**MEMORANDO**

Código 150

Bogotá D.C., julio de 2022

PARA: Dr. Felipe Jiménez Ángel
**Secretario Distrital de Gobierno**

DE: Jefe Oficina de Control Interno

ASUNTO: Informe de seguimiento a la verificación del cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, en la entidad comparado con la normatividad asociada a la ISO/IEC 27001 de 2013.

En cumplimiento de las funciones establecidas en la Ley 87 de 1993, del Plan Anual de Auditorías 2022, y del Decreto 648 de 2017 específicamente del Rol de evaluación y seguimiento, atentamente me permito remitir el informe de seguimiento a la verificación del cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, en la entidad comparado con la normatividad asociada a la ISO/IEC 27001 de 2013, con el fin de que sea socializado con su equipo de trabajo analizando su contenido y se tomen las respectivas acciones de mejora que a su consideración apliquen para el proceso evaluado.

Esta evaluación se da a conocer al señor Secretario en cumplimiento de lo dispuesto en el Decreto 338 de 2019 *"Por el cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción ARTÍCULO 1 PARÁGRAFO 1. Los informes de auditoría, seguimientos y evaluaciones tendrán como destinatario principal el representante legal de la entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva, y deberán ser remitidos al nominador cuando este lo requiera".*

De otra parte, me permito informar que el informe en mención se comunicó a la Dirección de Tecnologías e Información con comunicación No 20221500242723, se encuentra publicado en la página web https://www.gobiernobogota.gov.co/transparencia/control/reportes-control-interno-sgd

Finalmente, agradecemos la disposición y colaboración de sus equipos de trabajo durante el proceso de evaluación, reiterando nuestro compromiso de asesoría y acompañamiento a todos los procesos de la Entidad.

Cordial saludo,

(ORIGINAL FIRMADO)
**LADY JOHANNA MEDINA MURILLO**
Jefe Oficina de Control Interno

Anexo: Informe de seguimiento del cumplimiento y el grado de implementación del MSPI.

Revisó: Claudia Ochoa-Contratista de la OCI
Aprobó: Johana Murillo-Jefe de la OCI

# MEMORANDO

Código 150

Bogotá D.C., julio de 2022

PARA: Dr. Orlando Benavides Santacruz
**Dirección de Tecnologías e Información**

DE: Jefe Oficina de Control Interno

ASUNTO: Informe de seguimiento al cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, en la SDG comparado con la normatividad asociada a la ISO/IEC 27001 de 2013.

En desarrollo del Plan Anual de Auditorías 2022, el Decreto 1078 de 2015 y dando cumplimiento a los roles de enfoque hacia la prevención y de evaluación y seguimiento establecidos en el Artículo 17 del Decreto 648 de 2017, se programó y realizó seguimiento al cumplimiento seguimiento a la verificación del cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, en la entidad comparado con la normatividad asociada a la ISO/IEC 27001 de 2013. En este sentido, se remite el informe de seguimiento en archivo anexo.

1. **Objetivo:** Verificar el cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, en la entidad comparado con la normatividad asociada a la ISO/IEC 27001 de 2013. Así mismo, la documentación asociada al dueño del proceso.

2. **Alcance:** Se verifican la información, manuales, procesos y procedimientos que se tienen en la Dirección de Tecnologías de la Información de la SDG orientados a la implementación y el grado de cumplimiento del MSPI de la vigencia 2021.

Agradecemos la disposición y oportuna atención del proceso de auditoría y acciones orientadas a atender las recomendaciones presentadas.

Cordial saludo,

(ORIGINAL FIRMADO)
**LADY JOHANNA MEDINA MURILLO**
Jefe Oficina de Control Interno

Anexo: Informe de seguimiento del cumplimiento y el grado de implementación del MSPI

Revisó: Claudia Ochoa-Contratista de la OCI
Aprobó: Johana Murillo-Jefe de la OCI

Informe de seguimiento al cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, en la SDG comparado con la normatividad asociada a la ISO/IEC 27001 de 2013.

**Destinatarios**

- Dr. Felipe Jiménez Angel – Secretario Distrital de Gobierno.
- Dr. Orlando Benavides Santacruz- Dirección de Tecnologías e Información

## 1. Objetivos

### 1.1 Objetivo general

Verificar el cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, en la entidad comparado con la normatividad asociada a la ISO/IEC 27001 de 2013. Así mismo, la documentación asociada al dueño del proceso.

## 2. Alcance

El presente informe corresponde a la verificación de la información, manuales, procesos y procedimientos que se tienen en la Dirección de Tecnologías de la Información de la SDG orientados a la implementación y el grado de cumplimiento del MSPI de la vigencia 2021 y primer semestre de 2022.

## 3. Marco normativo o criterios del informe

Norma Externa:

- Decreto 1078 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*
- Decreto 1008 de 2018 *""Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*
- Resolución 500 de 2021, *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital"*.
- Resolución 001519 de 24 de agosto de 2020*, "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"*
- Norma ISO/IEC 27001 - Norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información.
- Manual para la Implementación de la Política de Gobierno Digital Versión 7 de abril de 2019
- CONPES 3854 de abril del 2016, Política de Seguridad Digital.

Norma Interna:

- Resolución 0236 de 2019
- GDI-TIC-M004 Manual de Gestión de Seguridad
- GDI-TIC-M006 Manual de Política de Tecnología e Información

- GDI-TIC-PL003 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

**4. Equipo auditor:**

Claudia Ximena Ochoa Angel- Contratista Oficina de Control Interno.
Lady Johana Medina Murillo-Jefe de la Oficina de Control Interno

**5. Metodología**

La Oficina de Control Interno solicitó a Dirección de Tecnologías e Información mediante memorando radicado No 20221500218053 del 12 de julio de 2022 la información que se relaciona a continuación:

- Indicar quien es el líder y/o responsable de seguridad de la información
- Mapa de Proceso
- Políticas de seguridad de la información formalizada y firmada
- Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.
- Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección
- Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección
- Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección
- Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)
- Procedimientos de control documental del MSPI
- Metodología de Gestión de riesgos
- Riesgos identificados y valorados de acuerdo con la metodología
- Planes de tratamiento de los riesgos
- Formatos de acuerdos contractuales para establecer responsabilidades de las partes en seguridad de la información
- Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.
- Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información
- Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección
- Inventario de áreas de procesamiento de información y telecomunicaciones
- Diagrama de red de alto nivel o arquitectura de TI
- Inclusión de la seguridad de la información en la gestión de proyectos
- Inventario de partes externas o terceros a los que se transfiere información de la entidad
- Formato de acuerdo de transferencia de información
- Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden
- Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.

