciones del cargo.

En el marco de la construcción del inventario de activos de información, identificar equipos de computo que almacenan de manera local información de carácter confidencial e implementar medidas de seguridad que impidan su acceso por alguien distinto al responsable del equipo.

Atender las vulnerabilidades encontradas del portal web de la Lotería de Bogotá. Implementar informes y procedimientos que permitan verificar y controlar globalmente todos los permisos de accesos actualmente configurados en los sistemas todos los aplicativos de la Lotería de Bogotá.

De ser posible, implementar informes de auditoría sobre el log de transacciones de la base de datos del software administrativo y financiero, que permita hacer seguimientos a las acciones realizadas por los usuarios, con información de: usuario, equipo, fecha-hora, tipo de acción (borrar, actualizar/modificar, crear), detalle de la acción.

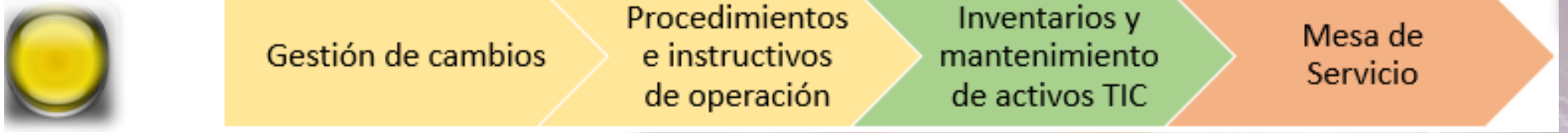
Elaborar e implementar una política para el uso controlado de dispositivos o medios de almacenamiento externo como USB ’s, deshabilitándolo en aquellos equipos que no sea indispensable su uso y controlando por contraseña o desde el cliente del antivirus el uso de los mismos.

Adelantar un plan de etiquetado y generación de diagrama en todos los closets de comunicaciones (Racks) del centro de cómputo para permitir la fácil ubicación y rápida identificación de equipos y puntos de red. Realizar un plan de mejoramiento y aseguramiento del cableado en todas las oficinas, y recoger cualquier cable de conexión de red que no se esté utilizando.

Se deben desactivar todos los puntos de red que no tengan uso continuo para evitar conexiones no permitidas.

Resultados por dominio

Administración de recursos TIC



Administración de recursos TIC

Administración de Recursos TIC

Observaciones Gestión del cambio, Procedimientos e Instructivos de Operación:

La identificación de necesidades de adquisición de recursos se realiza ya sea por solicitud de las áreas de negocio o por necesidades identificadas en el proceso de gestión de Tecnologías de Información. El parque informático responde a las demandas de crecimiento de la plataforma TI.
Los elementos y canales de comunicaciones se adquieren y actualizan de acuerdo con las necesidades de crecimiento, buscando un entorno seguro.

La entidad cuenta correctamente con procedimientos para la planeación, gestión y seguimiento a las adquisiciones y el proceso de gestión TIC ha demostrado cumplir con estos procedimientos en sus contrataciones.

El proceso a adelantado el contrato 072-2019 con HACHI S.A.S para la implementación de la herramienta de monitoreo, con lo cual se podrá hacer análisis predictivo de la capacidad a los servicios tecnológicos y llevar trazabilidad de eventos como criterio para determinar de manera oportuna los requisitos de plataforma tecnológica para asegurar la continuidad y desempeño de la operación

No se ha adelantado un procedimiento formal de gestión de cambio TIC de los dominios 12 y 14 de MSPI, que mitigue el riesgo de desequilibrio costo/beneficio en adquisiciones e incluya un formato de evaluación de criterios de satisfacción y viabilidad relacionados con: satisfacción de requisitos funcionales, estandarización, evolución, capacidad de integración, mantenimiento, desempeño, apropiación del conocimiento, riesgo tecnológico, seguridad de la información y sostenibilidad futura

El proceso solo cuenta con 4 procedimientos y 2 formatos relacionados con la gestión TIC, que resultan insuficientes para establecer los lineamientos de operación y cumplir con el alcance MSPI. De igual manera no se entregó evidencia de la existencia de instructivos de operación que son los documentos que constituyen la trasferencia de conocimiento documental sobre la operación de los activos TIC administrativos en ausencia temporal o definitiva de los responsables actuales, y que deben ser incluidos en la declaración de aplicabilidad y ajustados de acuerdo a las herramientas actuales e implementación real de controles de seguridad. Los usuarios entrevistados manifiestan no conocer los 2 formatos.

