IMPLEMENCIÓN DE LOS CONTROLES PRIORITARIOS DEL ANEXO A. DE LA NORMA ISO 27001/2013 EN BAINCOL S.A.S.

Yaneth Adiela Mopán Muñoz

Fundación Universitaria de Popayán
Ingeniería Industrial
Popayán
2021

IMPLEMENTACIÓN DE LOS CONTROLES PRIORITARIOS DEL ANEXO A. DE LA NORMA ISO 27001/2013 EN BAINCOL S.A.S.

Yaneth Adiela Mopán Muñoz

Asesor:

Luis Fernando Pedraza Ruiz

Fundación Universitaria de Popayán
Programa de Ingeniería Industrial
Popayán-Cauca
Proyecto
2021

TABLA DE CONTENIDO

1 RESUMEN

El presente proyecto se encuentra enmarcado en tres objetivos. El primero: Determinar el nivel de cumplimiento y madurez de la empresa Baincol SAS frente a los requisitos del estándar internacional ISO/IEC 27001/2013 Sistemas de Gestión de Seguridad de la Información, de modo que, faculte el análisis comparativo de la situación actual vs la situación esperada por la organización mediante la metodología del análisis GAP, así mismo, conocer las brechas en materia de seguridad de la información.
Como segundo objetivo se realizó una lista de chequeo con el apoyo de los interlocutores con el fin de determinar los controles aplicables o excluidos a la organización, de tal forma que se pudiera dar alcance a cada uno de los procesos de la empresa. Para culminar el último objetivo, fue necesario priorizar el grado de implementación de los subdominios de la norma mediante una mesa de trabajo conformada por 4 representantes de las áreas involucradas en la implementación de los mismos. La información anterior fue el insumo necesario para conocer las necesidades de la organización en materia de seguridad de la información y por consiguiente, para definir el plan de trabajo como tercer y final objetivo del proyecto aunado a las recomendaciones a considerar por la empresa. El presente trabajo permitió establecer que la organización no cumple con los controles sugeridos por el estándar internacional ISO/IEC 27001/2013 reflejado en un nivel de madurez de adopción de controles de 0,18 puntos con respecto al nivel objetivo planteado sobre 3. Como resultado de la priorización de implementación surgen 60 controles asociados a 19 subdominios de la norma para documentar.

2 INTRODUCCIÓN

La información se ha convertido en uno de los activos con mayor importancia en las organizaciones, cualquiera que sea su naturaleza, lo que ha generado la necesidad de implementar sistemas de gestión con el fin de preservar y controlar la confidencialidad, integridad y disponibilidad de la información. En 2016, Moreno, consideraba que a pesar de que la era tecnológica se encuentre en auge y las vulnerabilidades también aumentan proporcionalmente con respecto a las amenazas internas o externas; siempre existirán medidas de control que se podrán implementar para gestionar de manera adecuada los activos de información como la ISO 27001. (pp.32).

BANCA DE INVERSIONES DE COLOMBIA S.A.S en adelante BAINCOL, gestiona por medio de sus procesos transversales la información de las empresas que conforman el Grupo Empresarial Mundo Mujer en adelante el GEMM, de acuerdo con sus actividades económicas como:

- BANINCA: Actividad de agencias de cobranza y oficinas de calificación crediticia.
- INGEMM: Actividades mobiliarias realizadas a cambio de una retribución.
- INBAYAN: Actividades de las agencias de viaje.
- ADC: Actividades de bibliotecas y archivos.
- FMM: Actividades de otras asociaciones N.C.P (No Clasificado Previamente).

Se aclara que el alcance del proyecto comprende las actividades exclusivas de BAINCOL S.A.S y que no tiene alcance a las actividades directas del Banco Mundo

Mujer por tener sus propios procesos para el control de su actividad económica.

Por lo anterior, se puede inferir que la Gestión de información generada por la administración de las diferentes actividades económicas de las empresas asociadas, trae consigo mayor complejidad para su control lo que despierta un interés importante en BAINCOL, para establecer controles que escuden la organización contra posibles eventos que pongan en riesgo la operatividad de sus actividades. Para ello los ejecutivos de nivel corporativo comprenden la importancia de desarrollar un modelo de Gestión en Seguridad de la Información que brinde un valor agregado contribuyente al posicionamiento y sostenibilidad de la organización.

Actualmente la empresa., cuenta con el aval de la alta gerencia para la puesta en marcha de la implementación del programa de Gestión en Seguridad de la Información, dando el primer paso para la adopción de buenas prácticas en seguridad y protección de datos, que contrarresten el impacto generado por la materialización de riesgos como perdida o fuga de información y uso no autorizado de datos personales.

3 PROBLEMA

La infracción de la ley frente a la gestión de datos personales se convierte en una de las preocupaciones más comunes de las empresas en la actualidad; el desconocimiento de las normas no exime de responsabilidad a una entidad que recolecta, gestiona y dispone de información personal. BAINCOL SAS al prestar sus servicios de administración empresarial a BANINCA SAS, quien compra cartera castigada de manera directa al Banco Mundo Mujer, y por ende, información confidencial de personas con historial crediticio, se expone de tal forma que, la carencia de procedimientos y políticas que definen los fines de la recolección, el control y la gestión de la información, pueden concluir en sanciones millonarias impuestas por parte de la Superintendencia de Industria y Comercio SIC debido al incumplimiento de la Ley General de Protección de Datos Personales:

"Congreso de Colombia. (2012). Ley 1581 de 17 de octubre. Por la cual se dictan disposiciones generales. **Artículo 23.** Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

> a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;
>
> b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;
>
> c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;
>
> d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva."