- Plan de continuidad de la Secretaría Distrital de Gobierno aprobado
- Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información
- Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.
- Indicadores y métricas de seguridad de la información definidos.
- Declaración de aplicabilidad
- Aceptación de los riesgos residuales por parte de los dueños de los riesgos
- Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
- Avance en la ejecución del plan de tratamiento de riesgos
- Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.
- Política y medidas de seguridad de soporte, para proteger la información que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
- Política y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles
- Metodología de gestión de riesgos para protección de datos personales, herramienta identificación y gestión de riesgos a los datos personales, plan de tratamiento de riesgos de datos personales documentado.
- Política y procedimientos implementados de gestión de incidentes de seguridad de la información personal
- Proceso disciplinario formal para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. Medios de divulgación y comunicación del proceso.
- Política, procedimiento, o instructivo que permita realizar la gestión de la identificación, actualización y reporte de nuevas bases de datos con información personal a la SIC
- Proceso de gestión de usuarios para el acceso a las Bases de Datos
- Conforme a las evidencias aportadas en qué fase se encuentra la Secretaría de Gobierno (Implementación, Evaluación, o Mejora Continua).

La Dirección de Tecnologías e Información remitió respuesta a la solicitud realizada mediante memorando interno 20224400225893 del 19 de julio de 2022.

Se programó reunión con la Dirección de Tecnologías e Información por Microsoft Teams el 21 de julio con la participación de los profesionales a cargo de la implementación del Modelo MSPI. La verificación de las evidencias y documentación observada se validó mediante muestra selectiva de auditoría a registros y soportes el grado de avance conforme a los controles asociados a la implementación del Sistema de Gestión de Seguridad de la Información en la entidad basado en la norma ISO27001 de 2013, y el MSPI del MINTIC.

La entrevista se realizó a los siguientes profesionales de la Dirección de Tecnologías e Información:

- Rodrigo Hernández Cuenca- Profesional especializado
- Luis Alejandro Vargas Ruiz- Profesional especializado
- Ruth Lady Arias Rodríguez- Profesional especializado

- Nelson Mauricio Parada Botia- Profesional especializado
- Olga Milena Arias Aguirre-Profesional universitario
- José Leonardo Carrillo Cortes-Contratista

Dando cumplimiento a los roles de enfoque hacia la prevención y de evaluación y seguimiento establecidos en el Artículo 17 del Decreto 648 de 2017, la Oficina de Control Interno a partir de los soportes allegados, realizó una serie de recomendaciones frente al cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC.

## 6. Periodo de ejecución

1 al 31 de Julio de 2022

## 7. Desarrollo

Para realizar el análisis en relación con los controles asociados a la implementación del Sistema de Gestión de Seguridad de la Información en la SDG basado en la norma ISO27001 de 2013, y el MSPI del MINTIC se tomó como herramienta independiente por parte de esta oficina un tablero de seguimiento por dimensiones para validar el desarrollo de cada uno de los componentes.

En la fase de diagnóstico el ciclo de la operación para la implementación del MSPI se inicia con la identificación de un análisis preliminar a partir del cual se logra establecer el nivel de madurez y cumplimiento actual acerca de la gestión de seguridad de la información realizada en DTI de la SDG. Razón por la cual se ha implementado el instrumento diseñado por el MINTIC denominado Identificación de la línea base de seguridad, el cual tiene como propósito evaluar la efectividad de los controles conforme a los estándares internacionales según la ISO 27001.

En este sentido, se identifican los factores internos como: los procedimientos, estructura tecnológica, los factores externos como la competencia y proveedores con el objetivo de analizar las necesidades de la entidad para gestionar adecuadamente la información tanto interna como de las partes interesadas. Lo que permitirá en la fase de implementación contar con un modelo de gestión de seguridad de la información que aplique métodos seguros y efectivos que controlen y limiten el acceso a la información y a los sistemas que procesan las estrategias que tienen como punto esencial la implementación de políticas, controles de seguridad y de acceso lógico y los procedimientos para detectar amenazas que puedan producir vulnerabilidades y que se ponga el riesgo los activos de información. Teniendo con objetivo final proteger tanto la información como a los sistemas que almacenan y se administran en la SDG.

Con el fin de evaluar la brecha en que la entidad se encuentra para llegar a cumplir totalmente los requerimientos del modelo se validaron los requerimientos de la norma se realizaron entrevistas por medio de Microsoft Teams, análisis, revisión de la información, por lo cual se presenta por cada dominio el estado de implementación y aplicación de los controles consolidados.

En consecuencia, se validó la herramienta (Archivo anexo) con las siguientes convenciones para interpretar los resultados obtenidos.

**Herramienta:** VERIFICACIÓN SGSI, CONTROLES DE LA NORMA ISO 27001, IMPLEMENTACION SEGURIDAD DE LA INFORMACION EN DTI DE LA SDG.

| Estado | Descripción |
|---|---|
| Cumple satisfactoriamente | Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. |
| Cumple parcialmente | Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió, pero no se gestiona. |
| No cumple | No existe y/o no se está haciendo. |
| No aplica | El control no es aplicable para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad. |

| POR DOMINIO DE CONTROL | | | | | |
|---|---|---|---|---|---|
| NOMBRE DOMINIOS DE CONTROL | CONTROLES QUE APLICAN | IMPLEMENTADOS | PARCIALMENTE | NO CUMPLE | NO APLICA |
| DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN | 2 | 1 | 0 | 1 | 0 |
| DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 7 | 0 | 4 | 3 | 0 |
| DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS | 6 | 2 | 3 | 1 | 0 |
| DOMINIO 8 - GESTIÓN DE ACTIVOS | 10 | 0 | 7 | 3 | 0 |
| DOMINIO 9 - CONTROL DE ACCESO | 14 | 0 | 4 | 10 | 0 |
| DOMINIO 10 - CRIPTOGRAFÍA | 2 | 0 | 1 | 1 | 0 |
| DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO | 15 | 10 | 1 | 4 | 0 |
| DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES | 14 | 0 | 8 | 6 | 0 |
| DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES | 7 | 0 | 4 | 3 | 0 |
| DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 13 | 2 | 7 | 4 | 0 |
| DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES | 5 | 0 | 0 | 5 | 0 |
| DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 7 | 0 | 2 | 5 | 0 |
| DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO | 4 | 0 | 0 | 4 | 0 |
| DOMINIO 18 - CUMPLIMIENTO | 8 | 0 | 2 | 6 | 0 |
| | 114 | 15 | 43 | 56 | 0 |

*En el anexo 1 se puede observar con detalle por cada control de las evidencias verificadas y el estado evidenciado en el análisis realizado, con el fin de verificar el grado de cumplimiento de los requerimientos exigidos en la norma ISO 27001. Los resultados se consolidan por medio de tablas de niveles de cumplimiento. Para cada dominio u objetivo de control, se presentan las recomendaciones.

