Informe de auditoría interna

CONTROLES ISO 27002:2013

December 11, 2020

# **Objetivo de la auditoría**

Evaluar la madurez de la seguridad de la información en la empresa basado en el nivel de cumplimiento de los 114 controles definidos en el estándar ISO/IEC 27002:2013 y siguiendo el Modelo de Madurez de la Capacidad (CMM).

## **Objetivos específicos**

* Determinar el nivel de madurez para cada uno de los 114 controles de la ISO27002.
* Determinar el nivel de madurez para cada uno de los dominios de la ISO27002.
* Identificar posibles brechas que permitan identificar acciones a implementar para mejorar el nivel de madurez de la seguridad de la información.

# **Alcance de la auditoría**

Como parte de la auditoría se da alcance a los 114 controles definidos en el estándar ISO/IEC27002:2013, los cuales se encuentran divididos en 14 dominios:

* Política de Seguridad de la Información
* Organización de la Seguridad de la Información
* Seguridad en los Recursos Humanos
* Gestión de los activos
* Control de Acceso
* Criptografía
* Seguridad Física y del Entorno
* Seguridad de las Operaciones
* Seguridad de las Comunicaciones
* Adquisición, Desarrollo y Mantenimiento de Sistemas
* Relaciones con los Proveedores
* Gestión de incidentes de Seguridad de la Información
* Aspectos de seguridad de la información de la Gestión de Continuidad de Negocio
* Cumplimiento

# **Criterios de la auditoría**

La evaluación de madurez de los controles se realizó siguiendo el Modelo de Madurez de la Capacidad (CMM):

|  |  |  |  |
| --- | --- | --- | --- |
| **EFECTIVIDAD** | **CMM** | **SIGNIFICADO** | **DESRIPCIÓN** |
| **0%** | **L0** | Inexistente | Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver. |
| **10%** | **L1** | Inicial / Ad-hoc | Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo. |
| **50%** | **L2** | Reproductible, pero intuitivo | Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo |
| **90%** | **L3** | Proceso definido | La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento. |
| **95%** | **L4** | Gestionado y medible | Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia. |
| **100%** | **L5** | Optimizado | Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos. |

# **Metodología de la auditoría**

La metodología empleada para el desarrollo de la auditoría consiste en una primera fase de revisión documental para posteriormente realizar entrevistas con los dueños o responsables de cada uno de los controles y una visita a las instalaciones administrativas y centros de datos y cableado. Con base en las evidencias obtenidas durante las dos primeras fases se documentan las no conformidades y oportunidades de mejoras las cuales serán socializadas en la reunión de cierre de la auditoría.

# **Desarrollo de la auditoría**

La auditoría se realizo del 30 de noviembre de 2021 al 11 de diciembre del mismo año. Durante este tiempo se solicitó y revisó la documentación referente a la gestión de seguridad de la información y a los controles implementados, así mismo, se realizaron entrevistas con los dueños de la implementación y operación de los 114 controles.

**Documentación revisada:**

* Política de Seguridad de la Información
* Manual de gestión de Seguridad de la Información
* Estructura organizacional de seguridad de la información
* Manual de administración de personal
* Contrato de trabajo
* Cláusulas de información y confidencialidad
* Plan de capacitación de Seguridad de la Información 2021
* Presentación Inducción Corporativa
* Curso E-learning Seguridad de la Información
* Catálogo de aplicaciones y activos de tecnología
* Tablas de Retención documental TRD
* Procedimiento Gestión de medios removibles
* Procedimiento de Control de Acceso
* Procedimiento de Seguridad Física
* Contrato proveedor de equipos de computo
* Procedimiento Gestión de Cambios
* Procedimiento gestión de incidentes de SI
* Formatos incidentes de seguridad de la información
* Procedimiento de copias de respaldo
* Procedimiento para el control de software
* Procedimiento Gestión de Vulnerabilidades
* Procedimiento de Seguridad para redes de comunicación
* Procedimiento para la transferencia de información
* Manual de Continuidad de Negocio
* Evaluación de Riesgos de Continuidad de Negocio
* Análisis de Impacto al Negocio BIA

**Entrevistas realizadas:**

* Chief Information Security Officer (CISO)
* Oficial de Protección de Datos
* Líder de Comunicaciones y Servicios TI
* Coordinador de Tecnologías de la Información
* Coordinador de Infraestructura Tecnológica
* Coordinador de Continuidad de Negocio
* Coordinador de Seguridad Física
* Coordinador de Selección

**Visitas realizadas**

* Instalaciones físicas administrativas
* Centro de datos y cableado

El equipo de auditoria estuvo conformado por dos auditores con experiencia en sistemas de gestión de seguridad de la información, certificados como auditores líderes ISO27001:2013 quienes fueron los responsables de ejecutar cada una de las fases definidas y consolidar el informe de resultados.

# **Resultados de la auditoría**

## **No conformidades**

A continuación, se relacionan las no conformidades identificadas durante la auditoría respecto al cumplimiento de los controles ISO/IEC 27002:

| **Hallazgo** | **Evidencia** | **Requisito** | **Recomendación** | **Fecha Implementación** | **Responsable** |
| --- | --- | --- | --- | --- | --- |
| **Desactualización de la política de seguridad de la información.**  La Política de Seguridad de la Información fua actualizada por última vez en el año 2016, por lo cual no se encuentra alineada con el plan estratégico actual de la empresa. | * Política de Seguridad de la Información * Manual de gestión de Seguridad de la Información | A.5.1.2 Revisión de las políticas de seguridad de la Información | Actualizar la política de seguridad de la información asegurando su alineación con el plan estratégico de la empresa. | Febrero 2021 | Chief Information Security Officer (CISO) |
| **Alcance limitado en la definición de roles y responsabilidades para la gestión de seguridad de la información.**  Se han definido roles para la gestión de seguridad de la información asignando responsabilidades, sin embargo, no se contemplan todos los involucrados en la gestión de seguridad de la información. | * Manual de gestión de Seguridad de la Información * Estructura organizacional de seguridad de la información | A.6.1.1 Roles y responsabilidades en Seguridad de la Información | Realizar un análisis detallado de las áreas de la empresa que están involucradas con la gestión de seguridad de la información, para así, realizar la actualización de la estructura y establecer claramente los roles y responsabilidades de cada uno de los miembros de la estructura de seguridad de la información. | Febrero 2021 | Chief Information Security Officer (CISO) |
| **No se realiza segregación de funciones para los responsables de seguridad de la información.**  Se ha definido una matriz de segregación de funciones para los procesos de la empresa, sin embargo, no se realiza un análisis detallado respecto a las funciones de los responsables de seguridad de la información. | * Manual de gestión de Seguridad de la Información * Estructura organizacional de seguridad de la información | A.6.1.2 Separación de deberes | Realizar un análisis detallado que permita establecer las funciones actuales de los responsables de seguridad, de tal forma, que se realice una segregación de funciones para asegurar que no se asignen más permisos de los requeridos. | Febrero 2021 | Chief Information Security Officer (CISO) |
| **Ausencia de un procedimiento de contacto con las autoridades y grupos de interés.**  No se ha documentado un procedimiento de contacto con las autoridades y grupos de interés que establezca las acciones que deben ser ejecutadas al presentarse un incidente de seguridad de la información. | * Manual de gestión de Seguridad de la Información * Procedimiento gestión de incidentes de SI | A.6.1.3 Contacto con las autoridades  A.6.1.4 Contacto con grupos de interés especial | Documentar, formalizar y gestionar la aprobación y publicación de un procedimiento que establezca las acciones que deben ser ejecutadas para mantener contacto con las autoridades y grupos de interés en caso de presentarse un incidente de seguridad de la información. | Febrero 2021 | Chief Information Security Officer (CISO) |
| **Ausencia de un lineamiento y/o procedimientos de gestión de seguridad de la información para proyectos.**  Para nuevos proyectos, se revisan aspectos de seguridad de la información teniendo en cuenta la naturaleza del proyecto, sin embargo, no existen lineamiento al respecto. | No existe documentación | A.6.1.5 Seguridad de la información en proyectos | Definir y documentar los lineamientos de seguridad de la información y procedimientos que deben ser aplicados al definirse un nuevo proyecto de cualquier naturaleza, no solo, para proyectos de seguridad de la información. | Marzo 2021 | Chief Information Security Officer (CISO) |
| **Ausencia de una política para uso de dispositivos móviles.**  Se han implementado medidas de seguridad para el uso de dispositivos móviles, sin embargo, no se tiene documentación formal, así como tampoco se cuenta con una política que establezca los lineamientos frente al uso de dispositivos móviles en la empresa. | No existe documentación | A.6.2.1 Política de Dispositivo Móvil | Definir una política para el uso de dispositivos móviles en la empresa, que establezca claramente en qué casos esta autorizado el uso de dispositivos móviles, así como, cuales son los lineamientos y controles que se deben aplicar para el uso de estos dispositivos dentro de la red corporativa. | Abril 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Ausencia de una política y/o procedimiento de teletrabajo.**  Actualmente no se ha trabajado en la definición de una política y un procedimiento de teletrabajo, sin embargo, se esta realizando teletrabajo por parte de los empleados. | No existe documentación | A.6.2.2 Teletrabajo | Definir, documentar y gestionar la aprobación de una política y procedimiento de teletrabajo, donde se establezcan los lineamientos y controles que deben ser aplicados para el teletrabajo por parte de los empleados.  La definición de los controles a aplicar deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual esta definido iniciar en enero de 2021. | Mayo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **No se evidencia cumplimiento de las responsabilidades asignadas a la Alta Dirección.**  Como parte de la Política de Seguridad de la Información, se asigna la responsabilidad a la Alta Dirección de velar por su cumplimiento, sin embargo, no se evidencia el compromiso de la Alta Dirección respecto a la revisión de cumplimiento, actualización y aprobación de la misma. | * Política de Seguridad de la Información * Manual de gestión de Seguridad de la Información | A.7.2.1 Responsabilidades de la dirección | Realizar campañas de capacitación a Alta Dirección referentes a sus responsabilidades frente a la gestión de seguridad de la información.  Establecer como aspecto de revisión durante los comités de gerencia, los avances frente a la gestión de seguridad de la información en la empresa. | Enero 2021 | Chief Information Security Officer (CISO) |
| **No se aplican procesos disciplinarios ante el incumplimiento de la política de seguridad de la información.**  Como parte de la Política de Seguridad de la Información, se definen procesos disciplinarios como sanción por su incumplimiento. No se evidencia que se realice un análisis respecto al cumplimiento de la política por parte de los empleados. | * Política de Seguridad de la Información * Manual de gestión de Seguridad de la Información | A.7.2.3 Proceso disciplinario | Definir los criterios que deben ser tenidos en cuenta para determinar el cumplimiento de la política de seguridad de la información por parte de los empleados, así mismo, se debe definir la periodicidad con la cual se realizará la revisión de dichos criterios. En caso de identificar casos de incumplimiento se deberán aplicar los procesos disciplinarios definidos en la política. | Enero 2021 | Chief Information Security Officer (CISO) |