Portafolio (2020). La SIC reportó que durante el año 2020 impuso multas por $7.580 millones, y fueron emitidas 2.070 órdenes para que las empresas cumplan con la legislación de protección de datos personales. De acuerdo con la entidad, en lo que va de este Gobierno, desde agosto de 2018, ha recibido 33.784 quejas de parte de los ciudadanos, y se han impuesto 200 multas por $18.454 millones.

Por otro lado, la inexistencia de procedimientos y políticas en materia de Seguridad de la Información no solo puede incurrir en pérdidas económicas por sanciones legales, también se puede hacer acreedor de robo, perdida y/o fuga de información

por medio de nuevas y constantes modalidades de delitos cibernéticos, las cuales apuntan a el talón de Aquiles de cualquier compañía a nivel mundial “Cuentas Bancarias” y/o sistemas de información principales que soportan la operatividad principal de las organizaciones, permitiendo así, caer en redes de extorción dedicadas a exigir incuantificables sumas de dinero por la recuperación de activos de información.

Por lo anteriormente expuesto, se puede inferir que BAINCOL SAS, actualmente no cuenta con buenas prácticas que permitan proteger la seguridad y la privacidad de la información, más aún, cuando su actividad económica es la administración empresarial, servicio que presta a las empresas del Grupo Empresarial Mundo Mujer (Excepto Banco Mundo Mujer), lo cual incrementa su responsabilidad y control ante los posibles riesgos de fuga y/o perdida de información. Lo anterior se refleja en un punto de inflexión para el desarrollo del programa de gestión de seguridad de la información, pero que permite reconocer las vulnerabilidades actuales y la escasa protección y preparación ante los posibles riesgos que pueden afectar la información propia y transferida por las empresas del Grupo para el respectivo desarrollo de sus actividades.

¿La priorización e implementación de controles alineados al anexo A. de la Norma ISO 27001, puede generar buenas prácticas tendientes a proteger y mantener la confidencialidad, integridad y disponibilidad de la información en BAINCOL S.A.S.?

4 JUSTIFICACIÓN

El Tiempo, (2020). Durante el año 2019 se registró un incremento del 54 % de casos tipificados como delitos informáticos en Colombia, de acuerdo con el estudio realizado por investigadores del Tanque de Análisis y creatividad de las TIC (TicTac), la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y el Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional. Uno de los resultados importantes de este estudio, denota algunos de los mecanismos más comunes para el hurto de identidad y/o robo de información siendo estos la modalidad de phishing, con un 42 %; la suplantación de identidad, con 28 %; el envío de malware, con 14 %; y los fraudes en medios de pago en línea, con el 16 %, los tipos de ataques más reportados. De la misma manera el estudio permite comparar el incremento del 30% de estos incidentes reportados en el país con respecto a otros países latinoamericanos en el siguiente orden: Perú (16 %), México (14 %), Brasil (11 %) y Argentina (9 %).

De acuerdo con la información anterior se puede inferir que las empresas a nivel nacional cuentan con falencias de control interno y externo lo que las hace vulnerables ante ataques cibernéticos ya mencionados. Con el fin de contribuir con el primer paso para la protección y control de estos incidentes, se busca implementar los controles prioritarios definidos para la organización de acuerdo con su actividad económica los cuales corresponden al 54% del total de los controles aplicables para Baincol SAS.

Es fundamental para la organización empezar a ejercer controles que contribuyan a la conservación de los activos de información, permitiendo gestionar los riesgos y estar preparados para afrontarlos, lo que optimizará el tiempo de respuesta ante un incidente de seguridad, minimizará el impacto generado por la materialización de alguno y reducirá los posibles costos y/o consecuencias que puedan surgir de la atención. La responsabilidad incrementa mucho más al considerar que BAINCOL SAS también debe propender por garantizar la seguridad de la información de las empresas del Grupo Empresarial Mundo Mujer sujetas a su servicio administrativo. Adicionalmente, la aplicación de buenas prácticas en materia de seguridad de la información se convierte en un valor agregado para la prestación de sus servicios, logrando una ventaja altamente competitiva a nivel regional.

5 OBJETIVOS

5.1 Objetivo general

Implementar los controles prioritarios del anexo A. de la norma ISO 27001/2013 mediante el ciclo PHVA en la empresa BAINCOL S.A.S., con el fin de garantizar la Seguridad de la Información. Objetivos específicos.

5.2 Objetivos específicos

- Diagnosticar el nivel de cumplimiento de los controles aplicables del anexo A. del estándar ISO 27001/2013, en BAINCOL SAS.
- Estandarizar los controles prioritarios en la empresa.
- Evaluar el nivel de madurez, en materia de Seguridad de la Información, en la organización mediante auditoría interna.

6 MARCO REFERENCIAL

6.1 Localización

La empresa Baincol SAS bica su única sede en la Cra 9 N° 18N-143 de la ciudad de Popayán.