**8. Hallazgos, Observación o Recomendación (Cuando aplique)**

Conforme a las auditorías que se han realizado en la SDG a la implementación del MSPI se reiteran algunos hallazgos que se han evidenciado y se relacionan algunas novedades conforme a la entrevista realizada el 21 de julio al equipo de profesionales responsables de la implementación. Esto con el fin de realizar el tránsito de la fase de diagnóstico a la fase de implementación y evaluación.

**Ausencia en la gestión efectiva de:**

1. **Análisis de vulnerabilidades** en concordancia al control 12.7 de la Norma ISO 27001 y la Guía del Sistema de Gestión de la Seguridad de la Información del MINTIC.

   La Dirección de Tecnologías de la Información no cuenta con el documento de análisis de vulnerabilidades debidamente desarrollado por lo cual se hace necesario para la correcta construcción de la implementación del SGSI al interior de la entidad. En el documento se deben identificar los daños y las consecuencias para la entidad que podrían causar mediante un incidente descritos como amenazas asociadas a vulnerabilidades en los activos de información.

   Es importante tener presente que el objetivo de implementar este mecanismo es la detección temprana y proactiva de vulnerabilidades y amenazas que puedan afectar la seguridad de la información de los activos de la SDG y se consigue por medio de implementar un monitoreo constante del comportamiento de los sistemas con el objetivo de proporcionar una visibilidad de la infraestructura tecnológica y su nivel ante posibles anomalías, además de la perdida de la eficacia, las condiciones adversas de operación, perdida del negocio, reputación, daño entre otros..

2. **Plan de Continuidad del Negocio** en concordancia al dominio 17 de la Norma ISO 27001 y la Guía del Sistema de Gestión de la Seguridad de la Información del MINTIC.

   La Dirección de Tecnologías de la Información manifestó que no cuenta con este documento en el que se hace necesario para la implementación del SGSI al interior de la entidad, el objetivo de implementar este plan es que se tenga la capacidad de recuperar y restaurar todas las funciones críticas que hayan sido interrumpidos por algún incidente o desastre, y de esta manera poder seguir prestando los servicios en niveles aceptables que no afecten la continuidad del negocio, identificar amenazas potenciales a la entidad y el impacto que podría causar a la operación de negocio que en caso de materializarse.

   Con el fin de que la labor de control interno que realiza esta Oficina, en la Secretaría Distrital de Gobierno, conduzca a las dependencias auditadas hacia la mejora continua de sus procesos y procedimientos, a través del establecimiento de acciones de mejoramiento de su gestión; a partir de los resultados presentados en este informe, la Dirección de Tecnología e Información deberá elaborar y presentar un plan de mejoramiento que permita subsanar las causas de las no conformidades, y atender las oportunidades de mejora, en un plazo no mayor a 15 (quince) días calendario, contados a partir de la notificación de hallazgos por medio del aplicativo Mi Mejora Continua – MIMEC, con base en la publicación de este documento, en la página web de la Secretaría, a través del enlace de la Oficina de Control Interno.

Para la elaboración y presentación de dicho plan se deben tener en cuenta los lineamientos establecidos por la Oficina Asesora de Planeación, en el GCN-M002 Manual para la gestión de planes de mejoramiento, publicado en el Sistema Integrado de Gestión y Calidad; particularmente la política de operación que indica *"Los planes de acción deben ser formulados en su totalidad en un plazo máximo de 15 días calendario contados a partir de la notificación por medio del aplicativo".*

## 9. Conclusiones

- El MSPI se encuentra en etapa de diagnóstico desde hace dos años en la entidad por lo que se concluye que se debe revisar todos los controles para lograr en la siguiente vigencia la implementación del modelo en el nivel central y las Alcaldías.

- La matriz de riesgos de seguridad digital se presentó en un documento en Excel que mencionan los riesgos de seguridad digital que se tienen contemplados en la entidad, pero se encuentra desactualizado. Luego de la matriz de riesgos de seguridad desarrollada se debe continuar con la declaración de aplicabilidad y debe ser un contexto estratégico de los criterios básicos en el alcance, los limitantes y la gestión de riesgos de seguridad digital traerán consigo controles que incluyan el monitoreo y la revisión debe ser claramente definida.

- Se deben establecer las brechas e indicar que le hace falta al control o requisito para cumplir frente a la Norma ISO 27001 de 2013, en donde se incluyen los requisitos de Gobierno en Línea y el MSPI, no se han diligenciado ni se han incluido las actividades o acciones requeridas para cumplir con el componente del ciclo PHVA.

## 10. Recomendaciones

Conforme a las auditorías que se han realizado en la SDG a la implementación del MSPI se reiteran algunas recomendaciones que se han evidenciado y se relacionan algunas novedades conforme a la entrevista y revisión documental realizada por la OCI.

- La entidad deberá disponer de un oficial o responsable de seguridad de la información para mejorar la implementación del SGSI, a la fecha no se identifica o documenta la definición de estos roles o responsabilidades.

- Elaborar e implementar un plan de comunicaciones relacionado con los temas de seguridad y privacidad de la información dirigido a todos los funcionarios, contratistas y demás miembros externos asociados a la entidad con el fin de evidenciar que ocurre en caso que no se sigan los protocolos establecidos.

- Desarrollar un plan de trabajo enfocado a implementar los controles necesarios, con el fin de mitigar las vulnerabilidades a las cuales se encuentran expuestos y comprometidos los componentes informáticos.

- Realizar supervisión continua a las capacidades técnicas de los proveedores, para mantener la disponibilidad, confidencialidad e integridad de la información que se le entrega
- Requerir reportes e informes periódicos por parte del proveedor sobre las condiciones del servicio y seguridad que se hayan pactado.

Conforme a los dominios se realizan las siguientes observaciones:

- Dominio 5. Políticas de la seguridad de la información: Se debe realizar un entrenamiento y capacitación de los usuarios en las políticas de seguridad de la información.

- Dominio 6. Organización de la seguridad de la información: No se cuenta con los roles y responsabilidades de los proveedores relacionadas con la seguridad de la información. Se debe establecer el líder y/o responsable de la implementación el modelo, revisar el Manual de Funciones y otras alternativas para asignar este rol de oficial de cumplimiento.