Administración de Recursos TIC

Observaciones Inventarios y Mantenimiento de Hardware y Software:

Los inventarios de hardware se gestionan en el área de TI mediante un libro el Excel que se diligencia manualmente de acuerdo a información recolectada en las altas y bajas de la equipos, no se cuenta con agentes automatizados e integrados a una herramienta de mesa de servicio que permita realizar escaneos de red programados que identifiquen y actualicen automáticamente todo el hardware, periféricos y software que se encuentra instalado.

El inventario de software base se gestiona también manualmente en el formato de Excel en el cual no se relacionan los seriales y/o números de licencia en cada equipo, ni es posible identificar en que equipos esta instaladas las licencias.

Se tiene una carpeta física con toda la relación de licenciamiento, lo que dificulta la validación y seguimiento de cada licencia por equipo.

No se cuenta con un formato de hoja de vida de equipo de cómputo, en el que se especifique la información general del equipo, configuración de hardware y detalle de software, mantenimientos y datos del funcionario al que se le asigna el equipo. No hay formato de HV de servidores.

Las solicitudes de alta no se encuentran centralizadas en el área de recursos humanos pese a que es quien maneja la información de contrataciones, retiros, incapacidades, vacaciones y demás novedades que puedan afectar la seguridad de accesos a los servicios TIC.

Si bien desde la consola de antivirus Kaspersky se pueden generar informes de software instalado en los computadores que tiene instalado el cliente de antivirus, no se usa esta herramienta para llevar un control mas actualizado del inventario de software.

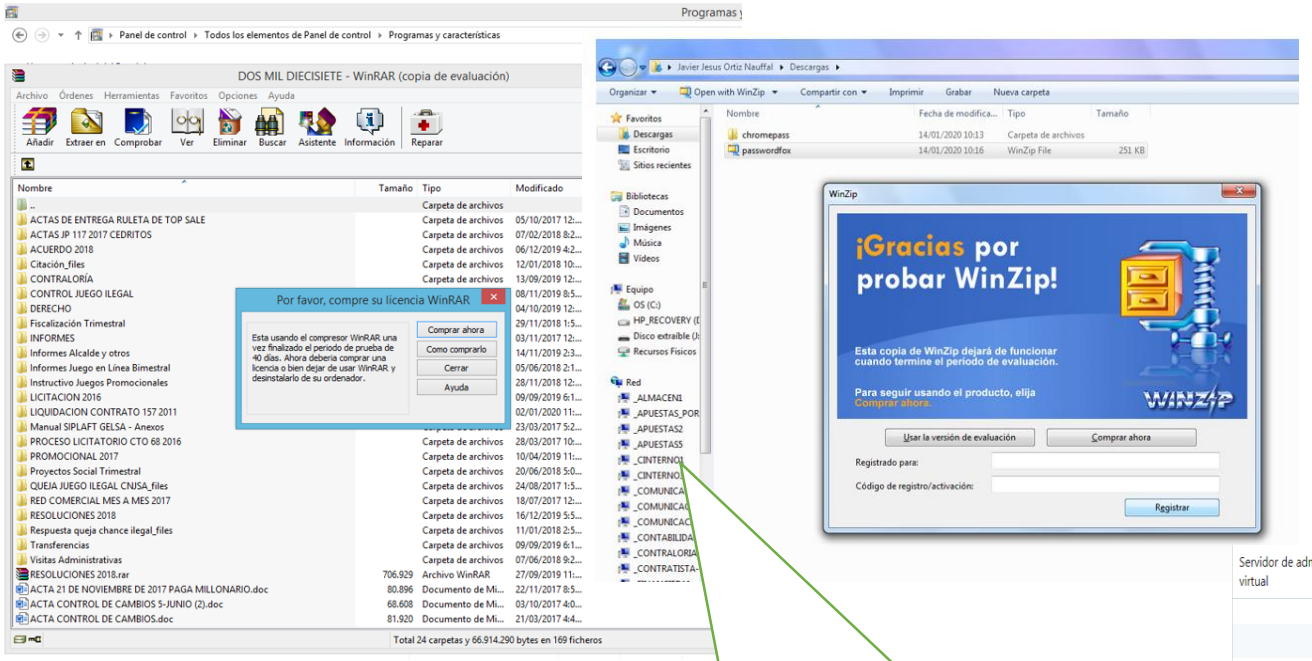
Se encontraron instalaciones de aplicaciones o herramientas que no se encuentran relacionadas dentro de las licencias adquiridas, lo cual expone a la Lotería de Bogotá a riesgo de uso de software ilegal.