Baincol S.A.S es una empresa con actividad económica principal la “Administración empresarial” servicio que presta en la actualidad a cinco de las empresas que componen el Grupo Empresarial Mundo Mujer: ADC, BANINCA, FUNDACIÓN MUNDO MUJER, INBAYAN e INGEMM.

Misión
Somos una organización que defina la estrategia del Grupo Empresarial Mundo Mujer; integramos las áreas transversales y administramos de forma rentable el patrimonio de la casa matriz Fundación Mundo Mujer.

Visión
Ser para el 2323 una compañía referente en estrategia, transformación digital, innovación, inteligencia de negocio y compliance, para las empresas del GEMM, que transmita el conocimiento a la casa matriz y unidades de negocio, potenciando su crecimiento y sostenibilidad.

Principios Organizacionales:

- Humildad: Aceptarnos como somos y reconocer nuestras debilidades para mejorar.
- Integridad: Actuar con honestidad para generar confianza.
- Liderazgo: Responsabilidad que entraña conducir personas y cumplir objetivos.
- Excelencia: Constancia, responsabilidad, efectividad.
- Respeto: Para influir, generar afiliación y ser admirado.

6.2 Marco Teórico

- **Activo:** Cualquier cosa que tiene valor para la organización.
- **Activos de Información:** De acuerdo con la ISO 27000 es todo conocimiento o información que tiene valor para la organización, lo que quiere decir que se encuentra alineada al contexto de la organización y lo que ella así determine para su control.
- **Análisis GAP:** Es una herramienta que permite establecer una comparativa entre el objetivo esperado y la situación actual de un proceso u organización con el fin de establecer cuán lejos se está de ese objetivo y determinar las estrategias para alcanzarlo.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.
- **Confidencialidad:** Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. El control de acceso debe estar sujeto a la necesidad y el cumplimiento de las funciones de

cada colaborador La revelación no autorizada de la información calificada de acuerdo con un nivel de confidencialidad alta, implica un grave impacto en la Superintendencia Nacional de Salud, en términos económicos, de su imagen y ante sus clientes.

- **Dato personal:** Un dato personal es la información concerniente a las personas físicas, que permiten identificarla gracias a la visión de conjunto que se haga de los mismos. Según su naturaleza, los datos personales, pueden ser clasificados como privados, semiprivados, públicos y sensibles; y existen varios tipos de datos personales, y no se limitan simplemente a los datos de identificación, sino que abarca, laborales, patrimoniales, académicos, ideológicos, de salud, características físicas, vida, hábitos, entre otros.
- **Declaración de aplicabilidad:** Es el vínculo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información. El objetivo de este documento es definir cuáles de los 114 controles sugeridos en el Anexo A de la norma ISO 27001 son los que se implementarán y cómo se realizará su implementación.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada. La información debe estar disponible cuando, donde y como se requiera, al igual que las aplicaciones o medios necesarios para su uso.
- **Ejecutivos de Nivel Corporativo:** Son considerados como las personas que guían y controlan una organización, en este caso, la empresa Baincol S.A.S.
- **Finalidad:** La finalidad corresponde a los fines exclusivos para los cuales fue entregada por el titular. Se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada, Cualquier utilización diversa, deberá ser autorizada en forma expresa por el Titular.
- **Incidente de Seguridad de la Información:** Es un evento o una serie de eventos de seguridad de la información no deseada o inesperada que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.
- **Información:** Hace referencia a los datos en formato digital o físico, tratados, creados, procesados, almacenados, archivados o borrados durante la ejecución de procesos misionales de la Superintendencia de Industria y Comercio.

  En la ley 1712 de 2014 en el artículo 6, la define como: “un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados genere obtenga, adquieran, transformen o controlen
- **Integridad:** Propiedad de la exactitud y la integridad. La falta de integridad de la información puede exponer a la empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas económicas.
- **Matriz de Roles y Perfiles:** Es un listado de las opciones autorizadas en los sistemas para los colaboradores de la organización dependiendo del cargo.
- **Seguridad de la Información:** Abarca todas las actividades orientadas a la preservación de la confidencialidad, integridad y disponibilidad de la información determinadas por la organización y alineadas a la aplicabilidad de los controles y el contexto de la misma.
- **Sistema de información:** Conjunto de elementos orientados al tratamiento y administración de datos e información organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

- **Sistema de Gestión de Seguridad de la Información (SGSI):** "(Inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua" (www.iso27000.es).

6.3 Marco Normativo

- La protección integral de los datos incluidos en bases de datos o archivos de cualquier fuente de información, garantizando a sus Titulares el ejercicio del derecho constitucional a conocer, actualizar y rectificar su información y demás garantías constitucionales contenidas en los artículos 15 y 20 de la Constitución Política de Colombia.
- Ley Estatutaria 1581 de 2012 establece las disposiciones generales para la Protección de Datos Personales y dentro de los deberes de los responsables del tratamiento, se encuentra el adoptar el Manual Interno de políticas y procedimientos que garantice el uso adecuado de la información y gestión de las consultas, peticiones y reclamos.
- Ley 87 de 1993 por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado
- Ley 489 de 1998 Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.
- A partir del Decreto 1377 de 2013, se dan los parámetros para facilitar la implementación y el cumplimiento de la Ley 1581 de 2012 y se facultan a los responsables y encargados del tratamiento de la información para el uso de mecanismos alternos como correos electrónicos, página web, mensajes de texto etc., para dar a conocer sus políticas y finalidades del tratamiento de la información.
- Circular Básica Jurídica 029 de 2014 de la Superintendencia Financiera. Aplica como buena práctica.
- ISO IEC 27001 Sistema de Gestión de la Seguridad de la Información. Esta norma cubre todo tipo de organizaciones (por ejemplo: empresas comerciales, agencias gubernamentales, organizaciones si ánimo de lucro). Esta norma específica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización. Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas.
- ISO/IEC 27002 Código de Practica para Controles de Seguridad de la Información. Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