- Dominio 7. Seguridad de los recursos humanos: El personal de la organización en el desarrollo de las actividades para los cuales fueron contratados, se hace necesario establecer controles para asegurar que son conscientes de los riesgos, responsabilidades y deberes con respecto a la seguridad de la información. Debe existir procedimientos y tecnologías requeridas por el SGSI a los funcionarios que aplique. Jornadas de sensibilización sobre el SGSI.

- Dominio 8. Gestión de activos: La entidad debe identificar sus activos relevantes, este inventario debe ser exacto, actualizado, alineado con la SDG para cada uno de los activos identificados, el propietario del activo debe ser asignado y la clasificación debe ser identificada. Implementar la política de gestión de incidentes y hacer seguimiento a su ejecución.

- Dominio 9. Control de acceso: Es importante actualizar la matriz de acceso de los activos, implementar la matriz de acceso en las plataformas de la entidad. Debe existir una política de uso de redes y de servicios de red.

- Dominio 10. Criptografía: Para los sistemas de información críticos que se manejan en la entidad debe establecer controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información. Se debe implementar una política en donde se tenga contemplado la gestión de claves criptográficas, que incluya la generación, almacenamiento, distribución, retiro y destrucción de dichas claves.

- Dominio 11. Seguridad física y del entorno: Se debe tener en cuenta la verificación que todos los equipos utilizados en la entidad cuenten con un programa de mantenimiento de acuerdo con las especificaciones técnicas del fabricante. Se debe mejorar los controles especificados en el SGSI el retiro de algún activo de las oficinas de la entidad solo puede permitirse con la debida autorización de un documento donde se asigne un responsable de la aplicación.

- Dominio 12. Seguridad de las operaciones: Se tiene que implementar un procedimiento de los ambientes de software separados en donde exista automatización de un conjunto de datos de pruebas que sea estándar, ya que en la entidad se manejan datos sensibles y estos no se deberían copiar en el entorno de pruebas a menos que se entreguen controles equivalentes para el ambiente de pruebas, realizar la separación de redes para los entornos de desarrollo, pruebas y operación.

- Dominio 13. Seguridad de las comunicaciones: Establecer la segmentación con base en el nivel de criticidad de los activos. Revisar las políticas de direccionamiento IP origen y destino, puertos para el tráfico autorizado(firewall). Evaluar el uso de analizadores de protocolos para seguimiento a reportes de anomalías en la red. Transmitir de manera segura la información, sin importar el medio y el mecanismo usado para la transferencia. Establecer una política y procedimiento y los controles de transferencia formal para proteger la información a través de todos los tipos de medios. Tener en cuenta las responsabilidades en las directrices de los acuerdos de confidencialidad.

- Dominio 14. Adquisición, desarrollo y mantenimiento de sistemas: La identificación y gestión de los requisitos de seguridad de información y los procesos asociados deben ser constituidos en etapas tempranas de los proyectos de los sistemas de información. Implementar los controles de acceso y protección de los datos expuestos en los servicios de red con base en las políticas del SGSI. Se deberá considerar la tecnología nueva para conocer los riesgos de seguridad. La introducción de nuevos sistemas de información y los principales cambios a los sistemas efectivos deben seguir un proceso formal de documentación, especificaciones, pruebas, control de calidad e implementación administrada. Cuando se hacen cambios a las plataformas operacionales, las aplicaciones críticas de la entidad deben ser revisadas y puesto a prueba para asegurar que no hay impacto desfavorable en la seguridad o de las operaciones, por lo que todos los cambios deben ser totalmente probados y documentados. Los nuevos sistemas se deben someter a pruebas verificables durante los procesos de desarrollo, incluida la preparación de un programa de actividades detallando las entradas y pruebas con los resultados esperados bajo una variedad de condiciones.

- Dominio 15. Relaciones con los proveedores: Se deben establecer y documentar acuerdos con los proveedores, para asegurar que no haya inconvenientes entre la entidad y el proveedor respecto a las obligaciones de ambas partes para cumplir con los requisitos relevantes de seguridad de la información. Es necesario establecer los controles de seguridad para garantizar que tienen en cuenta los requisitos del ejercicio en la entidad antes de gestionar compras para los servicios que afecten la seguridad de la información de la infraestructura sobre la cual esta soportada.

- Dominio 16. Gestión de incidentes de seguridad de la información: La entidad debe establecer en su política de seguridad de la información como es el compromiso, organización y asignación para su cumplimiento, de igual forma vela por mantener protegido los activos de información. Entrenamiento y sensibilización a los funcionarios en el reporte de eventos de seguridad. Establecer en el procedimiento el reporte de eventos de seguridad de la información y el punto de contacto al que dichos eventos deben ser reportados. Los incidentes de seguridad de la información deben ser analizados por el personal designado por DTI para identificar acciones de mejora en tal

sentido es necesario establecer controles de seguridad para garantizar un manejo eficaz y consistente los incidentes de seguridad de la información. Implementar que permitan la cuantificación y monitoreo y los costos de los incidentes de seguridad de la información.

- Dominio 17. Aspectos de seguridad de la información de la gestión de continuidad de negocio: La entidad debe determinar que la continuidad de la seguridad de la información permita minimizar el impacto generados por la capacidad de ejecución, creando el proceso de continuidad de negocio, y/o bien del proceso de gestión de recuperación de desastres. Aplicar el procedimiento de la continuidad de la seguridad en caso de que la contingencia se mantenga los requerimientos de confidencialidad e integridad para los activos involucrados en el evento de una contingencia. Implementar los respaldos requeridos para las plataformas de seguridad informática en caso de una contingencia.

- Dominio 18. Cumplimiento: Al decidir sobre la protección de los registros, se debe considerar la correspondiente clasificación basado en sistema de clasificación. Los controles específicos y las responsabilidades individuales para satisfacer estos requisitos deberían ser definidos y documentados. Realizar una revisión periódica de la legislación aplicable plasmada en el documento de metodología de identificación y clasificación de activos. Se deben revisar pruebas de penetración o evaluaciones de vulnerabilidad, se debe tener precaución ya que tales actividades podrían conducir a un compromiso de la seguridad del sistema. Se debe cumplir con las auditorías internas anuales para el cumplimiento de seguridad de la información.

