Nombre del activo	Descripción de actividades	Recursos generales y financieros necesarios	Persona responsable	Plazos de inicio y finalización	Programa de capacitación y Sensibiliación	Método para evaluación de resultados	Estado
Aire Acondicionado	A.12.1.3 Gestión de capacidad • Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema. • Análisis de capacidad del equipamiento de cómputo a alojar en centro de cómputo, identificando requerimientos de carga, BTUs, Condiciones ambientales.	Recursos requeridos: • Un documento formal de capacidades requeridas vs consumidas para saber si el aire acondicionado soporta los equipos del centro de cómputo con una holgura definida • Establecer umbrales y gestionar mediante herramienta de monitoreo	• Director de TIC • Coordinador de Operaciones TIC • Profesional de seguridad de la información	Enero a diciembre 2019	Crear una estrategia de concienciación sobre la importancia de diligenciar los documentos de capacidad condiciones ambientales y actualizarlos cada vez que llega un activo nuevo.	Para procedimientos: • Monitoreo permanente de niveles definidos.	Totalmente implementado
Aire Acondicionado	A.11.1.4 Protección contra amenazas externas y ambientales • Se debe diseñar y aplicar protecciones físicas contra daños por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastres natural o artificial. • Implementar un sistema de protección contra incendios de agente limpio y revisar condiciones y adecuación física.	Recursos Requeridos: • Un sistema de extinción de incendios de acuerdo a la normatividad vigente • tipo agente limpio. • proveedor del sistema de extinción • verificación de pre• requisitos y condiciones de instalación • Obras civiles	• Director de TIC • Coordinador de Operaciones TIC • Profesional de la seguridad de información • Jefe Administrativa	Enero a diciembre 2019	Capacitación y concienciación sobre la importancia y uso del sistema de extinción, el mecanismo de uso y los parámetros de seguridad a tener en cuenta.	Para nuevo equipamiento: • verificar si ha sido comprado y está en uso. • Este disponible el manual de uso y las normas de seguridad	Totalmente implementado
Aire Acondicionado	A.11.2.1 Ubicación y protección del equipo • Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado. • Se requiere adecuar la ubicación del aire acondicionado, ya que está sobre los equipos en el centro de cómputo. De acuerdo con las normas como por ejemplo ICREA• std• 131• 2013, TIA 942, etc., • Establecer áreas demarcadas, de energía, de procesamiento y medio ambiente.	Recursos Requeridos • Un Proveedor para adecuar el sistema de extinción con normas básicas definidas dentro de la construcción de Centro de Procesamiento de datos y definición clara de ANS. • Ampliar el espacio del Centro de Cómputo para ubicación del sistema de extinción	• Director de TIC • Coordinador de Operaciones TIC • Profesional de Seguridad de la Información • Coordinador de Soporte • Jefe Jurídica • Contratista seleccionado	Enero a diciembre 2019	• Plan de concienciación sobre la importancia de proteger los equipos. • Realizar capacitación en operación, administración y mantenimiento del sistema implementado	Para cambios de infraestructura: • Verificar y monitorear que los servicios prestados están operando correctamente y se haya cumplido los estándares mínimo definidos por la FCM • Para proveedores: • Verificar si se están cumpliendo los ANS.	Totalmente implementado
Aire Acondicionado	A.11.1.5 Trabajo en áreas seguras • Se debe diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras. • Revisar el Procedimientos para trabajo en áreas seguras de FCM, según NTC 1700.	Recursos requeridos: • Una Brigada de Emergencia que haga simulacros y tenga el plan de evacuación vigente.	• Director de Talento Humano • Analista de Salud Ocupacional • Brigadistas	Enero a diciembre 2019	Socializar, capacitar y concienciar sobre la importancia del plan de evacuación	Para Recurso Humano: • Verificar mediante encuesta o simulacro no planeado la efectividad de la implantación del plan de evacuación.	Totalmente implementado
Aire Acondicionado	A.12.6.1 Gestión de vulnerabilidades técnicas • La información de las vulnerabilidades técnicas de los sistemas de información que se utiliza se obtendrá en el momento oportuno, la exposición de la organización a este tipo de vulnerabilidades es evaluada y las medidas adecuadas son adoptadas para hacer fente al riesgo asociado. • Cambio del equipo que garantice las condiciones de enfriamiento exigidas para proteger los equipos instalados.	Recursos requeridos: • Un aire Acondicionado de mayor capacidad acorde con el plan de capacidad	• Director de TIC • Coordinador de Operaciones TIC • Profesional de Seguridad de la Información • Proveedor de sistemas de Aire Acondicionado y Extinción de Incendios	Enero a diciembre 2019	Capacitación sobre la importancia de la gestión de capacidades de condiciones ambientales y sistemas de protección contra incendios	Para nuevo equipamiento: • Verificar que se haya adquirido. Para proveedor: • Verificar el cumplimiento de ANS definidos.	Totalmente implementado