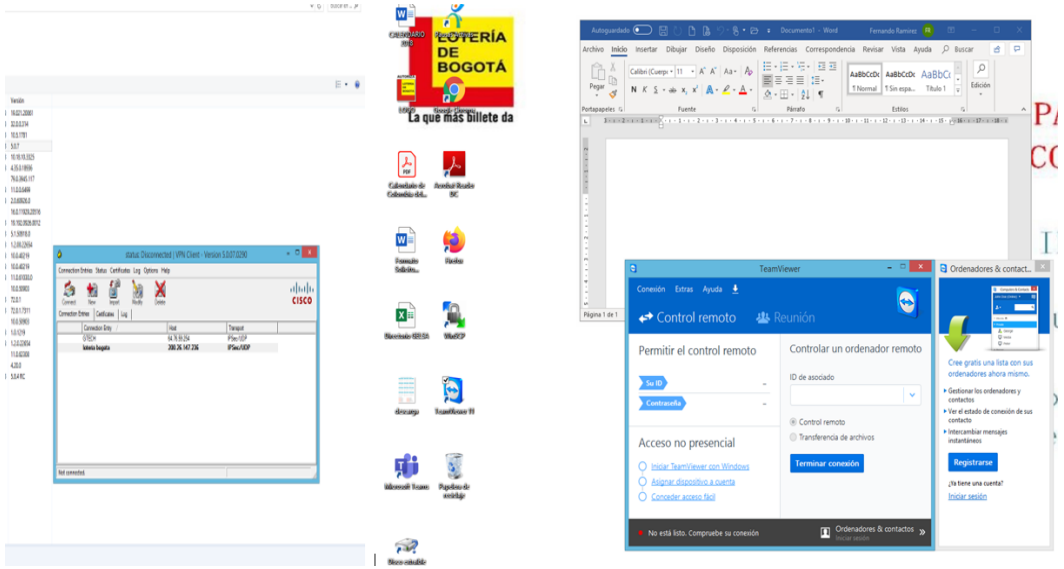
No se tiene programado un cronograma para el mantenimiento de los equipos de cómputo. El mantenimiento se está realizando como parte del soporte por demanda, por lo tanto, si un equipo no solicita soporte no recibe mantenimiento. Anteriormente se tenía tercerizado, pero en el 2019 no se renovó el contrato, ya que la mayoría de equipos son nuevos y aún tienen garantía. Se incluyo en el presupuesto 2020.

El mantenimiento de impresoras y escáneres, así como el suministro de los consumibles está en outsourcing que maneja el área de recursos físicos. Esta situación tiene la debilidad de la posible exclusión de estos activos de las implementaciones de controles de seguridad tales como impresión por código de acceso y direccionamiento de escáner a los correos institucionales.

Administración de Recursos TIC

Inventarios y Mantenimiento de Hardware y Software:





Uso de Herramientas con Periodo de evaluación vencido

Software de accesos remoto y juego instalados en equipo de usuario.

Servidor de administración virtual	Aplicación	Número de versión	Proveedor	Número de dispositivos	Número de grupos
	Synaptics WBF FP Reader	5.5.3.1099	Synaptics Incorporated	2	2
	Teams Machine-Wide Installer	1.2.0.22654	Microsoft Corporation	1	1
	TeamViewer	15.0.8397	TeamViewer	1	1
	TeamViewer 11	11.0.62308	TeamViewer	1	1
	TeamViewer 11	11.0.65452	TeamViewer	1	1
	TeamViewer 14	14.1.18533	TeamViewer	1	1
	TeamViewer 14	14.4.2669	TeamViewer	3	2
	TeamViewer 14	14.5.5819	TeamViewer	1	1
	Tecnología de gestión activa Intel®		Intel Corporation	2	2
	Text To PDF Converter v1.5		verypdf.com, Inc.	1	1
	TextPad 8	8.1.2	Helios	3	1
	Thunderbolt™ Software	17.3.72.250	Intel Corporation	2	2
	Tom Clancy's Rainbow Six Siege		Ubisoft Montreal	1	1
	Tom Clancy's Rainbow Six Siege TS		Ubisoft Montreal	1	1
	TortoiseSVN 1.10.1.28295 (64 bit)	1.10.1.28295	TortoiseSVN	1	1
	Trusteer Seguridad Terminal	3.5.1930.429	Trusteer	1	1

Administración de Recursos TIC

Observaciones Mesa de Servicio:

Recientemente se inició la implementación de la herramienta GLPI por parte de sistemas para la gestión de la mesa de servicio y ya se han realizado la configuración de usuarios administradores, configuración de perfiles y categorías de tipología de servicios. De igual manera, en el marco del contrato 65 de 2019 se incluyó la construcción, implementación en GLPI y capacitación a usuarios en el modelo de servicio de la entidad.