| **Ausencia de una política y procedimiento para la gestión de activos.**  Como parte de la Política de Seguridad de la Información se habla acerca del uso aceptable de los activos de información, sin embargo, no se tienen definidos lineamientos específicos. Adicionalmente, se cuenta con un inventario de activos de la empresa, donde se relacionan algunos de los activos asociados con información, para algunos de estos activos se tiene claramente identificados los propietarios. | * Política de Seguridad de la Información * Manual de gestión de Seguridad de la Información * Catálogo de aplicaciones y activos de tecnología | A.8.1.1 Inventario de Activos  A.8.1.2 Propiedad de los activos  A.8.1.3 Uso aceptable de los activos  A.8.1.4 Devolución de activos | Definir, documentar y gestionar la aprobación de una política la cual establezca claramente los lineamientos para el uso aceptable de los activos de información.  Definir, documentar y socializar un procedimiento de gestión de activos con base en los lineamientos dados en la política. | Abril 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Ausencia de un procedimiento para la clasificación y etiquetado de la información.**  Se han definido niveles de clasificación para la información personal, sin embargo, no se contemplan niveles diferentes a los definidos en la Ley 1581. Actualmente no se realiza etiquetado de la información. No existe documentación formal de los niveles de clasificación definidos. | * Manual de gestión de Seguridad de la Información * Tablas de Retención documental TRD | A.8.2.1 Clasificación de la información  A.8.2.2 Etiquetado y manejo de la información  A.8.2.3 Manejo de activos | Definir, documentar y socializar un procedimiento para la clasificación y etiquetado de la información. Como parte, del procedimiento se debe contemplar:   * Niveles de clasificación de toda la información corporativa. * Etiquetas que se deben aplicar de acuerdo con el nivel de clasificación. * Controles que se deben aplicar de acuerdo con los niveles de clasificación. | Junio 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **No se aplica el procedimiento para la disposición de medios.**  Se tiene definido un procedimiento para la disposición de medios, sin embargo, no se evidencia que sean aplicados por el proveedor que realiza cambios de los equipos de cómputo. | * Manual de gestión de Seguridad de la Información * Procedimiento Gestión de medios removibles | A.8.3.2 Disposición de los medios | Evaluar los acuerdos contractuales con el fin de asegurar que el proveedor que realiza los cambios de equipos de cumplimiento al procedimiento establecido. | Enero 2021 | Coordinador de Tecnologías de la Información |
| **Deficiencias en la definición de la política para transferencia de información.**  Se tiene definida una política para la transferencia de información, teniendo en cuenta que no se realiza clasificación de la información no se aplican controles de acuerdo con la criticidad de la información transmitida. | * Manual de gestión de Seguridad de la Información | A.8.3.3 Transferencia de los medios físicos  A.13.2.1 Política y procedimientos de transferencia de información  A.13.2.3 Mensajería electrónica | Con base en el procedimiento de clasificación y etiquetado de información, actualizar la política de transferencia de información, así mismo, definir y documentar un procedimiento donde se establezcan los controles que se deben aplicar para la transferencia de información de acuerdo con su nivel de clasificación. | Agosto 2021 | Coordinador de Tecnologías de la Información |
| **Deficiencia en la definición de controles de acceso a los sistemas de información y servicios de red.**  Se tiene definida una Política de control de acceso donde se dan los lineamientos para sistemas de información y servicios en red, sin embargo, no se evidencia una definición formal de los controles que deben ser implementados. No obstante, se evidencia que se tienen implementados controles de acceso | * Manual de gestión de Seguridad de la Información * Procedimiento de Control de Acceso | A.9.1.1 Política de control del acceso  A.9.1.2 Acceso a redes y a servicios en red  A.9.1.2 Acceso a redes y a servicios en red  A.9.4.1 Restricción de acceso a la información  A.9.4.2 Procedimiento de ingreso seguro  A.14.1.1 Análisis y especificación de los requisitos de seguridad de la información | Con base en los niveles de clasificación de la información se debe revisar los controles implementados actualmente y determinar la necesidad de implementar nuevos o ajustar con los existentes, así mismo, se deben identificar los controles que deben ser aplicados para el acceso a la red corporativa y servicios en red.  Una vez definidos los controles de acceso, se deben documentar los procedimientos correspondientes con el fin de especificar las actividades que deben ser ejecutadas para su correcta operación.  La definición de los controles a aplicar deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Abril 2021 | Coordinador de Tecnologías de la Información |
| **Deficiencias en la definición del procedimiento para la creación, modificación y eliminación de cuentas de usuario.**  Se evidencia la ejecución de procedimiento para la creación, eliminación y modificación de cuentas de usuario el cual es responsabilidad del área de Tecnología y Talento Humano. No existe documentación formal del procedimiento. | * Manual de gestión de Seguridad de la Información | A.9.2.1 Registro de usuarios y cancelación del registro de usuarios  A.9.2.2 Suministro de acceso de usuarios  A.9.2.3 Gestión de derechos de acceso privilegiado  A.9.2.4 Gestión de información de autenticación secreta de usuarios  A.9.2.5 Revisión de los derechos de acceso de usuarios  A.9.2.6 Retiro o ajuste de los derechos de acceso | Definir, documentar y formalizar el procedimiento para la creación, modificación y eliminación de cuentas de usuario. Como parte del procedimiento se deben contemplar la asignación de contraseñas de usuario y el proceso de notificación por por parte del área de Talento Humano cada vez que ingrese, se retire o se cambie de área a un empleado. | Marzo 2020 | Coordinador de Tecnologías de la Información |
| **Ausencia de un sistema para la gestión de contraseñas.**  Se cuenta con una aplicación para la generación de contraseñas de manera aleatoria. Sin embargo, no se evidencia que las aplicaciones estén configuradas para solicitar la configuración de contraseñas con los parámetros definidos en la política de control de acceso. Así mismo, no se evidencia un software para la custodia de contraseñas de administración. | * Manual de gestión de Seguridad de la Información | A.9.4.3 Sistema de gestión de contraseñas | Implementar un software para la custodia de contraseñas de administrador.  Configurar las aplicaciones de tal forma, que al realizar los cambios de contraseñas se solicite que cumpla con los parámetros definidos en la política de control de acceso.  La definición de los controles a aplicar deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Junio 2021 | Coordinador de Tecnologías de la Información |