Aire Acondicionado	A.8.2.4 Mejoramiento Condiciones Técnicas / Repotenciación Tecnológica • Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización, contar con mecanismos tecnológicos e infraestructura que asegure la disponibilidad y fiabilidad de la información. • Renovar el equipo actual por uno equipo con mayor capacidad. • Adquirir un Sistema de Aire Acondicionado para piso 10	Recursos requeridos: • Un aire Acondicionado de mayor capacidad acorde con lo establecido en el plan de capacidad diseñado. Tanto para centro de cómputo como para centro de cableado	• Director de TIC • Coordinador de Operaciones TIC • Profesional de Seguridad de la Información • Proveedor seleccionado	Enero a diciembre 2019	Capacitar sobre el operación, administración y soporte de los sistemas adquiridos	Para nuevo equipamiento: • Verificar que se haya adquirido. Para proveedor: • Verificar el cumplimiento de ANS definidos	Totalmente implementado

Nombre del activo	Descripción de actividades	Recursos generales y financieros necesarios	Persona responsable	Plazos de inicio y finalización	Programa de capacitación y Sensibiliación	Método para evaluación de resultados	Estado
Bodega de Datos FCM • DWH	A.15.1.3 Cadena de suministro de tecnología de información y comunicación. • Acuerdos con proveedores incluirán requisitos para hacer frente los riesgos de seguridad de información, relacionados con la información y Servicios de tecnología de las comunicaciones y la cadena de suministro de productos. • Implementar un contrato de soporte y mantenimiento con un proveedor que preste servicios de implementación de sistemas TSM • Implementar un contrato de servicio de custodia de medios y poder tener todas las copias en un lugar seguro fuera de las instalaciones físicas de la FCM.	Recursos Requeridos: • Proveedor seleccionado para prestar el servicio requerido de soporte a fallas y plan de migración a nueva versión de TSM. • Licenciamiento de TSM actualizado con suscripción de actualización de versiones y soporte de fábrica sobre producto • Proveedor de servicios de Custodia, transporte, archivo y rearchivo 5 x8 y emergencia 7x24 de medios en Bóveda especializada. • Definición de ANS • Manual de Solicitud de Servicios.	• Director de TIC • Coordinador de Operaciones TIC • Dirección jurídica • Coordinador de operaciones TIC. • Proveedor que preste servicios de instalación, configuración y operación de sistemas TSM. • Proveedor que preste servicios de custodia de medios.	Enero a diciembre 2019	• Capacitación en el procedimiento de Solicitud de Soporte al proveedor. • Concienciar a los funcionarios de TIC sobre la importancia de mantener actualizadas las versiones de software y herramientas informáticas. • Capacitar sobre la importancia de mantener copias de respaldo fuera de la entidad.	• Auditoría y control sobre el contrato prestado. • Medición sobre los ANS prestados por el proveedor. • Auditoria periódicas para asegurar cumplimiento de ANS.	Totalmente implementado
Bodega de Datos FCM • DWH	A.12.6.1 Gestión de vulnerabilidades técnicas. • El Director de TIC es el responsable de supervisar todas las vulnerabilidades de las aplicaciones y de los demás sistemas, y el Profesional de seguridad de la Información debe escoger las medidas que se tomarán en caso que se identifiquen nuevas vulnerabilidades. • Migrar como mínimo a la última versión según la cobertura de la suscripción mediante la cual se compró la versión instalada, asegurar y verificar los respaldos por diversos mecanismos mientras se migra a última versión. • Generar copia de la BD de TSM de manera independiente • Comprobar copias de respaldo de información periódicamente	Recursos Requeridos: • Licenciamiento de la versión del software de TSM que se adquirió con la compra. • Proveedor de servicios especializados en migración de TSM. • Plan de migración • Plataforma de pruebas de recuperación de cintas de respaldo. • Servicio tercerizado para recuperar cinta desde partiendo de la Base de Datos de TSM, con ANS definidos y pruebas de cintas de respaldo	• Director de TIC • Coordinador de Operaciones TIC • Proveedor que preste servicios de custodia de medios. • Jefe Oficina Jurídica • Proveedor de Servicios de Infraestructura de computo	Enero a diciembre 2019	• Capacitación en Instalación, configuración de reglas o políticas de respaldo, administración y mantenimiento del software de TSM versión adquirida. • Concienciar sobre el uso y administración del sistema TSM y cómo implementar políticas de respaldo alineados con la política de seguridad de la información y procedimiento de copias de respaldo.	• Auditoría y control sobre el contrato prestado por terceros. • Auditoria sobre el cumplimiento de las políticas de la seguridad de la información y el procedimiento de backup de la información. • Pruebas de recuperación de copias de seguridad periódicas • Pruebas de recuperación partiendo de la BD de TSM en sitio alterno	Totalmente implementado
Bodega de Datos FCM • DWH	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información • Todos los colaboradores de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concienciación y actualizaciones regulares sobre las políticas y procedimiento de la organización, según sea pertinente para sus funciones laborales. • Establecer procedimiento sobre gestión de las copias de respaldo, reclamación, manejo de cintas removiéndolas de la librería.	Recursos requeridos: • Librería con doble drive • Cartuchos de Cintas para respaldo de datos • Cintas de limpieza de la librería • Plan de mantenimiento de la librería • Procedimiento gestión de cintas de respaldo Abuelo, padre, hijo, full e incremental con copias offsite.	• Director de TIC • Coordinador de Operaciones TIC • Proveedor de servicios especializados en TSM	Enero a diciembre 2019	Capacitación y concienciación sobre la importancia de generar copias de respaldo según las políticas de respaldo por sistema, gestión de cintas fuera de la entidad.	Auditoria de la operación y manipulación de cintas de respaldo.	Totalmente implementado