- ISO/IEC 27005 Gestión de Riesgos en la Seguridad de la Información. muestra un enfoque directamente centrado en Risk Management para Tecnologías de la Información. Este enfoque tiene que estar alineado con la Gestión de Riesgos Empresarial general de la compañía. Esta norma parte del mismo modelo definido en ISO 31000.
- ISO 27035 explica un enfoque de mejores prácticas destinado a la gestión de la información de incidentes de la seguridad.
- ISO/IEC 31000 Gestión del Riesgo. Se basa en 11 principios que encajan con toda la estructura y objetivos de la organización y que están relacionadas con las normativas de la implementación de riesgos. Podemos considerar esta norma como una guía de buenas prácticas para las actividades relacionadas con la gestión del riesgo.

6.4 Estado del Arte

Moreno (2016), Plantea implementar el Sistema de gestión de seguridad de la información en el ministerio de defensa nacional específicamente en el áreas de talento humano, dentro de su implementación encontró que la seguridad de la información nunca va poder ser total, por el contrario cada vez será vulnerable a nuevas amenazas internas o externas, sin embargo, refiere que la información se podrá hacer más segura con la aplicación de medidas y controles apoyadas en guías o normas como la ISO 27001.

Villamil (2017), realiza el Diagnóstico y Planificación de la implementación del Modelo de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional de Cundinamarca, concluyendo que la fase diagnostica le permitió determinar la criticidad en los sistemas de información, para posterior mente establecer la planificación de acciones orientadas a la implementación de algunos componentes que hacen parte del sistema de gestión de seguridad de la información, como: La Política de Seguridad de la Información, Identificación de activos de Tecnologías de Información, plan de comunicaciones y un plan de gestión de riesgos.

Restrepo (2017), realiza el diagnóstico del estado actual de la seguridad de la información basado en la norma ISO 27001:2013, en la institución educativa técnico industrial sede mercedes pardo de simmonds de la ciudad de Popayán, para lo cual refiere que “la falta de conocimiento sobre la importancia de la seguridad de la información, como uno de los mayores activos de la organización, conlleva a un conjunto de malas prácticas dentro de los procedimientos realizados, de omisión de responsabilidades en los diferentes cargos por desconocimiento o por la falta de implementación de políticas de seguridad que permitan proteger adecuadamente la información del proceso gestión académica”.

7 METODOLOGÍA

El desarrollo del presente trabajo se realiza mediante el método de investigación de causal comparativo a través del cual se pretende establecer los beneficios de la implementación de los controles prioritarios a corto plazo en la empresa Baincol SAS apoyados en fuentes de información primaria y secundaria, que permita relacionar los datos reales de la organización con fuentes y/o datos externos y el resultado final del proyecto. Por medio del diagnóstico, priorización y posterior implementación de controles de seguridad de la información, se dará el primero y más importante paso para la prevención y protección de la confidencialidad, integridad y disponibilidad de la información, este será el esquema más importante para concientización sobre la importancia del Sistema de Gestión de Seguridad de la Información desde los ejecutivos de nivel corporativo de la empresa hasta los terceros vinculados. Este proyecto permitirá tener una visión panorámica sobre las vulnerabilidades y riesgos de la empresa frente a la gestión de la información, pero también, será la base para la identificación de controles que pueden afectar de manera significativa el desarrollo de las actividades operativas de la empresa para posteriormente dar un enfoque al inicio de la aplicabilidad de los controles prioritarios y la implementación de los mismos adoptando como estrategia la implementación del ciclo PHVA con el fin crear una cultura de mejora continua que permita la conservación del SGSI en el tiempo:

Planear. En esta fase se hará uso del análisis GAP como herramienta diagnostica con el fin de evaluar el estado de cumplimiento actual de la organización frente a los dominios A. de la ISO 27001/20013 y así mismo, conocer las brechas de seguridad de la información. De manera paralela, se deberá realizar la declaración de aplicabilidad que permita justificar la aplicación o exclusión de cada control de acuerdo con la naturaleza de la organización, actividad de la cual resultará un entregable para la empresa denominado: Declaración de aplicabilidad, la cual deberá ser aprobada por los ejecutivos de nivel corporativo o quienes ellos designen para tal fin. Posteriormente se procederá a priorizar la implementación de los controles aplicables por medio de una mesa de trabajo con participación de 4 áreas de la empresa: Seguridad de la Información, Tecnología Informática, Organización y Métodos y el área de Auditoria. Los resultados de la información anterior facilitarán plasmar mediante un diagrama de GANTT el plan de trabajo propuesto para alcanzar, a corto plazo, el objetivo deseado por la organización. El nivel de cumplimiento, la declaración de aplicabilidad, la priorización de implementación y el plan de trabajo, serán el marco de referencia para continuar con la siguiente fase.