| **Uso de programas utilitarios.**  No se evidencia la definición e implementación de controles que restrinjan el uso de programas utilitarios o las excepciones de uso. | No existe documentación | A.9.4.4 Uso de programas utilitarios privilegiados | Definir, documentar y formalizar un procedimiento que restrinjan el uso de programas utilitarios, como parte del procedimiento se deben contemplar las excepciones y los procesos que se deben seguir para la autorización de instalación de estos programas.  La definición de los controles a aplicar deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Mayo 2021 | Coordinador de Tecnologías de la Información |
| **Deficiencias en los controles de acceso a códigos fuentes de programas.**  No se evidencia la definición de controles de acceso al código fuente. | No existe documentación | A.9.4.5 Control de acceso a códigos fuente de programas | Definir, implementar y documentar los controles de acceso que deben ser aplicados al código fuente de los programas con base en los roles y funciones de los empleados.  La definición de los controles a aplicar deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Junio 2021 | Coordinador de Tecnologías de la Información |
| **Deficiencias en la definición de controles criptográficos.**  Se evidencia que se cuenta con controles criptográficos los cuales han sido implementados a demanda. No existe documentación formal. | No existe documentación. | A.10.1.1 Política sobre uso de controles criptográficos  A.10.1.2 Gestión de llaves  A.18.1.5 Reglamentación de los controles criptográficos | Definir una política de uso de controles criptográficos. Con base en la política definir, documentar e implementar un procedimiento para el uso de controles criptográficos que considere los lineamientos para el uso de llaves criptográficas.  La definición de los controles a aplicar deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Junio 2021 | Coordinador de Tecnologías de la Información |
| **20**  **Deficiencias en la definición de controles de seguridad física.**  Se tienen definidos controles de seguridad física, sin embargo, no existe una identificación formal de las áreas seguras de trabajo y los controles que se deben aplicar en las zonas de carga. | * Manual de gestión de Seguridad de la Información * Procedimiento de Seguridad Física | A.11.1.1 Perímetro de seguridad física  A.11.1.2 Controles de acceso físicos  A.11.1.3 Seguridad de oficinas, recintos e instalaciones  A.11.1.4 Protección contra amenazas externas y ambientales  A.11.1.5 Trabajo en áreas seguras  A.11.1.6 Áreas de despacho y carga | Definir, documentar e implementar un procedimiento de seguridad física que contemple:   * Controles para áreas donde se maneja información confidencial. * Perímetros de seguridad. * Controles de acceso a las instalaciones para empleados y terceros. * Controles contra desastres naturales. * Controles que deben ser aplicados en las áreas de carga. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Seguridad Física |
| **Deficiencias en la implementación de controles para el cableado.**  Se cuenta con controles de acceso físico a los cuartos de cableado. Los racks se encuentran desorganizados, lo que puede llegar a generar consecuencias en el cableado. Para los cables que llegan a los puestos de trabajo no se tienen implementadas medidas de seguridad. | No existe documentación | A.11.2.3 Seguridad del cableado | Implementar controles de protección física para los cables que llegan a los puestos de trabajo.  Definir un proyecto que permita cablear los racks de manera organizada teniendo en cuenta los servicios de conexión para cada rack. | Abril 2021 | Chief Information Security Officer (CISO)  Coordinador de Infraestructura Tecnológica |
| **Deficiencias en los controles de seguridad aplicados a los equipos de cómputo fuera de las instalaciones.**  Actualmente los empleados pueden retirar los equipos de cómputo de las instalaciones, el único control implementado es la planilla de ingreso y retiro de portátiles ubicada en la recepción del edificio.  No se tienen controles para proteger la información almacenada en los equipos de cómputo. | * Manual de gestión de Seguridad de la Información | A.11.2.5 Retiro de activos  A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones | Definir, documentar y formalizar un procedimiento para el retiro de equipos de computo y uso fuera de las instalaciones.  Se deben definir controles para los equipos de computo con base en la clasificación de la información que almacena. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Deficiencias en la aplicación del procedimiento para la disposición de medios.**  Se tienen definidos procedimiento para la disposición de medios, sin embargo, no se evidencia que sean aplicados por el proveedor que realiza cambios de los equipos de cómputo. | * Manual de gestión de Seguridad de la Información | A.11.2.7 Disposición segura o reutilización de equipos | Aplicar los acuerdos contractuales al proveedor con el fin de garantizar el cumplimiento del procedimiento para la disposición de medios.  Asignar una persona responsable de realizar seguimiento al proveedor cada vez que se realice un cambio de equipo con el fin de garantizar que el proceso se cumpla a cabalidad. | Febrero 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Inexistencia de una política de escritorio y pantalla limpia.**  No se evidencia la definición de una política de escritorio limpio. | * Manual de gestión de Seguridad de la Información | A.11.2.9 Política de escritorio limpio y pantalla limpia | Definir, documentar y gestionar la aprobación de una política que establezca los lineamientos para no conservar información confidencial en los puestos de trabajo, así mismo, se debe aplicar el uso de pantalla limpia. | Marzo 2021 | Chief Information Security Officer (CISO) |
| **Deficiencias en la documentación de los procedimientos de seguridad de la información.**  Se tienen definidos procedimientos respecto a seguridad de la información, sin embargo, no se han documentado formalmente. Las personas que los ejecutan actualmente son quienes tienen el conocimiento. | * Manual de gestión de Seguridad de la Información | A.12.1.1 Procedimientos de operación documentados | Definir, documentar y publicar todos los procedimientos referentes a la gestión de seguridad de la información. Los procedimientos deben ser socializados con los responsables de su operación. | Mayo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Deficiencias en el comité de cambios.**  Se tiene definido un comité de cambios, solo para algunos casos se ponen en consideración aspectos de seguridad de la información, previo a la ejecución del cambio. El responsable de seguridad de la información solo es citado al comité en casos específicos. | * Manual de gestión de Seguridad de la Información * Procedimiento Gestión de Cambios | A.12.1.2 Gestión de cambios | Estructurar adecuadamente el comité de cambios, de tal forma, que se involucre al CISO como miembro activo del comité y cada cambio sea analizado desde el punto de vista de seguridad de la información. | Febrero 2021 | Chief Information Security Officer (CISO)  Líder Comité de Cambios |