CCTV/Control de Acceso	A.11.1.3 Seguridad de oficinas, habitaciones e instalaciones • Se debe diseñar y aplicar la seguridad física para recintos e instalaciones. • No se puede acceder a las instalaciones desde áreas públicas y las áreas seguras no son visibles para personas ajenas a la empresa. • Implementar un sistema de CCTV en piso 18 y piso 11 de la FCM	Recursos requeridos: • Cámaras IP 360 Grados, • Cableado • Sistema DVR o NVR • Servicios de implementación.	• Director de TIC • Coordinador de Operaciones TIC • Profesional de Seguridad de la Información • Jefe Administrativa	Enero a diciembre 2019	Plan de capacitación en operación, administración y mantenimiento del DVR o NVR	Para nuevo equipamiento: • Verificar si ha sido comprado y está en uso	Parcialmente implementado
CCTV/Control de Acceso	A.9.1.1 Política de control de acceso • Se debe establecer, documentar y revisar la política de control de acceso con base en los requerimientos del negocio y de la seguridad para el acceso. • Revisar la política y asegurar su cumplimiento	Recursos requeridos: • Revisar la política de control de acceso	• Director de TIC • Coordinador de Operaciones TIC • Profesional de seguridad de la información	Enero a diciembre 2019	Plan de concienciación sobre la importancia de la política de seguridad de la información	Para recurso humano: • Evaluar y auditar que la política se cumple	Parcialmente implementado
CCTV/Control de Acceso	A.9.1.2 Acceso a redes y a servicios de red • Los usuarios únicamente deberán disponer de acceso a la de la red Servicios a la cual están autorizados. • Aplicar las recomendaciones del informe de análisis de vulnerabilidades. Versión CCTV vulnerable acceso escritorio remoto	Recursos requeridos • Especialista en seguridad informática que asegure según recomendación.	• Director de TIC • Coordinador de infraestructura de TIC • Profesional de seguridad de la información	Enero a diciembre 2019	Plan de concienciación al personal de TIC sobre la importancia de asegurar las redes de datos tanto a nivel interno.	Para Aseguramiento de Redes: • Pruebas de vulnerabilidad periódicas y de ataques internos. • Verificación de aplicación de recomendaciones del análisis de vulnerabilidades LAN / WAN	Parcialmente implementado
CCTV/Control de Acceso	A.12.6.1 Gestión de vulnerabilidades técnicas • El Director de TIC es el responsable de supervisar todas las vulnerabilidades de las aplicaciones y de los demás sistemas, y el Profesional de seguridad de la Información debe escoger las medidas que se tomarán en caso que se identifiquen nuevas vulnerabilidades • Activar el Firewall del S.O y bloquear el sistema de accesos remotos	Recursos requeridos: • Gestionar las vulnerabilidades técnicas con un especialista en seguridad informática	• Director de TIC • Profesional de seguridad de la información • Coordinador de infraestructura TIC	Enero a diciembre 2019	Plan para concienciar a los funcionarios TIC y usuarios sobre la importancia de la gestión de vulnerabilidades y bloqueo de servicio vulnerables a accesos remotos	Para procedimientos: • Verificar que se hayan ejecutado. • Realizar de auditoría periódicas.	Parcialmente implementado

Nombre del activo	Descripción de actividades	Recursos generales y financieros necesarios	Persona responsable	Plazos de inicio y finalización	Programa de capacitación y Sensibiliación	Método para evaluación de resultados	Estado
Centro de Cableado	A.11.1.2 Controles físicos de ingreso • El acceso a las áreas seguras de la organización debe estar controlado a través de mecanismos como cámaras de CCTV, sistemas de control de acceso biométrico en entrada de centro de cómputo. • Instalar cámara y control de acceso en entrada del Centro de Cableado	Recursos Requeridos: • Instalar Cámara, cableado, DVR para registro, lectores Biométricos para ingreso y servicios de implementación.	• Director de TIC • Coordinador de Operaciones TIC • Proveedor de Servicios de cableado estructurado y centros de cableado.	Enero a diciembre 2019	Realizar capacitación y concienciación sobre la importancia de las seguridad de la información, monitoreo, diligenciamiento de las bitácoras de acceso al centro de cableado y al mismo tiempo el mantener la organización y las políticas de seguridad en los centros de cableado.	Para nuevo equipamiento: • Verificar si ha sido comprado y está en uso Para documentos: • Revisar que si el contrato del tercero cumple con todo los solicitado por la FCM • Validar Lista de chequeo de entregables • Verificar cumplimiento de políticas • Verificar si han sido redactados y aprobados los documentos de política	Parcialmente implementado