La entidad no cuenta con procedimientos estructurados de Modelo de servicio debidamente implementado a través de una herramienta tecnológica. Los soportes se reciben por teléfono o correo y no se tiene establecidos acuerdos de niveles de servicio.

No se tiene implementado un modelo de servicios para los terceros que prestan soporte y/o desarrollo de software

No se han desarrollado los procedimientos de trasferencia de conocimiento de soporte y mantenimiento de los terceros a cargo de sistemas de información hacia la entidad.

Pese a que el cargo de la profesional especializada es el liderazgo del área de sistemas, los usuarios manifiestan que varios soportes son atendidos directamente por ella dado su conocimiento exclusivo sobre la plataforma.

No se lleva registro estructurado de los soportes a terceros.

El área manifiesta que es difícil que los usuarios acepten tramitar todas sus solicitudes por una herramienta de mesa de servicio, pero en las entrevistas adelantas una vez explicadas las ventajas, se mostraron abiertos al cambio

Administración de Recursos TIC

Recomendaciones

Implementar herramientas de monitoreo y análisis predictivo de la capacidad y documentar los procedimientos e instructivos alineados a la herramienta, en el marco del dominio 12 del MSPI

Documentar, formalizar y divulgar un protocolo de administración del cambio para todos los elementos de TI, bajos los criterios de capacidad, soporte, competitividad, dirección organizacional y seguridad: Hardware, Software base, Comunicaciones, Software aplicativo o sistemas de información, Recurso Humano, Políticas y/o Procedimientos y Servicios

Alinear la construcción de los documentos de operación de la gestión TIC y de la Gestión de Seguridad de la información siguiendo los lineamientos establecidos por el MSPI y adelantar la declaración de aplicabilidad para identificar el universo de políticas, procedimientos, instructivos y formatos.

Implementar en el software GLPI de mesa de ayuda que se está liberando para su uso en la Lotería de Bogotá, con el agente: *Fusión Inventory* para programar la ejecución periódica y automática, por escaneo la actualización periódica del inventario de hardware y software

Relacionar en cada la hoja de equipos del GLPI el licenciamiento correspondiente y crear un procedimiento para su revisión periódica de acuerdo a lo detectado por el agente del GLPI para desinstalar cualquier software no licenciado o no permitido por la entidad.

Incorporar en los registros de procesos y procedimientos un acta de alta de activos de información que incluya equipos, software y accesos. . Esta acta es base para el control de devolución de activos de información al cese de la relación contractual de que habla el control ISO 27002:2013 9.2.6 Eliminación o ajuste de los derechos de acceso.

Junto con la entrega del equipo y los accesos acompañar al usuario en el ingreso a cada servicio para garantizar que cambia la clave en el primer inicio de sesión, aunque la herramienta no lo exija. Entregar las claves iniciales personalmente no enviarlas explícitas por correo ni por GLPI.

Se deben programar un cronograma de mantenimiento físico y lógico a los equipos de cómputo de la Entidad, si bien las garantías cubren daños físicos, no cubren los daños lógicos o por virus y puede afectar el rendimiento de los equipos. Incluir en el mantenimiento preventivo un guion de subsanación de debilidades en los PC presentadas por el auditor.

Centralizar y clasificar todos los soportes relacionados con los sistemas y plataforma tecnológica de la Lotería de Bogotá, incluyendo los sistemas de información y configurar el direccionamiento de estos soportes a los proveedores de los mismos, con el objeto de poder generar indicadores de todos los servicios y soportes del área y de sus proveedores, incluyendo el cumplimiento de ANS

Revisar los criterios para la configuración de la herramienta GLPI relacionados en el informe de la Auditoria y realizar planes de sensibilización a usuarios para la implementación del nuevo modelo de servicio centralizado.


GRACIAS!