Hacer. Para la segunda fase se deberá consolidar los controles prioritarios definiendo los procesos, políticas, procedimientos y demás documentos necesarios para dar alcance al objetivo esperado, logrando la documentación, estandarización e implementación de los controles prioritarios, para ello será necesario poner en marcha el plan de trabajo propuesto resultante de la fase anterior. Por otro lado, se deberá documentar las actividades que permitan evidenciar los controles implementados con el fin de medir y controlar la eficacia de los controles implementados para facilitar el desarrollo de la tercera fase.

Verificar. En esta fase será indispensable que la organización cuente con un programa de auditoría, donde se podrá realizar el cronograma de auditoria para evaluar el nivel de madurez de la organización frente el diagnóstico realizado. El

informe de auditoría será la evidencia objetiva de confrontación del resultado inicial con el estado a la fecha de finalización del plan de trabajo. Esto a su vez será el insumo para iniciar la etapa final mediante un informe resultados y plan de acción para los hallazgos encontrados. Esta información deberá ser plasmada de la misma manera que el diagnóstico inicial con el fin de presentar el nivel alcanzado mediante la culminación del plan de trabajo.

Actuar. se deberá ejecutar y/o mejorar el plan de acción sugerido por auditoria cumpliendo con la documentación y evidencias necesarias que permitan validar la ejecución y validación del mismo.

8 ANALISIS DE RESULTADOS

8.1 Diagnosticar el nivel de cumplimiento de los controles aplicables del anexo A. del estándar ISO 27001/2013, en BAINCOL SAS.

Esta etapa hace parte del desarrollo del primer objetivo del presente trabajo relacionado con la etapa del Planear del ciclo PHVA, para lo cual se ejecuta en 3 fases específicas, con el fin de definir de definir las actividades secuenciales, la interrelación y el resultado de cada una:
Fase I: Determinar el cumplimiento actual de los dominios del anexo A de la norma ISO/IEC 27001/2013 en la empresa.

Un análisis GAP es un método para evaluar las brechas entre los sistemas de información de una empresa o las aplicaciones de software para determinar si se cumplen los requisitos del negocio y, de no ser así, qué pasos se deben tomar para garantizar que se cumplan con éxito. [6]).

Para dar inicio a la aplicación de esta herramienta fue necesario determinar los interlocutores, cuáles serían áreas y/o cargos específicos con la responsabilidad de un proceso asociado a uno o varios de los controles de la norma, y que por su experticia en el tema fue clave para responder al cuestionario de cumplimiento de los controles del anexo A. del estándar, relacionados en la Tabla 1.

DOMINIO	INTERLOCUTORES
A5. Políticas de Seguridad de la Información	Oficial de Seguridad - Todas las áreas
A6. Organización de la Seguridad de la Información	Oficial de Seguridad
A7. Seguridad en los Recursos Humanos	Coordinadora de Recursos Humanos
A8. Gestión de Activos	Oficial de Seguridad y jefe de TI
A9. Control de Acceso	Gerente Administrativo y de Operaciones
A10. Criptografía	Jefe de Tecnología e Innovación
A11. Seguridad Física y del entorno	Gerente Administrativo y de Operaciones
A12. Seguridad en las Operaciones	Oficial de Seguridad y jefe de TI
A13. Seguridad en las Comunicaciones	Oficial de Seguridad y jefe de TI
A14. Adquisición, desarrollo y mantenimiento de sistemas de información	Jefe de Tecnología e Innovación
A15. Relación con Proveedores	Gerente Administrativo y de Operaciones
A16. Gestión de incidentes de seguridad de la información	Oficial de Seguridad y jefe de TI
A17. Gestión de la Continuidad del Negocio	Oficial de Seguridad - Todas las áreas
A18. Cumplimiento	Area Jurídica

Tabla 1 Interlocutores
Fuente: Elaboración propia

Una vez definidos los interlocutores, se aplicó el cuestionario teniendo en cuenta los niveles de madurez definidos en la Tabla 2.

5	**Optimizado**	Existe un control interno y continúo sobre la aplicación de controles y cumplimiento de requisitos. Se mide la eficacia de los controles estableciendo objetivos de mejora.
4	**Medible**	Existe un control interno sobre la aplicación de controles y cumplimiento de requisito.
3	**Definido**	Los controles están en su lugar y están documentados adecuadamente
2	**Ejecutado**	Los controles existen, pero no están documentados.
1	**Ad-hoc**	Existe cierto reconocimiento de la necesidad de control interno o requisito.
0	**No existencia**	No hay reconocimiento de la necesidad del control o requisito.

Tabla 2 Niveles de Madurez
Fuente: Análisis GAP ISO/IEC 27001

Los niveles de la organización son valorados en una escala de 0 a 5. [6] Como se muestra en la Tabla 2, donde se asigna un criterio a la valoración y su respectiva descripción para brindar al interlocutor las posibilidades necesarias para emitir una calificación objetiva.