| **Inexistencia de un procedimiento para el análisis de capacidades.**  No se realiza un análisis de las capacidades requeridas para el desempeño óptimo de los sistemas. | No existe documentación | A.12.1.3 Gestión de capacidad | Definir, documentar y formalizar un procedimiento para el análisis de capacidades que contemple el seguimiento al uso de los recursos y proyección de los requisitos futuros con base en la evolución de la plataforma tecnológica.  La definición del procedimiento deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Abril 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Inexistencia de documentación formal respecto a la separación de ambientes de desarrollo.**  Existe una separación de los ambientes de desarrollo, pruebas y producción a los cuales tienen acceso únicamente los empleados que por sus funciones lo requieran. | * Manual de gestión de Seguridad de la Información. | A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación | Documentar formalmente los controles que han sido aplicados para mantener los ambientes de desarrollo separados. | Febrero 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Inexistencia de documentación de los controles contra código malicioso definidos.**  Se han definido e implementado controles contra código malicioso. No se cuenta con documentación formal acerca de la operación de dichos controles. | * Manual de gestión de Seguridad de la Información * Procedimiento gestión de incidentes de SI | A.12.2.1 Controles contra códigos maliciosos | Documentar formal los controles que han sido implementados contra código malicioso, como parte de su documentación se debe contemplar: la forma en que son operados dichos controles, los responsables de su operación, la periodicidad de revisión que permita identificar posibles ajustes en cuanto a su operación.  Los controles implementados deberán ser revisados con el fin de asegurar la alineación con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Junio 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información  Coordinador de Infraestructura Tecnológica |
| **Deficiencias en el procedimiento de copias de respaldo.**  Se tiene definido un procedimiento para la generación de copias de respaldo, sin embargo, no se tiene definida la criticidad de la información para así determinar el tipo de backup que se debe realizar, de igual forma, como parte del procedimiento no se contempla pruebas de restauración. | Procedimiento de copias de respaldo | A.12.3.1 Respaldo de la información | Revisar y actualizar las políticas de backup teniendo en cuenta la clasificación de la información.  Definir un plan de pruebas en el cual se realicen pruebas periódicas de restauración de las copias realizadas.  La definición del procedimiento deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. |  | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Deficiencias en el proceso de registro de eventos.**  No se tiene controles definidos para proteger la información del registro. Así mismo, no se tiene habilitado el registro de eventos de usuarios administradores, por capacidad de almacenamiento en los servidores. | No existe documentación | A.12.4.2 Protección de la información del registro  A.12.4.3 Registros de administrador y de operador | Habilitar el registro de eventos para usuarios administradores para los sistemas de mayor criticidad para la empresa, los cueles deben estar integrados con n un correlacionador de eventos que genere alertas oportunas sobre comportamientos inusuales. De igual forma, se debe definir que roles deben tener acceso a estos registros y garantizar que los controles de acceso se configuren correctamente.  La definición del procedimiento deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Junio 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Deficiencias en la definición de controles para proteger la información.**  Se ha trabajado en la implementación de algunos controles para proteger la información almacenada en sistemas de información, debido a que no existe una clasificación de la información, no se han determinado los controles de acuerdo con el nivel de criticidad de la información. Así mismo, se evidencia la implementación de controles para asegurar la transmisión de información, sin embargo, no se ha realizado un análisis respecto a los controles que deben ser implementados de acuerdo con la criticidad de la información. | * Manual de gestión de Seguridad de la Información | A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas  A.14.1.3 Protección de transacciones de los Servicios de las aplicaciones | Revisar los controles que han sido implementados para determinar la necesidad de implementar nuevos controles que aseguren la confidencialidad e integridad de la información que es transmitida por redes públicas.  La definición de los controles a aplicar deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Junio 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Inexistencia de un procedimiento para el control de cambios en sistemas.**  No se establece un procedimiento para el control de cambios durante el ciclo de vida de desarrollo de software. | * Manual de gestión de Seguridad de la Información | A.14.2.2 Procedimiento de control de cambios en sistemas | Definir, documentar y formalizar un procedimiento que permita revisar, registrar y aprobar los cambios que se requieran para cada uno de los sistemas de la empresa. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Inexistencia de un procedimiento de revisión de la construcción y cambios de software.**  Cuando se realizan cambios significativos en cuanto a las plataformas que soportan la operación crítica, se realiza un análisis de aspectos de seguridad de la información y continuidad de negocio, sin embargo, no tiene definido un procedimiento formal que debe ser aplicado. De igual forma, no se tienen claramente definidos los aspectos de seguridad de la información que deben ser evaluados para la construcción y modificación del software. | * Manual de gestión de Seguridad de la Información | A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación  A.14.2.4 Restricciones en los cambios a los paquetes de software  A.14.2.5 Principios de construcción de los sistemas seguros | Definir, documentar y formalizar un procedimiento que contemple:   * Los principios de seguridad de la información que deben ser tenidos en cuenta para la construcción de nuevos sistemas. * Proceso de revisión respecto a seguridad de la información que se debe realizar a los sistemas una vez se hayan realizado cambios en sus funcionalidades. * Restricciones de cambios para sistemas.   