Centro de Cableado	A.11.1.3 Seguridad de oficinas, habitaciones e instalaciones • Se debe diseñar y aplicar la seguridad física para recintos e instalaciones. • Instalar cámara de CCTV dentro del Centro de Cableado	Recursos Requeridos: • Una cámara IP 360 Grados, cableado, DVR, servicios de implementación.	• Director de TIC • Coordinador de Operaciones TIC	Enero a diciembre 2019		Para nuevo equipamiento: verificar si ha sido comprado y está en uso	Totalmente implementado
Centro de Cableado	A.11.1.4 Protección contra amenazas externas y ambientales • Se debe diseñar y aplicar protecciones físicas contra daños por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastres natural o artificial. • Implementar un sistema de protección contra incendios	Recursos Requeridos: • Un sistema de extinción de incendios de acuerdo a la normatividad vigente - tipo agente limpio. • Revisar condiciones y adecuación física.	• Director de TIC • Coordinador de Operaciones TIC	Enero a diciembre 2019	Realizar sesiones de capacitación y concienciación sobre la importancia y uso del sistema de extinción, el mecanismo de uso y los parámetros de seguridad a tener en cuenta.	Para nuevo equipamiento: • Este disponible el manual de uso y las normas de seguridad • Verificar si ha sido comprado y está en uso.	Totalmente implementado
Centro de Cableado	A.11.1.5 Trabajo en áreas seguras • Se debe diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras. • Ajustar los Procedimientos para trabajo en áreas seguras de FCM.	Recursos requeridos: • Los procedimientos o normas necesarias para trabajos en áreas seguras.	• Jefe de Recursos Humanos • Profesional de Salud Ocupacional • Brigadista • Profesional de la Seguridad de Información	Enero a diciembre 2019	Concienciar sobre la importancia del mantener el centro de cableado libre de elementos ajenos al centro de cableado.	Para Recurso Humano: • Llevar bitácora de ingreso con estricto cumplimiento • Verificar que se aplica procedimiento.	Parcialmente implementado
Centro de Cableado	A.11.2.3 Seguridad en el cableado • El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegido contra interceptaciones o daños. • Organizar, marquillar y mejorar cableado de datos, diagramas lógicos de la red de datos.	Recursos requeridos: • Contratar un servicio especializado para organizar el cableado y adecuar las acometidas eléctricas del centro de cómputo.	• Director de TIC • Coordinador de Operaciones TIC • Profesional de Seguridad de la Información. • Proveedor del servicio o si hay un experto interno que lo pueda realizar	Enero a diciembre 2019	Concienciación sobre la importancia de mantener organizado en Centro de Cableado cumpliendo las normas de seguridad	Para el Proveedor: • Verificar el cumplimiento de ANS. • Verificar que sean entregados diagramas de cableado estructurado y organización según las normas básicas de centros de cableado. • Verificar que este organizado y cumpliendo las normas de seguridad.	Totalmente implementado
Centro de Cableado	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información • Todos los colaboradores de la organización y, en su caso, los contratistas deberán recibir educación adecuada conciencia y formación y actualizaciones regulares en las políticas y procedimientos de la organización, como Relevante para su función de trabajo. • Mantener centro de cableado y centro de cómputo libre de elementos ajenos al mismo.	Recursos requeridos: • Consultor en seguridad informática	• Director de TIC • Coordinador de Operaciones TIC • Profesional de Seguridad de la Información. • Jefe de Recursos Humanos	Enero a diciembre 2019	Concienciación sobre la importancia de cumplir las normas de seguridad de la información y protección para mitigar riesgos	Para Recurso Humano: • Ejecutar revisiones periódicas a los sitios • Verificar que se aplica procedimiento.	Parcialmente implementado
Centro de Computo	A.11.1.2 Controles físicos de ingreso • El acceso a las áreas seguras de la organización debe estar controlado a través de mecanismos como cámaras de CCTV, sistemas de control de acceso biométrico en entrada de centro de cómputo. • Instalar cámara y control de acceso en entrada del CC.	Recursos Requeridos: • Instalar Cámara, cableado, un DVR para registro, lectores Biométricos para ingreso y servicios de implementación.	• Director de TIC • Coordinador de Operaciones TIC • Proveedor de Servicios	Enero a diciembre 2019	Realizar sesiones de capacitación y concienciación sobre la importancia de las seguridad de la información, el monitoreo y el diligenciamiento de las bitácoras de acceso	Para nuevo equipamiento: • verificar si ha sido comprado y está en uso. Para documentos: • Verificar si han sido redactados y aprobados los documentos de política. • Validar Lista de chequeo de entregables	Totalmente implementado
Centro de Computo	A.11.1.3 Seguridad de oficinas, habitaciones e instalaciones • Se debe diseñar y aplicar la seguridad física para recintos e instalaciones. • Instalar cámara de CCTV dentro del Centro de Cómputo.	Recursos Requeridos: • Una cámara IP 360 Grados, cableado, DVR, servicios de implementación.	• Director de TIC • Coordinador de Operaciones TIC	Enero a diciembre 2019		Para nuevo equipamiento: verificar si ha sido comprado y está en uso	Totalmente implementado