El cuestionario aplicado corresponde a preguntas específicas sobre los controles con los que cuenta la organización actualmente, permitiendo seleccionar los criterios de respuesta acorde a los niveles de madurez antes mencionados. A continuación, se presenta un ejemplo de las preguntas correspondientes al dominio A.5 de la norma. Ver Tabla 3.

Cláusula	**ANEXO A ISO/IEC 27001/2013**
A5	**Políticas de Seguridad de la Información**
A.5.1	**Dirección de gestión para la seguridad de la información**
1	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?
2	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?

Tabla 3 Cuestionario Anexo A5. ISO/IEC 27001
Fuente: Análisis GAP ISO/IEC 27001

NIVELES DE MADUREZ					
No existente	**Ad-hoc**	**Ejecutado**	**Definido**	**Manipulable y Medible**	**Optimizado**
0	**1**	**2**	**3**	**4**	**5**
0					
0					

Tabla 4 Respuestas Cuestionario Anexo A5. ISO/IEC 27001
Fuente: Análisis GAP ISO/IEC 27001.

La Tabla 4 es la continuación de la Tabla 3. donde se pueden apreciar la respuesta obtenida de cada control perteneciente al dominio A.5 del estándar. El modelo del cuestionario es el mismo para todos los dominios. Se aplicó la cantidad de preguntas requeridas para evaluar cada uno de los controles requeridos por la norma.

A continuación, se promedian los datos resultantes de la calificación de los controles pertenecientes a cada dominio.

DOMINIO	**Suma total Dominio**	**Controles por dominio**	**Promedio**
A.5	0,00	2	0,00
A.6	1,00	7	0,14
A.7	3,00	7	0,43
A.8	1,00	10	0,10
A.9	3,00	14	0,21
A.10	0,00	2	0,00

A.11	8,00	13	0,62
A.12	4,00	16	0,25
A.13	0,00	6	0,00
A.14	0,00	13	0,00
A.15	1,00	5	0,20
A.16	0,00	7	0,00
A.17	0,00	4	0,00
A.18	4,00	8	0,50
		114	0,18

Tabla 5 Promedio de calificación por dominio- Cuestionario Anexo A5. ISO/IEC 27001
Fuente: Elaboración Propia.

De acuerdo con el resultado de la calificación promedio obtenida por cada dominio se evidencia una valoración de nivel de cumplimiento general de 0,18 puntos; razón por la cual se establecen los criterios de cumplimiento acorde a la situación actual de la organización expuestos en tabla 6.

De acuerdo con el resultado reflejado en la Fig. 1, el Oficial de Seguridad de la Información de la empresa BAINCOL SAS establece como nivel Definido, equivalente a 3 la calificación objetivo para evaluar ecuánimemente el cumplimiento de la empresa, referenciado en el Diagnóstico y Planificación de la Implementación del Modelo de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional de Cundinamarca – Car (Villamil, 2020). Debido al evidente grado de incumplimiento, por parte de la organización, que presenta ante los requisitos que sugiere el estándar internacional, los cuales deben ser evaluados con respecto a su grado de madurez actual.

Criterio	No cumple	Cumple parcialmente	Cumple
Valor	0	1-2	3

Tabla 6 Criterios de Cumplimiento
Fuente: Elaboración propia

Posteriormente se realizó la sumatoria total por dominio de las valoraciones obtenidas de acuerdo con los criterios definidos en la Tabla 6 permitiendo tener una noción de cumplimiento. Lo anteriormente expuesto se puede validar en la Tabla 7 de resultados:

Dominio	Cumple 3	Cumple Parcialmente 1-2	No Cumple 0	Total Controles
A.5	0	0	2	2
A.6	0	1	6	7
A.7	0	2	5	7
A.8	0	1	9	10
A.9	0	3	11	14
A.10	0	0	2	2
A.11	0	7	6	13
A.12	0	3	13	16
A.13	0	0	6	6
A.14	0	0	13	13
A.15	0	1	4	5
A.16	0	0	7	7
A.17	0	0	4	4
A.18	0	2	6	8
Total	0	20	94	114

Tabla 7 Resultados de cumplimiento
Fuente: Elaboración Propia

En la Tabla 7 se puede evidenciar que no se presentan calificaciones sobre 3. Lo que reduce el nivel de cumplimiento a un rango de 0 a 2, determinado por incumplimiento total o parcial del control. Con los datos obtenidos fue posible

graficar el nivel de cumplimento actual de cada dominio correspondiente al Anexo A. de la norma ISO/IEC 27001/2013 en la empresa BAINCOL SAS. Ver Fig. 1.