Los controles implementados deberán ser revisados con el fin de asegurar la alineación con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Deficiencias en los requerimientos de seguridad de la información para el software desarrollado por terceros.**  Actualmente no se realiza un seguimiento de requerimientos de seguridad de la información para el desarrollo de software contratado con terceros. | * Manual de gestión de Seguridad de la Información | A.14.2.7 Desarrollo contratado externamente | Definir, documentar y formalizar un procedimiento donde se establezcan los controles de seguridad de la información que deben ser implementados por los terceros durante el desarrollo de software.  El procedimiento definido deberá ser revisado con el fin de asegurar la alineación con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Inexistencia de un procedimiento de pruebas para paso a producción de los sistemas.**  Los requisitos de seguridad de la información no son contemplados dentro de los requisitos iniciales del desarrollo de software. Como parte de las pruebas de aceptación se evalúan aspectos de seguridad de la información. No existe documentación formal del proceso que se deba seguir. | * Manual de gestión de Seguridad de la Información | A.14.2.8 Pruebas de seguridad de sistemas  A.14.2.9 Prueba de aceptación de sistemas | Definir, documentar y formalizar un procedimiento en el cual se establezca la definición de requisitos de seguridad de la información desde la fase de diseño del software hasta las pruebas para aprobación del paso a producción. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Inexistencia de un lineamiento para la protección de datos de prueba.**  No se han realizado definiciones para la protección de datos de prueba. | * Manual de gestión de Seguridad de la Información | A.14.3.1 Protección de Datos de Prueba | Establecer un política y procedimiento respecto a los controles que deben ser implementados para asegurar la confidencialidad de los datos que son utilizados durante las fases de desarrollo y pruebas de nuevos sistemas.  La definición de los controles a aplicar deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Inexistencia de controles de seguridad de la información para terceros.**  Se contemplan aspectos de seguridad de la información asociados a la operación por parte de terceros durante los procesos de contratación, como son cláusulas de confidencialidad respecto a la información a la cual tendrán acceso. No se evidencia una documentación formal de los requisitos de seguridad que deben cumplir los terceros. | * Cláusulas de información y confidencialidad | A.15.1.1 Política de seguridad de la información para las relaciones con los proveedores  A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores  A.15.1.3 Cadena de suministro de tecnología de información y comunicación | Definir, documentar y formalizar un procedimiento que contemple los controles de seguridad de la información que deben cumplir los terceros de acuerdo con el servicio a prestar a la empresa. | Abril 2021 | Chief Information Security Officer (CISO) |
| **Inexistencia de auditorías a terceros para verificar el cumplimiento de los requisitos de seguridad de la información.**  Teniendo en cuenta la criticidad de los servicios prestados por el proveedor, se realiza un análisis del impacto generado respecto a seguridad de la información para los cambios propuestos. No se tiene documentado un procedimiento. No se realizan auditorías de seguridad de la información a los servicios contratados con terceros. | No existe documentación | A.15.2.1 Seguimiento y revisión de los servicios de los proveedores  A.15.2.2 Gestión de cambios en los servicios de los proveedores | Definir y ejecutar un plan de auditoría orientado a los servicios que han sido contratados con terceros. Como parte del plan se debe establecer los requisitos de seguridad de la información que deberán ser revisados para cada proveedor. | Marzo 2021 | Chief Information Security Officer (CISO) |
| **Deficiencias en la definición de los requisitos de seguridad de la información a los cuales se debe dar cumplimiento.**  Se tienen definidos y documentados los requisitos legales de seguridad de la información a los cuales debe dar cumplimiento a empresa. No se ha realizado un análisis detallado del cumplimiento para cada una de las normativas aplicables. No se tienen claramente identificados los requisitos contractuales a los cuales se debe dar cumplimiento. | * Manual de gestión de Seguridad de la Información | A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales | Definir, documentar y formalizar un procedimiento el cual contemple la revisión periódica de requerimientos legales, normativos y contractuales respecto a seguridad de la información, así como, la definición de métricas que permitan establecer el nivel de cumplimiento respecto a los requerimientos aplicables. | Febrero 2021 | Chief Information Security Officer (CISO) |
| **Inexistencia de un procedimiento para determinar el cumplimiento respecto al licenciamiento de software.**  No se tiene definido un procedimiento que permita establecer el nivel de cumplimiento respecto al licenciamiento de software utilizado en la empresa. | * Manual de gestión de Seguridad de la Información | A.18.1.2 Derechos de propiedad intelectual (DPI) | Definir, documentar y formalizar un procedimiento que contemple la revisión de software instalado en los equipos de cómputo, el análisis de software autorizado y no autorizado y las acciones que deben ser ejecutadas para dar total cumplimiento a la Ley de Propiedad Intelectual. | Abril 2021 | Chief Information Security Officer (CISO) |
| **Inexistencia de un procedimiento para la revisión periódica de la gestión de seguridad de la información.**  No se tiene definido un procedimiento que asegure revisiones periódicas que permitan determinar el nivel de cumplimiento de los requisitos de seguridad de la información. | No existe documentación | A.18.2.1 Revisión independiente de la seguridad de la información  A.18.2.2 Cumplimiento con las políticas y normas de seguridad  A.18.2.3 Revisión del cumplimiento técnico | Definir, documentar y formalizar un procedimiento para la revisión periódica de la gestión de seguridad de la información que determine el nivel de cumplimiento. Como parte del procedimiento se deben establecer los responsables de la revisión donde se debe involucrar a Alta Dirección. | Marzo 2021 | Chief Information Security Officer (CISO) |