Centro de Computo	A.11.1.4 Protección contra amenazas externas y ambientales • Se debe diseñar y aplicar protecciones físicas contra daños por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastres natural o artificial. • Implementar un sistema de protección contra incendios tipo agente limpio y revisar condiciones para adecuación física.	Recursos Requeridos: • Un sistema de extinción de incendios de acuerdo a la normatividad vigente - tipo agente limpio. • Servicios de instalación	• Director de TIC • Coordinador de Operaciones TIC	Enero a diciembre 2019	Realizar sesiones de capacitación y concienciación sobre la importancia y uso del sistema de extinción, el mecanismo o parámetros de seguridad a tener en cuenta.	Para nuevo equipamiento: • verificar si ha sido comprado y está en uso. • Este disponible el manual de uso y las normas de seguridad	Totalmente implementado

Nombre del activo	Descripción de actividades	Recursos generales y financieros necesarios	Persona responsable	Plazos de inicio y finalización	Programa de capacitación y Sensibiliación	Método para evaluación de resultados	Estado
Centro de Computo	A.11.1.5 Trabajo en áreas seguras • Se debe diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras. • Ajustar los Procedimientos para trabajo en áreas seguras de FCM, según norma NTC 1700.	Recursos requeridos: • Los necesarios para activar la Brigada de Emergencia mantenerla vigente y hacer simulacros, del plan de evacuación	• Jefe de Recursos Humanos • Profesional de Salud Ocupacional • Brigadista	Enero a diciembre 2019	Socializar, capacitar y concienciar sobre la importancia del plan de evacuación.	Para Recurso Humano: • Hacer evaluación de conocimientos o simulacros no planeados la efectividad del plan de evacuación. • Llevar registro de actividades de la brigada de emergencia	Totalmente implementado
Centro de Computo	A.11.2.3 Seguridad en el cableado • El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegido contra interceptaciones o daños. • Organizar, marquillar el cableado de datos, diagramas lógico y eléctrico.	Recursos requeridos: • Contratar un servicio especializado para organizar el cableado y adecuar las acometidas eléctricas del centro de cómputo.	• Director de TIC • Coordinador de Operaciones TIC • Profesional de Seguridad de la Información. • Proveedor del servicio o si hay un experto interno que lo pueda realizar	Enero a diciembre 2019	Concienciación sobre la importancia de mantener organizado en CC cumpliendo normas de seguridad	• Verificar que este organizado y cumpliendo las normas de seguridad. • Medir y Verificar el cumplimiento de ANS. • Verificar que sean entregados diagramas de cableado y organización y recomendaciones de mantenimiento	Totalmente implementado
Centro de Computo	A.18.2.2. Cumplimiento con las políticas y estándares de seguridad • Todos los propietarios de activos de información, como también la dirección, revisan periódicamente la implementación de los controles de seguridad y el aseguramiento de cumplimiento de estándares. • Definir que normas se pueden aplicar y que nivel aceptable de Centro de Procesamiento es aceptable dentro del marco de seguridad de la información.	Recursos requeridos: Opción 1: Mejorar Centro de Procesamiento: • Un Experto en construcción de CC para identificar que adecuaciones se podrían implementar y que nivel aceptable debería implementarse, con una estimación de costos. • Establecer parámetros de gestión de servicios tercerizados ej. Bonificación / Penalización por ANS.	• Director de TIC • Coordinador de Operaciones TIC • Administrador de Aplicaciones y Bases de Datos • Profesional de Seguridad de la Información • Coordinador de Soporte	Enero a diciembre 2019	• Ejecutar plan de capacitación sobre la importancia de la seguridad y protección de información y el Aseguramiento del cumplimiento de estándares y mantener la organización. • Para Servicios tercerizados: Plan de Capacitación de Gestión de ANS para supervisar su cumplimiento.	Para cambios de infraestructura: • Verificar y monitorear que los servicios prestados están operando correctamente y se haya cumplido los estándares y nivel mínimo definidos por la FCM. Para recurso humano: • Verificar que el centro de cómputo se mantenga con las normas básicas. • Para el Proveedor: Verificar el cumplimiento de ANS.	Totalmente implementado
Centro de Computo	A.8.2.4 Mejoramiento Condiciones Técnicas / Repotenciación Tecnológica Asegurar que la información reciba un nivel adecuado de protección de acuerdo con Su importancia para la organización, contar con mecanismos tecnológicos e infraestructura que asegure la disponibilidad y fiabilidad de la información. • Opción 1: Mejorar las condiciones del centro de cómputo basados en estándares como: TIA 942 o ICREA STD 131 – 2013, • Opción 2: Trasladar el centro de cómputo a un Datacenter externo • Opción 3: Contratar un servicio en la nube, definiendo los ANS y mecanismos de aprovisionamiento en línea.	