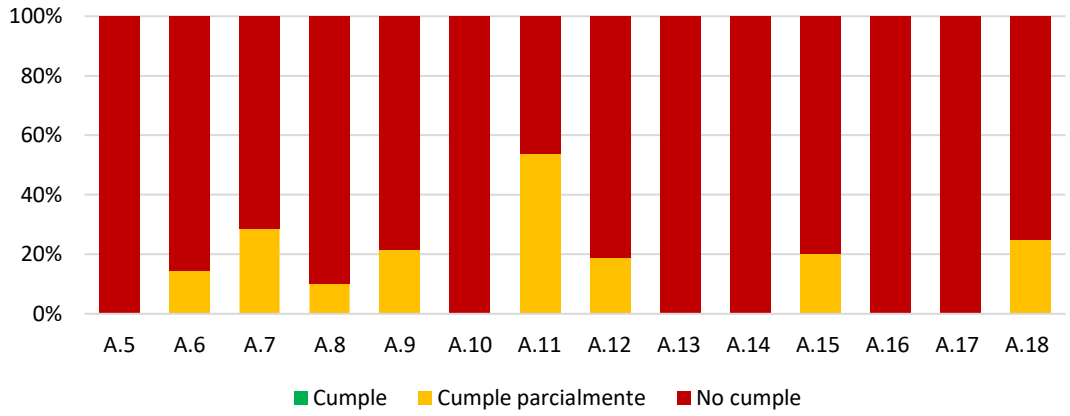


Fig.1 Niveles de cumplimiento Anexo A. ISO/IEC 27001
Fuente: Elaboración propia

De la Fig 1. es posible precisar que ningún dominio normativo cumple con los controles definidos. Por el contrario, los dominios A5, A10, A13, A14, A16 y A17 no son reconocidos como una necesidad para la organización lo que dificulta la evolución del nivel de madurez de la empresa en materia de Seguridad de la Información. Desde otro ángulo, se puede observar un cumplimiento parcial de los controles restantes, lo que sugiere que existen algunos controles aplicados actualmente pero no documentados o insuficientes. Sin embargo, indica un grado de importancia sobre la implementación del control, lo cual se puede mejorar por medio de la documentación y sensibilización.

DOMINIO	CALIFICACIÓN ACTUAL	CALIFICACIÓN OBJETIVO
A5. Políticas de Seguridad de la Información	0,00	3,00
A6. Organización de la Seguridad de la Información	0,14	3,00
A7. Seguridad en los Recursos Humanos	0,43	3,00
A8. Gestión de Activos	0,10	3,00
A9. Control de Acceso	0,21	3,00
A10. Criptografía	0,00	3,00
A11. Seguridad Física y del entorno	0,62	3,00
A12. Seguridad en las Operaciones	0,25	3,00
A13. Seguridad en las Comunicaciones	0,00	3,00
A14. Adquisición, desarrollo y mantenimiento de sistemas de información	0,00	3,00
A15. Relación con Proveedores	0,20	3,00
A16. Gestión de incidentes de seguridad de la información	0,00	3,00
A17. Gestión de la Continuidad del Negocio	0,00	3,00
A18. Cumplimiento	0,50	3,00

Tabla 8. Tabla de calificación actual de dominios en BAINCOL SAS
Fuente: Elaboración propia

Por otro lado, al relacionar esta información en la tabla 8 con los niveles de madurez definidos en la Tabla 2 es apropiado concluir que la empresa BAINCOL SAS se encuentra ubicado en un nivel de madurez 0 equivalente a “No existencia” con brechas de seguridad asociadas a cada dominio del estándar internacional.

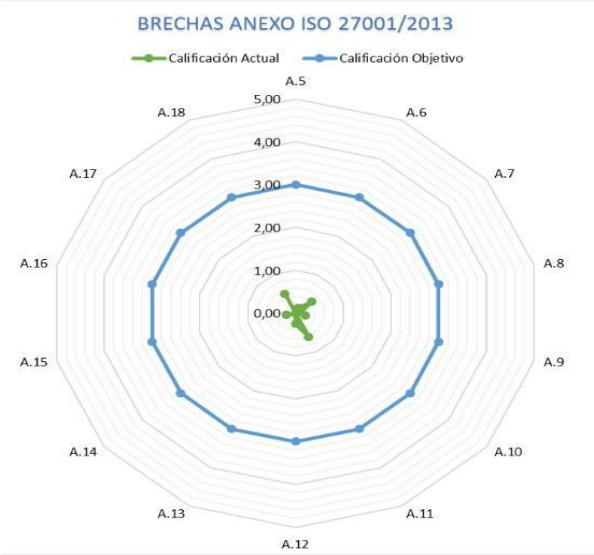


Fig. 2. Brechas Dominios Anexo A. 27001
Fuente: Elaboración propia

Al utilizar esta herramienta como mecanismo de autoevaluación para determinar el cumplimiento de Baincol SAS frente al anexo A de la norma ISO/IEC 27001/2013. Se logran establecer las brechas en materia de Seguridad de la Información con respecto a la calificación o nivel objetivo dado como punto de partida inicial de la organización, como lo muestra la Tabla 6. Es de aclarar que el nivel objetivo será directamente proporcional al nivel de madurez alcanzado por la organización de acuerdo con sus exigencias planteadas y evaluadas mediante auditoría interna. Esto quiere decir, que el nivel objetivo podrá ser modificado de acuerdo con los indicadores de mejora continua establecidos por la empresa.

Además, se logra establecer el nivel de cumplimiento y madurez visualizado como NO EXISTENTE dentro de la organización (como se ilustra en la Tabla 5) y que será el insumo para determinar la aplicabilidad de cada control o la exclusión de acuerdo con el contexto de la empresa, como desarrollo de la fase II.

Fase II: Realizar la declaración de aplicabilidad de los controles del anexo A. para la organización.