(ORIGIANL FIRMADO)

| Elaborado por | | Revisado y Aprobado por | |
|---|---|---|---|
| **CLAUDIA XIMENA OCHOA ANGEL**<br>Profesional Universitario<br>Oficina de Control Interno. | | **LADY JOHANA MEDINA MURILLO**<br>Jefe Oficina de Control Interno. | |
| Fecha: | 29 de julio de 2022 | Fecha: | 29 de julio de 2022 |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A5** | **POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION** | | | |
| **A5.1** | Orientación de la dirección para la gestión de la seguridad de la información | | | |
| **Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes** | | | | |
| **A5.1.1** | Políticas para la seguridad de la información | Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes. | Cumple satisfactoriamente | Mejorar la comunicación a los funcionarios y partes externas correspondientes |
| **A5.1.2** | Revisión de las políticas para la seguridad de la información. | Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas. | No cumple | Se debe revisar periódicamente y a través de una planeación de acuerdo a la efectividad de los controles y de acuerdo a un plan de mejoramiento continuo |
| **A6** | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION** | | | |
| **A6.1** | Organización interna | | | |
| **Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.** | | | | |
| **A6.1.1** | Roles y responsabilidades para la seguridad de la información | Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información. | No cumple | Faltan contemplar los roles Las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales<br>Se debe definir el líder de la implementación del modelo MSPI. |
| **A6.1.2** | Separación de deberes | Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización | No cumple | No existe documentación asociada al proceso por lo que no se cuenta totalmente con separación de deberes<br>Por lo que no se debe implementar controles que compensen la separación de deberes y realizar la revisión periódica en los SI, implementar rastros de auditoría<br>Esto va de la mano con las responsabilidades de la entidad en cuanto a la seguridad de la información |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A6.1.3** | Contacto con las autoridades | Control: Se deben mantener contactos apropiados con las autoridades pertinentes. | Cumple parcialmente | No existe procedimiento formal interno, porque todo se hace a través de la alta consejería distrital, Por lo que se recomienda tener un procedimiento formal de la SDG. |
| **A6.1.4** | Contacto con grupos de interés especial | Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad | Cumple parcialmente | Se tiene el contacto a través de la Alta Consejería Distrital de las Tics<br>Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. |
| **A6.1.5** | Seguridad de la información en la gestión de proyectos. | Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. | No cumple | Si bien se tiene contemplado en el PETI en cuanto a las necesidades de capacitación y las buenas prácticas de la Seguridad de la Información<br>Se debe contemplar la Arquitectura Gestión de proyectos de TI de MINTIC que contemple los objetivos de la seguridad de la información se incluyan en los objetivos de los proyectos identificar los controles necesarios; y que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada. |
| **A6.2** | Dispositivos móviles y teletrabajo | | | |
| **Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles** | | | | |
| **A6.2.1** | Política para dispositivos móviles | Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | Cumple parcialmente | Tener en cuenta los dispositivos móviles así como los controles de seguridad que la entidad utilizará para proteger, mitigar, supervisar y<br>monitorear los riesgos asociados al acceso y divulgación no autorizada de la información. |
| **A6.2.2** | Teletrabajo | Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. | Cumple parcialmente | Conforme a lo observado el manual de talento humano se tiene es una lista de chequeo de requerimientos básicos en cuanto al equipo de cómputo pero se requiere crear un procedimiento formal que contemple los especificando la seguridad física existente en el sitio del teletrabajo. |
| **A7** | **SEGURIDAD DE LOS RECURSOS HUMANOS** | | | |
| **A7.1** | Antes de asumir el empleo | | | |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.** | | | | |
| **A7.1.1** | Selección | Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos. | Cumple parcialmente | Existe el Procedimientos en gestión humana, pero se debe automatizar, sistematizar la selección de personal, conteniendo la evaluación de desempeño ya que actualmente se encuentra a través de una tabla de excel |
| **A7.1.2** | Términos y condiciones del empleo | Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información. | No cumple | Obligaciones contractuales de los contratistas en cuanto a la confidencialidad de la entidad y código disciplinario para los de planta<br>Pero para el caso de seguridad de la información no se tiene contemplado en algunos contratos de prestación de servicios observados no se observó el cumplimiento de la seguridad de la información |
| **A7.2** | Durante la ejecución del empleo | | | |
| **Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.** | | | | |
| **A7.2.1** | Responsabilidades de la dirección | Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. | Cumple satisfactoriamente | |
| **A7.2.2** | Toma de conciencia, educación y formación en la seguridad de la información. | Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | Cumple parcialmente | No se cuenta con un plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A7.2.3** | Proceso disciplinario | Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. | Cumple satisfactoriamente | |
| **A7.3** | Terminación y cambio de empleo | | | |
| **Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo** | | | | |
| **A7.3.1** | Terminación o cambio de responsabilidades de empleo | Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir. | Cumple parcialmente | En obligaciones contractuales Si bien se describe en el contrato que se debe mantener la confidencialidad no existe un acuerdo más claro y con sus respectivas vigencias del cumplimiento de la seguridad de la información |
| **A8** | **GESTION DE ACTIVOS** | | | |
| **A8.1** | Responsabilidad por los activos | | | |
| **Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.** | | | | |
| **A8.1.1** | Inventario de activos | Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos. | Cumple parcialmente | No se cuenta con los activos debidamente aprobados por la alta dirección.<br>Se deben hacer reuniones de seguimiento con las diferentes áreas para revisar que activos de información se deben custodiar |
| **A8.1.2** | Propiedad de los activos | Control: Los activos mantenidos en el inventario deben tener un propietario. | Cumple parcialmente | Se deben actualizar ya que se debe realizar un chequeo de que activos se deben proteger |
| **A8.1.3** | Uso aceptable de los activos | Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. | Cumple parcialmente | Establecer un procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos. |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A8.1.4** | Devolución de activos | Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. | Cumple parcialmente | En caso de que un funcionario o tercero sea el dueño del activo indague como se asegura la transferencia de la información a la Entidad y el borrado seguro de la información de la Entidad. |
| **A8.2** | Clasificación de la información | | | |
| **Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.** | | | | |
| **A8.2.1** | Clasificación de la información | Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. | Cumple parcialmente | No se encuentra totalmente diligenciada la clasificación de información y deberá valorarse teniendo en cuenta la confidencialidad, integridad y disponibilidad. Definir cada cuanto debe revisarse la clasificación de un activo |
| **A8.2.2** | Etiquetado de la información | Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. | Cumple parcialmente | Se debe el etiquetado de los activos en formatos físicos y electrónicos y que refleje el esquema de clasificación establecido |
| **A8.2.3** | Manejo de activos | Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. | No cumple | Contar con un procedimiento para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. Este debe ser adoptado por la entidad. |
| **A8.3** | Manejo de medios | | | |
| **Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios** | | | | |
| **A8.3.1** | Gestión de medio removibles | Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización. | Cumple parcialmente | No se cuenta con la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles |
| **A8.3.2** | Disposición de los medios | Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. | No cumple | No existe procedimiento que garantice los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas. |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A8.3.3** | Transferencia de medios físicos | Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. | No cumple | No existe un procedimiento para verificar la identificación de los servicios de mensajería.<br>Solicite los registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino. |
| **A9** | **CONTROL DE ACCESO** | | | |
| **A9.1** | Requisitos del negocio para el control de acceso | | | |
| **Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.** | | | | |
| **A9.1.1** | Política de control de acceso | Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información. | Cumple parcialmente | Procedimiento para el ingreso a los sistemas de información de manera segura |
| **A9.1.2** | Acceso a redes y a servicios en red | Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. | Cumple parcialmente | No se cuenta con los requisitos de autenticación de usuarios para acceder a diversos servicios de red<br>No se tiene contemplado el acceso a redes |
| **A9.2** | Gestión de acceso de usuarios | | | |
| **Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.** | | | | |
| **A9.2.1** | Registro y cancelación del registro de usuarios | Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. | No cumple | No se cuenta con la identificación y eliminación o la deshabilitación periódicamente las identificaciones de usuario redundantes |
| **A9.2.2** | Suministro de acceso de usuarios | Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. | No cumple | No se adaptado los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización<br>No se cuenta con una política de eliminación/gestión de usuarios |
| **A9.2.3** | Gestión de derechos de acceso privilegiado | Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | No cumple | No se cuenta la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso pertinente |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A9.2.4** | Gestión de información de autenticación secreta de usuarios | Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal. | No cumple | Se debe estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura |
| **A9.2.5** | Revisión de los derechos de acceso de usuarios | Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares. | No cumple | Definir las autorizaciones para los derechos de acceso privilegiado y revisar periódicamente |
| **A9.2.6** | Retiro o ajuste de los derechos de acceso | Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios. | No cumple | Se debe crear el procedimiento de como se hace con los derechos de acceso a la información y a los activos asociados, antes de que el empleo termine o cambie, que incluya terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, revisar las responsabilidades. |
| **A9.3** | Responsabilidades de los usuarios | | | |
| **Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.** | | | | |
| **A9.3.1** | Uso de información de autenticación secreta | Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta. | No cumple | Se tiene indicaciones en manual de seguridad. Falta documentar, políticas de seguridad clave y contraseña temporalidad<br>Mejorar el instructivo del acceso por VPN debido a que si no se vence la contraseña del usuario no debería dejar ingresar con la misma contraseña que se venció<br>Mantener la confidencialidad de la información de autenticación secreta,<br>asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad |
| **A9.4** | Control de acceso a sistemas y aplicaciones | | | |
| **Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.** | | | | |
| **A9.4.1** | Restricción de acceso a la información | Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. | No cumple | Contemplar en el procedimiento de control de acceso en donde se especifique la restricción de acceso a la información y a las funciones de las aplicaciones por parte de los usuarios y el personal de soporte, de acuerdo con la política definida de control de acceso. |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A9.4.2** | Procedimiento de ingreso seguro | Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro. | Cumple parcialmente | Falta visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador |
| **A9.4.3** | Sistema de gestión de contraseñas | Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. | Cumple parcialmente | Falta apartes de las actividades listadas Gestión de contraseñas tener en cuenta la VPN |
| **A9.4.4** | Uso de programas utilitarios privilegiados | Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones. | No cumple | Se debe contemplar la restricción, automatización y el control del uso de los programas utilitarios que puedan anular los controles de los sistemas y las aplicaciones. |
| **A9.4.5** | Control de acceso a códigos fuente de programas | Control: Se debe restringir el acceso a los códigos fuente de los programas. | No cumple | No se tiene gestionado los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos |
| **A10** | **CRIPTOGRAFIA** | | | |
| **A10.1** | Controles criptográficos | | | |
| **Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información** | | | | |
| **A10.1.1** | Política sobre el uso de controles criptográficos | Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. | Cumple parcialmente | Utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación |
| **A10.1.2** | Gestión de llaves | Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida. | No cumple | Implementar una política sobre el uso, protección y tiempo de vida de las llaves para diferentes sistemas criptográficos y en las diferentes aplicaciones |
| **A11** | **SEGURIDAD FISICA Y DEL ENTORNO** | | | |
| **A11.1** | Áreas seguras | | | |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.** | | | | |
| **A11.1.1** | Perímetro de seguridad física | Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información. | Cumple parcialmente | Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información. |
| **A11.1.2** | Controles de acceso físicos | Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado. | Cumple satisfactoriamente | |
| **A11.1.3** | Seguridad de oficinas, recintos e instalaciones. | Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.. | Cumple satisfactoriamente | |
| **A11.1.4** | Protección contra amenazas externas y ambientales. | Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. | Cumple satisfactoriamente | |
| **A11.1.5** | Trabajo en áreas seguras. | Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras. | Cumple satisfactoriamente | |
| **A11.1.6** | Áreas de carga, despacho y acceso público | Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. | Cumple satisfactoriamente | |
| **A11.2** | Equipos | | | |
| **Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.** | | | | |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A11.2.1** | Ubicación y protección de los equipos | Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | Cumple satisfactoriamente | |
| **A11.2.2** | Servicios de suministro | Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | Cumple satisfactoriamente | |
| **A11.2.3** | Seguridad en el cableado. | Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño. | Cumple satisfactoriamente | |
| **A11.2.4** | Mantenimiento de los equipos. | Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. | Cumple satisfactoriamente | |
| **A11.2.5** | Retiro de activos | Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa | Cumple satisfactoriamente | |
| **A11.2.6** | Seguridad de equipos y activos fuera de las instalaciones | Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. | No cumple | No se controla los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina) |
| **A11.2.7** | Disposición segura o reutilización de equipos | Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso. | No cumple | Se debe contemplar en el procedimiento de verificar todos los elementos de los equipos de computo que contengan medios de almacenamiento y asegurar la correcta eliminación de datos sensibles de forma segura |
| **A11.2.8** | Equipos de usuario desatendido | Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada. | No cumple | Establecer un procedimiento en donde se contemplen el cierre de las sesiones activas cuando hayan terminado, Capacitación a usuarios en donde se asegurar mediante un mecanismo de bloqueo apropiado |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A11.2.9** | Política de escritorio limpio y pantalla limpia | Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información. | No cumple | Capacitar a todos los funcionarios y proveedores en la política de escritorio limpio y pantalla limpia en las instalaciones de procesamiento de información. |
| **A12** | **SEGURIDAD DE LAS OPERACIONES** | | | |
| **A12.1** | Procedimientos operacionales y responsabilidades | | | |
| **Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.** | | | | |
| **A12.1.1** | Procedimientos de operación documentados | Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan. | No cumple | Definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema<br>Se ha especificado como punto único de ingreso de solicitudes a mesa de servicio<br>Un manual de la política de documentación basada en el sistema de gestión de calidad para la entidad |