Recursos requeridos: Opción 1 Mejorar el CC actual: • Contratar un proveedor para que realice las adecuaciones según el nivel de disponibilidad del Datacenter (ej. 95%, 95.5, 96.5% 99%, etc.). • Ampliar el espacio del Centro de Cómputo acorde con el nivel de centro de cómputo a implementar Opción 2 trasladar: el centro de cómputo a un Datacenter externo para soportar los sistemas críticos: Opción 3 contratar un servicio en la nube: • Contratar proveedor de servicios de infraestructura en la nube para que soporte mínimo los sistemas críticos, con definición clara de ANS. Asegurando contingencia	• Director de TIC • Coordinador de Operaciones TIC • Administrador de base de datos • Administrador de Aplicaciones • Profesional de Seguridad de la Información • Coordinador de Soporte	Enero a diciembre 2019	• Ejecutar plan de capacitación para administrar remotamente la infraestructura en Datacenter o en la nube en caso de optar por una de estas opciones. • Crear un programa de Sensibilización para los colaboradores acerca de la administración y operación del centro de cómputo ya sea propio o bajo sistemas tercerizados. • Importancia Aseguramiento del cumplimiento de estándares y mantener la organización. • Para Servicios tercerizados: Plan de Capacitación de Gestión de ANS para supervisar su cumplimiento. Capacitación sobre aprovisionamiento de servicios en la nube.	• Verificar y monitorear que los servicios prestados están operando correctamente y se haya cumplido los estándares mínimos definidos por la FCM. • Medición sobre los ANS prestados por el proveedor.	Totalmente implementado
Equipos de Red	A.12.3.1 Copia de seguridad de la información • Las copias de seguridad de la información, software y sistemas imágenes serán tomado y analizado periódicamente de acuerdo con una copia de seguridad acordado Política. • Realizar una política respecto a las configuraciones de los equipos de red, definiendo su ruta de almacenamiento.	Recursos requeridos: • procedimiento para respaldar las configuraciones de cada equipos de red. • Espacio de almacenamiento	• Director de TIC • Coordinador de Operaciones TIC • Profesional de la seguridad de la información	Enero a diciembre 2019	Sesiones de capacitación y concienciación sobre la importancia de generar copias de respaldo de las configuraciones de cada uno de los equipos de red	Para procedimientos: • Verificar que se ejecuta la política y su almacenamiento • Pruebas periódicas de restauración	Parcialmente implementado
Equipos de Red	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información • Todos los colaboradores de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concienciación y actualizaciones regulares sobre las políticas y procedimiento de la organización, según sea pertinente para sus funciones laborales. • Plan de concienciación sobre la importancia de copiar las configuraciones de los equipos de red	Recursos requeridos: • Un especialista en networking • Aula	• Director de TIC • Coordinador de Operaciones TIC • Profesional de seguridad de la información	Enero a diciembre 2019	Sesiones de capacitación y concienciación sobre la importancia de generar copias de respaldo de cada uno de los equipos de red.	Para procedimiento: • Verificar que fue ejecutado y se cumple con las copias de las configuraciones	Totalmente implementado
Equipos de Red	A.15.1.3 Cadena de suministro de tecnología de información y comunicación • Acuerdos con proveedores incluirán requisitos para hacer frente los riesgos de seguridad de información, relacionados con la información y Servicios de tecnología de las comunicaciones y la cadena de suministro de productos. • Transferir a un tercero el mantenimiento de los equipos de red.	Recursos Requeridos • Proveedor de servicios de mantenimiento de los equipos de red • Un contrato de mantenimiento con ANS definidos	• Director de TIC • Coordinador de Operaciones TIC • Profesional de Seguridad de la Información • Proveedor seleccionado • Dirección Jurídica	Enero a diciembre 2019		Para el Proveedor: • Verificar que se cumplen los ANS definidos. • Verificar que los equipos están cubiertos por el contrato de mantenimiento.	Totalmente implementado

Nombre del activo	Descripción de actividades	Recursos generales y financieros necesarios	Persona responsable	Plazos de inicio y finalización	Programa de capacitación y Sensibiliación	Método para evaluación de resultados	Estado
Firewall	A.12.6.1 Gestión de vulnerabilidades técnicas • La información de las vulnerabilidades técnicas de los sistemas de información que se utiliza se obtendrá en el momento oportuno, la exposición de la organización a este tipo de vulnerabilidades es evaluada y las medidas adecuadas son adoptadas para hacer frente al riesgo asociado. • Implementar un sistema Firewall en Activo / Pasivo según las reglas de configuración basadas en el análisis de vulnerabilidades de LAN / WAN y las políticas de seguridad de la FCM.	Recursos Requeridos: • Dos firewall (Actualmente disponibles en FCM - Dell Sonic Wall NSA 3600) • Disponibilidad de espacio en rack. • Energía y condiciones ambientales óptimas. • Servicio especializado para configurar el firewall	• Director de TIC • Coordinador de Operaciones TIC • Proveedor que preste servicios STS. • Profesional de Seguridad de la Información	Enero a diciembre 2019	Capacitación en instalación configuración, administración y operación del sistema de firewall Dell Sonic Wall implementados en las oficinas FCM.	Auditoría y control sobre el contrato prestado.	Totalmente implementado
Firewall	A.15.1.3 Cadena de suministro de tecnología de información y comunicación. • Acuerdos con proveedores incluirán requisitos para hacer frente los riesgos de seguridad de información, relacionados con la información y servicios de tecnología de las comunicaciones y la cadena de suministro de productos. • Implementar un contrato de soporte y mantenimiento con un proveedor que preste servicios de seguridad Firewall y redes.	Recursos requeridos: • Proveedor seleccionado para prestar el servicio requerido	• Director de TIC • Coordinador de Operaciones TIC • Dirección jurídica • Proveedor que preste servicios de instalación, configuración y operación de sistemas seguridad, firewall y redes.	Enero a diciembre 2019	Capacitación en el procedimiento de solicitudes de soporte técnico y atención a fallas.	• Auditoria y control sobre el contrato prestado. • Medición sobre los ANS prestados por el proveedor	Totalmente implementado