## **Oportunidades de mejora**

A continuación, se relacionan las oportunidades de mejora identificadas durante la auditoría respecto al cumplimiento de los controles ISO/IEC 27002:

| **Oportunidad de mejora** | **Evidencia** | **Requisito** | **Recomendación** | **Fecha Implementación** | **Responsable** |
| --- | --- | --- | --- | --- | --- |
| **Debilidades frente a la definición y aplicación de los planes de capacitación.**  Anualmente se definen planes de capacitación y sensibilización, sin embargo, estos planes no son definidos con base en las necesidades de seguridad de la información identificadas. No se evidencia el cumplimiento de los planes definidos. | * Plan de capacitación de Seguridad de la Información 2021 * Presentación Inducción Corporativa * Curso E-learning Seguridad de la Información | A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información | Definir los planes de capacitación y sensibilización con base en las necesidades de seguridad de la información identificadas durante el año anterior.  Establecer un responsable de realizar seguimiento periódico y asegurar el cumplimiento de los planes definidos. | Enero 2021 | Chief Information Security Officer (CISO) |
| **No existe un procedimiento para la revocación de accesos a sistemas de información y redes corporativas.**  Se tienen definidos y documentados los procedimientos para la desvinculación o cambio de funciones de un empelado, sin embargo, no se contemplan aspectos respecto a los accesos a sistemas de información y redes corporativas. | * Manual de administración de personal * Paz y Salvo Empleados | A.7.3.1 Terminación o cambio de responsabilidades de empleo | Incluir como parte del procedimiento de desvinculación o cambio de empleados, la revisión y revocación de accesos a sistemas de información y redes corporativas. | Febrero 2021 |  |
| **Exceso de excepciones para la habilitación de puertos USB.**  Se tiene definida y documentada una política para el uso de medios removibles en la cual se establece que todos los equipos de cómputo deben tener deshabilitados los puertos USB, sin embargo, actualmente existen excepciones para el 85% de empleados. | * Manual de gestión de Seguridad de la Información * Procedimiento Gestión de medios removibles * Registro de excepciones USB en el Directorio Activo | A.8.3.1 Gestión de los medios removibles | Revisar y actualizar la asignación de excepciones de habilitación de puertos USB.  Revisar y actualizar la política para el uso de medios removibles con el fin de asegurar que no se asignen excepciones para un gran porcentaje de empleados. | Febrero 2021 | Coordinador de Tecnologías de la Información |
| **Incumplimiento de los lineamientos respecto al uso de información de autenticación.**  Como parte de las cláusulas de información y confidencialidad se dan lineamiento respecto al uso de información de autenticación secreta, sin embargo, se evidencia que los empleados no dan cumplimiento a cabalidad. | * Cláusulas de información y confidencialidad | A.9.3.1 Uso de información de autenticación secreta | Realizar campañas de sensibilización para todos los empleados respecto a los lineamientos definidos para el uso de información de autenticación.  Realizar auditorías en campo que permitan determinar el nivel de incumplimiento respecto al control para aplicar los procesos disciplinarios definidos en el apolítica de seguridad de la información. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Ausencia de controles contra desastres naturales en las instalaciones.**  Se cuenta con controles de acceso físico a cada uno de los pisos donde se encuentran las estaciones de trabajo, sin embargo, no se evidencian detectores de incendio en los pisos. No se cuenta con documentación formal. | No existe documentación | A.11.2.1 Ubicación y protección de los equipos | Documentar el procedimiento de seguridad física con base en los controles definidos e implementados.  Considerar la necesidad de contratar detectores de incendio en los pisos donde se encuentran ubicados los equipos de cómputo. | Agosto 2021 | Chief Information Security Officer (CISO)  Coordinador de Seguridad Física |
| **Deficiencias en la asignación de responsabilidades de uso de las plantas eléctricas.**  Se cuenta con plantas eléctricas, sin embargo, no existe una asignación formal frente a la administración de estas. | No existe documentación | A.11.2.2 Servicios de suministro | Asignar formalmente la responsabilidad de administración, mantenimiento y uso de las plantas eléctricas con las que cuenta la empresa actualmente. | Enero 2021 | Chief Information Security Officer (CISO)  Coordinador de Seguridad Física |
| **Ausencia de mantenimiento preventivo para los equipos de cómputo.**  Como parte del contrato de adquisición de equipos se incluye una cláusula en la cual se especifica que se debe realizar mantenimiento preventivo a los equipos de cómputo y servidores, sin embargo, solo se está realizando mantenimiento correctivo. | * Contrato proveedor de equipos de computo | A.11.2.4 Mantenimiento de equipos | Aplicar los acuerdos contractuales con el proveedor con el fin de realizar mantenimiento preventivo a los equipos de cómputo para así prevenir posibles fallos. | Febrero 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Deficiencias en la aplicación de la política de bloqueo de sesión.**  Se tiene definida una política de bloqueo de sesión la cual se aplica por Directorio Activo, el tiempo de inactividad configurado son 10 minutos. No se evidencia la cultura de bloqueo de sesión al retirarse del puesto de trabajo, así mismo, se evidencia, que el bloque de sesión automáticamente no se aplica en todos los equipos de acuerdo con la política configurada. | * Manual de gestión de Seguridad de la Información | A.11.2.8 Equipos de usuarios desatendido | Actualizar la política de bloqueo de sesión configurada en el Directorio Activo de tal forma que se aplique para todos los equipos de cómputo.  Definir campañas de sensibilización para todos los empleados respecto a la importación de bloquear los equipos cada vez que se retiran de sus puestos. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **No se realiza una revisión de los logs generados.**  Para los sistemas de información más críticos se tiene habilitado el registro de eventos, sin embargo, no se realiza una revisión automatizada que permita generar alertas acerca de comportamientos que puedan representar un riesgo de seguridad de la información. | * Manual de gestión de Seguridad de la Información | A.12.4.1 Registro de eventos | Integrar los logs con un correlacionador de eventos con el fin de generar alertas oportunas sobre comportamientos que puedan representar un riesgo de seguridad de la información.  La definición de los controles a aplicar deberá estar alineado con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Junio 2021 | Coordinador de Infraestructura Tecnológica |