| **A12.1.2** | Gestión de cambios | Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. | No cumple | Implementar y capacitar los procesos de negocio de los sistemas de información de manera segura. |
| **A12.1.3** | Gestión de capacidad | Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. | Cumple parcialmente | Revisar los procedimientos para la gestión de la demanda de capacidad. |
| **A12.1.4** | Separación de los ambientes de desarrollo, pruebas y operación | Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. | Cumple parcialmente | Automatización de conjunto de datos de pruebas que sea estándar<br>Definición de los requerimientos para la transición entre ambientes. |
| **A12.2** | Protección contra códigos maliciosos | | | |
| **Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.** | | | | |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A12.2.1** | Controles contra códigos maliciosos | Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. | Cumple parcialmente | Establecer una política formal que prohíba el uso de software no autorizado<br>implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (listas negras)<br>Crear un procedimiento en donde se especifique sobre el modo de operación de las plataformas |
| **A12.3** | Copias de respaldo | | | |
| **Objetivo: Proteger contra la perdida de datos** | | | | |
| **A12.3.1** | Respaldo de la información | Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Cumple parcialmente | Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada, entrenar a los responsables de activos y administradores de plataformas en la política de generación y restauración de copias de respaldo. |
| **A12.4** | Registro y seguimiento | | | |
| **Objetivo: Registrar eventos y generar evidencia** | | | | |
| **A12.4.1** | Registro de eventos | Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. | Cumple parcialmente | Revisar los eventos en donde se tenga en cuenta los registros de intentos de acceso al sistema exitosos y rechazados |
| **A12.4.2** | Protección de la información de registro | Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado. | No cumple | Se debe incluir la verificación de las alteraciones a los tipos de mensaje que se registran; revisar establecer los archivos log que son editados o eliminados; verificar cuando se excede la capacidad de almacenamiento del medio de archivo log periódico. |
| **A12.4.3** | Registros del administrador y del operador | Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad. | No cumple | Establecer que solo los roles con función de auditoría tienen acceso a los logs de eventos. |
| **A12.4.4** | Sincronización de relojes | Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo. | Cumple parcialmente | Se deben verificar con los nuevos sistemas de información que están en proceso de implementación. |
| **A12.5** | Control de software operacional | | | |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **Objetivo: Asegurarse de la integridad de los sistemas operacionales** | | | | |
| **A12.5.1** | Instalación de software en sistemas operativos | Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. | Cumple parcialmente | Actualizar el software operacional, aplicaciones. |
| **A12.6** | Gestión de la vulnerabilidad técnica | | | |
| **Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas** | | | | |
| **A12.6.1** | Gestión de las vulnerabilidades técnicas | Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. | Cumple parcialmente | Definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología |
| **A12.6.2** | Restricciones sobre la instalación de software | Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios. | No cumple | Se debe implementar un documento donde contenga las restricciones de la instalación del software más detallado, así mismo capacitar a todos los funcionarios y colaboradores en el procedimiento |
| **A12.7** | Consideraciones sobre auditorias de sistemas de información | | | |
| **Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos** | | | | |
| **A12.7.1** | Controles de auditorías de sistemas de información | Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio. | No cumple | Aplicar la auditoría interna de acuerdo con las normas establecidas del SGSI |
| **A13** | **SEGURIDAD DE LAS COMUNICACIONES** | | | |
| **A13.1** | Gestión de la seguridad de las redes | | | |
| **Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.** | | | | |
| **A13.1.1** | Controles de redes | Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. | Cumple parcialmente | Si bien se encuentran los controles que se apliquen en forma coherente a través de la infraestructura de procesamiento de información |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A13.1.2** | Seguridad de los servicios de red | Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente. | Cumple parcialmente | Definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red |
| **A13.1.3** | Separación en las redes | Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes. | No cumple | Separación de redes van por diferente usuarios, equipos Establecer una segmentación de redes con base en el nivel de criticidad de los activos |
| **A13.2** | Transferencia de información | | | |
| **Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.** | | | | |
| **A13.2.1** | Políticas y procedimientos de transferencia de información | Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. | No cumple | Debe existir un protocolo y procedimiento interno en la transferencia de información segura entre la entidad o entidades externas<br>establecer la política o directrices que presentan el uso aceptable de las instalaciones de comunicación |
| **A13.2.2** | Acuerdos sobre transferencia de información | Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas. | Cumple parcialmente | Establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo |
| **A13.2.3** | Mensajería Electronica | Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica. | Cumple parcialmente | Definir niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente |
| **A13.2.4** | Acuerdos de confidencialidad o de no divulgación | Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. | No cumple | Se debe proteger los medios de acuerdos de confidencialidad de transferencia de información. Garantizar que no se presente uso inadecuado cuando la información sale de la entidad |
| **A14** | **Adquisición, desarrollo y mantenimiento de sistemas** | | | |
| **A14.1** | Requisitos de seguridad de los sistemas de información | | | |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes .** | | | | |
| **A.14.1.1** | Análisis y especificación de requisitos de seguridad de la información | Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. | Cumple satisfactoriamente | |
| **A.14.1.2** | Seguridad de servicios de las aplicaciones en redes públicas | Control: La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas. | Cumple satisfactoriamente | |
| **A.14.1.3** | Protección de transaccciones de los servicios de las aplicaciones. | Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada. | No cumple | No se tiene la documentación acerca de la seguridad que este integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro Utilizar una autoridad confiable en donde se asegure que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente |
| **A14.2** | Seguridad en los procesos de Desarrollo y de Soporte | | | |
| **Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.** | | | | |
| **A.14.2.1** | Política de desarrollo seguro | Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización. | Cumple parcialmente | No se tiene definido la seguridad del ambiente de desarrollo, las directrices de codificación seguras para cada lenguaje de programación usado |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A.14.2.2** | Procedimientos de control de cambios en sistemas | Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. | No cumple | Elaborar un procedimiento en donde se establezca el registro de los niveles de autorización asegurar que los cambios se presenten a los usuarios autorizados |
| **A.14.2.3** | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización. | No cumple | El líder de seguridad debe realizar pruebas para validar que los datos mantengan la protección de la confidencialidad, integridad y disponibilidad con base en el SGSI |
| **A.14.2.4** | Restricciones en los cambios a los paquetes de software | Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente. | Cumple parcialmente | El líder de seguridad debe realizar pruebas para validar que los datos mantengan la protección de la confidencialidad, integridad y disponibilidad con base en el SGSI |
| **A.14.2.5** | Principio de Construcción de los Sistemas Seguros. | Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. | Cumple parcialmente | Se debe incluir los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información |