Firewall	A.8.2.4 Mejoramiento Condiciones Técnicas / Repotenciación Tecnológica. • Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización, contar con mecanismos tecnológicos e infraestructura que asegure la disponibilidad y fiabilidad de la información. • Implementar dos canales de acceso a internet cada uno con un proveedor diferente y con diferente acometida y salida internacional (interactúa con todos los servicios y activos informáticos de FCM, que lo demanden)	Recursos requeridos: • Proveedores de internet. • Configuración del direccionamiento IP con los respectivos proveedores de internet. • Configuración de los dominios con los respectivos proveedores de internet. • Plan de redirecionamiento ante contingencia	• Director de TIC • Coordinador de Operaciones TIC • Dirección jurídica • Profesional de seguridad de la información • Proveedor de internet	Enero a diciembre 2019	Capacitación en el procedimiento de solicitudes de soporte técnico y atención a fallas	• Auditoria y control sobre el contrato prestado. • Medición sobre los ANS prestados por los proveedores • Pruebas periódicas de contingencia	Totalmente implementado
Servicio de Voz	A.12.6.1 Gestión de vulnerabilidades técnicas. •El Director de TIC es el responsable de supervisar todas las vulnerabilidades de las aplicaciones y de los demás sistemas, y el Profesional de seguridad de la Información debe escoger las medidas que se tomarán en caso que se identifiquen nuevas vulnerabilidades. • Actualizar a la última versión del sistema Elastix, adicionalmente deben tener configurado las políticas de seguridad para sistemas de telefonía IP.	Recursos Requeridos: • Instalar el software última versión 2.4.0 de Elastix. • Configurar políticas de seguridad sobre sistemas IP • Teléfonos IP que soporten protocolo SIP • Softphones SIP • ATA (Adaptadores Terminales Analógicos) y todos ellos que soporten protocolo SIP.	• Director de TIC • Coordinador de Operaciones TIC • Profesional de la seguridad de la información • Proveedor que preste servicios de instalación, configuración y operación de sistemas de telefonía IP Sobre Software Libre como Asterisk y Elastix	Enero a diciembre 2019	• Capacitación en instalación configuración, administración y operación del sistema de telefonía IP con Elastix última versión. • Capacitación sobre seguridad de telefonía IP sobres protocolos SIP • Concienciación sobre manejo de copias de respaldo de las configuraciones sistema y tarificación.	• Auditorias periódicas sobre la actualización del sistema de Software de IP PBX. Así como asegurar y restaurar copias de respaldo de la información (configuración, log, registro de llamadas, tarificación) y revisión de los protocolos de seguridad del mismo (firewall interno). • Auditoría y control sobre el contrato prestado.	Totalmente implementado
Servicio de Voz	A.15.1.3 Cadena de suministro de tecnología de información y comunicación • Acuerdos con proveedores incluirán requisitos para hacer frente los riesgos de seguridad de información, relacionados con la información y servicios de tecnología de las comunicaciones y la cadena de suministro de productos. • Implementar un contrato de soporte y mantenimiento con un proveedor que preste servicios de telefonía IP sobre sistemas libres como Asterisk y Elastix.	Recursos Requeridos: • Proveedor seleccionado para prestar el servicio requerido • Definir los ANS	• Director de TIC • Coordinador de Operaciones TIC • Dirección jurídica • Proveedor que preste servicios de instalación, configuración y operación de sistemas de telefonía IP Sobre Software Libre como asterisk y Elastix	Enero a diciembre 2019	Realizar capacitación en el procedimiento de solicitudes de soporte y atención a fallas y medición de ANS del mismo.	• Auditoria y control sobre el contrato prestado. • Medición sobre los ANS prestados por el proveedor.	Totalmente implementado
Servicio de Voz	A.8.2.4 Mejoramiento Condiciones Técnicas / Repotenciación Tecnológica • Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización, cuenta con mecanismos que aseguren su disponibilidad. • Implementación de dos nuevos servidores de telefonía IP uno en funcionamiento y el otro de respaldo, con última versión del sistema Elastix, adicionalmente deben tener configurado las políticas de seguridad para sistemas de telefonía IP y todos los servicios (fax, extensiones análogas y salida de llamadas a celular) que tienen actualmente con la planta Panasonic TDA- 200 al sistema de telefonía IP Elastix.	Recursos Requeridos: • Teléfonos IP que soporten protocolo SIP • Softphones SIP • ATA (Adaptadores Terminales Analógicos) y todos ellos que soporten protocolo SIP. • Dos servidor con las siguientes especificaciones mínima RAM 8 GB, dos (2) Discos de 1TB, R1, última versión del software Elastix (PBX IP) • 4 Balun de conexión • 2 tarjetas PCI de E1 para las troncales SIP. • Servicios de instalación y configuración y soporte	• Director de TIC • Coordinador de Operaciones TIC • Dirección jurídica • Proveedor que preste servicios de instalación, configuración y operación de sistemas de telefonía IP Sobre Software Libre como Asterisk y Elastix • Profesional de seguridad de la información	Enero a diciembre 2019	Capacitación sobre la configuración operación, administración y mantenimiento de los nuevos servicios implementados en el sistema de telefonía IP.	Auditoria y control sobre el contrato prestado.	Totalmente implementado