| **Inexistencia de un procedimiento para la sincronización de relojes en los servidores.**  Los relojes de los servidores se encuentran sincronizados, sin embargo, no existe documentación acerca de la fuente de referencia utilizada, así como tampoco un lineamiento asociado. | * Manual de gestión de Seguridad de la Información | A.12.4.4 Sincronización de relojes | Documentar formalmente el procedimiento que se aplica para asegurar que los relojes de los servidores se encuentren sincronizados. | Enero 2021 | Coordinador de Infraestructura Tecnológica |
| **Exceso de excepciones en la asignación de permisos de administrador.**  Se tiene restringidos los permisos de administrador en los equipos de usuario con el fin de no permitir la instalación de software, sin embargo, se ha evidenciado que el 60% de los empleados tiene excepción de usuario administrador. | * Manual de gestión de Seguridad de la Información * Procedimiento para el control de software | A.12.5.1 Instalación de software en sistemas operativos  A.12.6.2 Restricciones sobre la instalación de software | Revisar las excepciones asignadas para permisos de administrador con el fin de evaluar la necesidad de asignar dicha excepción, de esta forma, se restringe la instalación de software en los equipos de cómputo.  Los controles implementados deberán ser revisados con el fin de asegurar la alineación con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Junio 20221 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Ausencia de métricas que permitan establecer la efectividad de los controles implementados.**  Se tienen definidos, implementados y operando controles para garantizar la seguridad en la red. Los procedimientos correspondientes a los controles implementados se encuentran documentados, sin embargo, no se han establecido métricas o revisiones periódicas que permitan determinar la necesidad de implementar acciones de mejora. | * Manual de gestión de Seguridad de la Información * Procedimiento de Seguridad para redes de comunicación | A.13.1.1 Controles de las redes  A.13.1.2 Seguridad de los servicios de red  A.13.1.3 Separación en las redes | Definir métricas que permitan medir la efectividad de los controles implementados periódicamente de tal forma que se identifiquen oportunidades de mejora respecto a los controles.  Los controles implementados deberán ser revisados con el fin de asegurar la alineación con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Marzo 2021 | Líder de Comunicaciones y Servicios TI |
| **Ausencia de una política el desarrollo de software.**  No existe una política de desarrollo seguro, sin embargo, como parte del Procedimiento para la adquisición, instalación, actualización y eliminación de software se establecen lineamientos respecto al análisis de código de software que va a ser adquirido. | * Manual de gestión de Seguridad de la Información * Procedimiento para la adquisición, instalación, actualización y eliminación de software | A.14.2.1 Política de desarrollo seguro | Evaluar la necesidad de implementar una política que establezca claramente los lineamientos respecto al desarrollo seguro.  Los lineamientos dados deberán ser revisados con el fin de asegurar la alineación con la implementación del proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” el cual está definido iniciar en enero de 2021. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información |
| **Deficiencias en el proceso de mejora continua para la gestión de incidentes de seguridad de la información.**  Se cuenta con un Procedimiento de gestión de incidentes de seguridad de la información aprobado y publicado, en el cual se establecen los criterios que deben ser evaluados para determinar si la situación presentada debe ser clasificada como un incidente de seguridad de la información. De igual forma, se definen las acciones a ejecutar para dar respuesta a incidente, sin embargo, no se tienen claramente definidos los responsables de ejecutar cada una de las acciones definidas. Así mismo, se establecen las acciones a ejecutar posterior a la atención del incidente para así identificar oportunidades de mejora. Como parte del procedimiento se contempla el proceso de recolección de evidencias el cual es realizado por un tercero, así como también, se contempla los medios de reporte que están habilitados para que los empleados y terceros notifiquen situaciones inseguras respecto a seguridad de la información. El procedimiento también contempla indicadores para medir la gestión de incidentes en la empresa, sin embargo, no se evidencia la definición de acciones de mejora respecto a los resultados de las mediciones realizadas. | * Procedimiento gestión de incidentes de SI * Formato incidentes de seguridad de la información | A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información | Establecer como parte del procedimiento de gestión de incidentes de seguridad de la información la definición de acciones de mejora con base en los resultados de las mediciones realizadas y los resultados obtenidos ante la materialización de incidentes. | Marzo 2021 | Chief Information Security Officer (CISO)  Coordinador de Tecnologías de la Información  Coordinador de Infraestructura Tecnológica |
| **Inexistencia de criterios para determinar la criticidad de los sistemas.**  Se han definido esquemas de redundancia de acuerdo con la criticidad de los sistemas de información. No existe documentación formal del análisis realizado ni los parámetros tenidos en cuenta para determinar la criticidad de los sistemas. | No existe documentación | A.17.2.1 Disponibilidad de instalaciones de procesamiento de información | Definir y documentar formalmente los criterios que son evaluados para determinar la criticidad de los sistemas de información para así definir los sistemas que requieren esquemas de lata redundancia. | Abril 2021 | Coordinador de Continuidad de Negocio  Coordinador de Tecnologías de la Información |

# **Conclusiones**

Como parte de la auditoría se identificaron 42 no conformidades y 15 oportunidades de mejora:

* Se dio cumplimiento al objetivo planteado para la auditoría en la cual se revisó el diseño y operación de los 114 controles definidos en el estándar ISO/IEC27002.
* Se evidencio compromiso por parte de la organización en cuanto a la implementación de los controles. Se han tenido avances significativos respecto a su implementación, sin embargo, es necesario reforzar el diseño e implementación de los controles con base en las recomendaciones dadas.
* Con el proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios” se evidencia una optimización en cuanto a la implementación de los controles, es necesario, que las políticas y procedimientos definidas sean ajustadas con base en el proyecto.
* Se requiere definir e implementar un plan de auditoría con el fin de realizar revisiones periódicas respecto al diseño e implementación de los controles para así asegurar su correcto funcionamiento o identificar oportunidades de mejora para implementar acciones oportunamente.