| **A.14.2.6** | Ambiente de desarrollo seguro | Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. | Cumple parcialmente | No se tiene contemplado la definición de los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema |
| **A.14.2.7** | Desarrollo contratado externamente | Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente. | Cumple parcialmente | No se tiene definido los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente |
| **A.14.2.8** | Pruebas de seguridad de sistemas | Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad. | No cumple | Los procesos para asegurar los sistemas desarrollados cumplan con las funcionalidades de seguridad es necesario realizar pruebas especificas de seguridad. |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A.14.2.9** | Prueba de aceptación de sistemas | Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados. | Cumple parcialmente | Se cuenta con un ambiente de pruebas por lo que se hace necesario documentar el control de cambios. |
| **A14.3** | Datos de prueba | | | |
| **Objetivo: Asegurar la protección de los datos usados para pruebas.** | | | | |
| **A.14.3.1** | Protección de datos de prueba | Control:Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente. | Cumple parcialmente | Actualmente se cuenta con un ambiente de pruebas se debe realizar el copiado de información operacional o un rastro de auditoría.<br>Se debe definir que la información operacional en el ambiente de pruebas inmediatamente después de finalizar las pruebas. |
| **A15** | **RELACIONES CON LOS PROVEEDORES** | | | |
| **A15.1** | Seguridad de la información en las relaciones con los proveedores. | | | |
| **Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.** | | | | |
| **A15.1.1** | Política de seguridad de la información para las relaciones con proveedores | Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar. | No cumple | Se debe establecer un procedimiento en donde la entidad indique los ANS en cuanto a la Seguridad de la Información en relación con los proveedores. |
| **A15.1.2** | Tratamiento de la seguridad dentro de los acuerdos con proveedores | Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. | No cumple | En la matriz de riesgos no se tiene contemplado como se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, se debe incluir si se llegaran a presentar incidentes de seguridad de la información y la revaloración de los riesgos. |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A15.1.3** | Cadena de suministro de tecnología de información y comunicación | Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | No cumple | No se evidencian |
| **A15.2** | Gestión de la prestación de servicios de proveedores | | | |
| **Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores** | | | | |
| **A15.2.1** | Seguimiento y revisión de los servicios de los proveedores | Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. | No cumple | Se debe tener un control de cambios en la gestión de incidentes y un monitoreo constante |
| **A15.2.2** | Gestión del cambio en los servicios de los proveedores | Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos. | No cumple | Aplicar la política de gestión del cambio del SGSI en la relación con los proveedores |
| **A16** | **GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION** | | | |
| **A16.1** | Gestión de incidentes y mejoras en la seguridad de la información | | | |
| **Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.** | | | | |
| **A16.1.1** | Responsabilidades y procedimientos | Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. | Cumple parcialmente | No se tiene contemplado en el procedimiento la planificación y preparación de respuesta a incidentes; el proceso de seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A16.1.2** | Reporte de eventos de seguridad de la información | Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. | Cumple parcialmente | Se deben informar a través de los canales de gestión apropiados |
| **A16.1.3** | Reporte de debilidades de seguridad de la información | Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. | No cumple | Debe existir capacitación a las personas interesadas de la entidad |
| **A16.1.4** | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. | No cumple | Se debe contemplar que la evidencia de los incidentes de SGSI tienen que ser categorizados y se cuenta con planes de respuesta para cada categoría. |
| **A16.1.5** | Respuesta a incidentes de seguridad de la información | Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. | No cumple | Se debe cumplir un procedimiento donde se indique los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. |
| **A16.1.6** | Aprendizaje obtenido de los incidentes de seguridad de la información | Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros. | No cumple | No se evidencia |
| **A16.1.7** | Recolección de evidencia | Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. | No cumple | Faltan los procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. |
| **A17** | **ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO** | | | |
| **A17.1** | Continuidad de Seguridad de la información | | | |
| **Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.** | | | | |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A17.1.1** | Planificación de la continuidad de la seguridad de la información | Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. | No cumple | Se debe establecer procedimientos específicos que respondan a las interrupciones del servicio con el fin de proteger y recuperar las funciones críticas del negocio<br>Identificar las aplicaciones y las plataformas criticas<br>Establecer los tiempos mínimos de recuperación requerido para la operación |
| **A17.1.2** | Implementación de la continuidad de la seguridad de la información | Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. | No cumple | Implementar procedimientos específicos y guías de operación<br><br>Identificar los riesgos de la continuidad |
| **A17.1.3** | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. | No cumple | Capacitación inicial para el correcto funcionamiento al personal necesario |
| **A17.2** | Redundancias | | | |
| **Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.** | | | | |
| **A17.2.1** | Disponibilidad de instalaciones de procesamiento de información | Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. | No cumple | No se cuenta en la actualidad con arquitecturas redundantes. |
| **A18** | **CUMPLIMIENTO** | | | |
| **A18.1** | Cumplimiento de requisitos legales y contractuales | | | |
| **Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.** | | | | |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A18.1.1** | Identificación de la legislación aplicable. | Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización. | No cumple | Verificar el cumplimiento de la SGSI en la entidad Ley de protección de datos. |
| **A18.1.2** | Derechos propiedad intelectual (DPI) | Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. | No cumple | Se debe tener una política publicada sobre el cumplimiento no solo del software si no a los documentos gráficos.<br><br>Contemplar un procedimiento para el cumplimiento de los requisitos y contractuales relacionados y el uso de productos de software por patente. |
| **A18.1.3** | Protección de registros | Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. | Cumple parcialmente | Se deben incluir procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos<br>Se debe mencionar de las arquitecturas de sistemas de información |
| **A18.1.4** | Privacidad y protección de información de datos personales | Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable. | Cumple parcialmente | Falta el repositorio de datos personales y aumentar la toma de datos personales para todos los procesos de la entidad. |
| **A18.1.5** | Reglamentación de controles criptográficos. | Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. | No cumple | Se debe especificar los controles criptograficas en donde se debe contemplar principios integridad, disponibilidad y confidencialidad |
| **A18.2** | Revisiones de seguridad de la información | | | |
| **Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.** | | | | |

| ANEXO | | | VALORACION | RECOMENDACION |
|---|---|---|---|---|
| **A18.2.1** | Revisión independiente de la seguridad de la información | Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. | No cumple | No se evidencian evaluaciones independientes |
| **A18.2.2** | Cumplimiento con las políticas y normas de seguridad | Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad. | No cumple | Se deberá realizar pruebas de cumplimiento y ser medible y con los estándares establecidos |
| **A18.2.3** | Revisión del cumplimiento técnico | Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. | No cumple | Se debe realizar revisiones a los lineamientos de la seguridad de la información por medio de ayuda de herramientas automatizadas que generen informes técnicos, para posterior análisis por un especialista. |

Fuente: NTC-ISO-IEC 27001:2013