Servicio de Voz	A.5.1.1 Políticas para seguridad de la información. • Brindar orientación y apoyo a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y leyes pertinentes. • Elaborar una política seguridad de la información sobre los sistemas de telefonía IP.	Recursos Requeridos: • Documentación de vulnerabilidades sobre sistemas de telefonía IP. • Especialista de telefonía IP.	• Director de TIC • Coordinador de Operaciones TIC. • Profesional de seguridad de la información • Especialista de telefonía IP.	Enero a diciembre 2019	• Capacitación sobre la política de seguridad de la información. • Capacitación sobre la vulnerabilidades sobre sistemas de telefonía IP	Auditoria periódica sobre la política de la seguridad de la información.	Planificado

Nombre del activo	Descripción de actividades	Recursos generales y financieros necesarios	Persona responsable	Plazos de inicio y finalización	Programa de capacitación y Sensibiliación	Método para evaluación de resultados	Estado
Sistema Antivirus	A.12.7.1 Controles de auditoría sobre los sistemas de información • Requisitos y actividades relacionadas con la verificación de las operaciones de auditoría sistemas deberán ser cuidadosamente planificadas y acordadas para reducir al mínimo Interrupciones en los procesos de negocio y sus sistemas informáticos que los soportan. • Aseguramiento de aplicación de políticas de seguridad y actualización de antivirus.	Requisitos requeridos: • Planificar auditorías internas / externas • Auditores internos / externos	• Director de TIC • Coordinador de Operaciones TIC • Profesional de Seguridad de la Información • Jefe de Control Interno	Enero a diciembre 2019	Concienciar sobre la importancia de las auditorias	Para procedimientos: • Verificar ejecución de las auditorias • Gestionar las acciones preventivas y correctivas	Totalmente implementado
Sistema Antivirus	A.18.2.1 Revisión independiente de la seguridad de la información • El enfoque de la organización para la gestión de seguridad de la información y su puesta en práctica (es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se revisarán de forma independiente a intervalos planificados o cuando ocurran cambios significativos. • Formalizar la revisión periódica de la política de seguridad de la información	Recursos requeridos: • Revisar la política de seguridad de la información, en cuanto a protecciones contra software malicioso	• Director de TIC • Profesional de Seguridad de la Información • Jefe de Control Interno	Enero a diciembre 2019	Plan de concienciación a los colaboradores para proteger información contra software malicioso	Para procedimientos y políticas: • Asegurar su cumplimiento	Totalmente implementado
UPS	A.12.6.1 Gestión de vulnerabilidades técnicas • La información de las vulnerabilidades técnicas de los sistemas de información que se utiliza se obtendrá en el momento oportuno, la exposición de la organización a este tipo de vulnerabilidades es evaluada y las medidas adecuadas son adoptadas para hacer frente al riesgo asociado. • Revisar si es factible Instalarle a las UPS el sistema de monitoreo por medio de un protocolo SNMP (Simple Network Management Protocol).	Recurso requerido • Consultar al fabricante de las UPS si es factible implementar sistema de monitoreo SNMP. • Tarjeta de monitoreo compatible a la UPS	• Director de TIC • Profesional de seguridad de la información • Coordinador de infraestructura TIC	Enero a diciembre 2019		Para procedimiento: • Verificar que la actualización fue realizada	Parcialmente implementado
UPS	A.8.2.4 Mejoramiento Condiciones Técnicas / Repotenciación Tecnológica • Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización, contar con mecanismos tecnológicos e infraestructura que asegure la disponibilidad y fiabilidad de la información. • Cambiar las UPS por unas de mayor capacidad con redundancia de componentes N+1 equivalentes y/o con la misma asignación y capacidad.	Recursos requeridos • UPS que tengan la capacidad correspondiente al 70% del factor de carga máximo medio de todos los componentes del sistema. • Instalación y adecuación del espacio a ser instaladas	• Director de TIC • Profesional de seguridad de la información • Coordinador de infraestructura TIC • Proveedor de las UPS	Enero a diciembre 2019	Capacitación sobre operación, administración y mantenimiento de UPS	Para equipamiento nuevo: • Verificar que se compraron los equipos y están instalados.	Totalmente implementado

Elaborado por: Harol Méndez Collo	**Aprobado por: Alejandro Murillo Pedroza**
Cargo: Profesional Oficial de Seguridad Informática	**Cargo: Director Técnico - Dirección de Tecnologias de la Información**
Firma: *ORIGINAL FIRMADO*	**Firma:** *ORIGINAL FIRMADO*
Lugar y Fecha: Bogotá 31 de Enero de 2019	**Lugar y Fecha: Bogotá 31 de Enero de 2019**