Como resultado del diagnóstico es posible afirmar que la organización no cumple con buenas prácticas en materia de Seguridad de la Información, por tal razón es indispensable establecer la aplicabilidad de los controles del estándar internacional acorde a sus actividades operacionales a fin de generar un fundamento que permita la adopción de estos, para garantizar la confidencialidad, integridad y disponibilidad de la información en Baincol SAS.

Para ello fue necesario recurrir a la matriz de riesgos gestionada por la organización, donde fue posible identificar los riesgos inherentes clasificados como graves asociados a seguridad de la información mencionando los siguientes:

Riesgos de Seguridad de la Información	
N°	**Descripción**
R1	Modificación o Alteración de la información (Integridad)
R2	Acceso no autorizado sobre la información (Confidencialidad)
R3	Pérdida total o parcial de la información (Disponibilidad)
R4	Multas y/o sanciones impuestas por la SIC por incumplimiento de la normatividad de Protección de Datos Personales.

Tabla 9. Riesgos de seguridad de la información en la empresa Baincol SAS
Fuente: Elaboración propia

Conforme al resultado del análisis de riesgos, es válido inferir que se tuvo en cuenta los controles planteados para la mitigación del impacto del riesgo vinculados a las causas establecidas y fueron el sostén para definir los controles aplicables a la organización.

Para efectuar la declaración de aplicabilidad, se realiza una lista de chequeo con la inclusión de los controles establecidos por el estándar internacional justificando la exclusión de los controles A9.4.5, A11.1.6, A14.2.6 descritos en la Tabla 10. Esta actividad es liderada por el Oficial de Seguridad de la Información, con la participación de los interlocutores definidos en la fase anterior. De manera simultánea, el área de Seguridad de la Información y el área de Tecnología Informática establecen los procesos documentales necesarios para dar cumplimiento a cada control aplicable.

APLICABILIDAD DE CONTROLES ANEXO A. ISO/IEC 27001/2013						
N°	**Categoría**	**Control**	**Aplica**		**Justificación**	**Doc. Ref.**
			Si	**No**		
A 9.4	Control de Acceso a Sistemas y Aplicaciones	**9.4.5.** Control de Acceso a Códigos Fuente de Programas		X	La organización no cuenta con desarrollos propios	N/A
A 11.1	Áreas Seguras	**11.1.6** Áreas de Despacho y Carga		X	La organización no cuenta con área de despacho y carga, de acuerdo con sus actividades operacionales.	N/A
A 14.2	Seguridad en los Procesos de Desarrollo y de Soporte	**14.2.6** Ambiente de Desarrollo Seguro		X	La organización no cuenta con ambiente de desarrollo.	N/A

Tabla 10 Aplicabilidad de controles Anexo A. ISO/IEC 27001
Fuente: Elaboración propia

Debido a la extensión de la información que contiene la aplicabilidad y justificación de todos los controles sugeridos por la norma, se presenta a modo de ejemplo el resultado de la exclusión de 3 controles determinados por la organización en la Tabla 10.

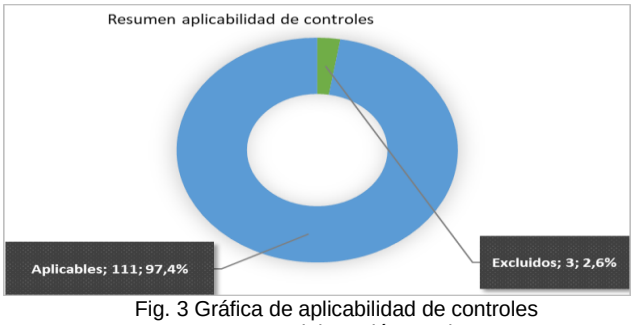


Fig. 3 Gráfica de aplicabilidad de controles
Fuente: Elaboración propia

En la Fig. 3 se puede ver representado que 3 de los 114 controles sugeridos por el estándar internacional, resultaron excluidos por la organización de acuerdo con la justificación indicada en la Tabla 10. Lo que refiere la adopción, por parte

de la empresa, de 111 controles. Esto corresponde al 2,6% de los controles excluidos Vs el 97.4% de controles aplicables determinados por Baincol SAS.

DOCUMENTO REFERENCIA	ALCANCE DE CONTROLES
Política se Seguridad de la Información.	A5.1.1/A5.1.2 A6.1.1/A6.1.2/A6.1.3 6.1.4/6.1.5 A17.1.1/A17.1.2/A17.1.3
Aseguramiento de Infraestructura Tecnológica	A6.2.1 A11.2.1/A11.2.2/A11.2.3 /A11.2.5/A11.2.6/A11.2.7 A11.2.8/A11.2.9 A12.2.1/A12.4.4/A12.5.1/A12.6.2
Teletrabajo y Trabajo en Casa	A6.2.2
Actualizar- "Reclutamiento, Selección y contratación de Personal".	A7.1.1/A7.1.2
Actualizar- "Inducción de nuevos colaboradores" Proceso Integral del Cargo (PIC)	A7.2.1/A7.2.2/A7.2.3
Actualizar- "Retiro de personal y liquidación definitiva".	A7.3.1
Gestión de Activos de Información Matriz de Inventario de Activos de Información	A8.1.1/A8.1.2/A8.1.3/A8.1.4 A8.2.1/A8.2.2/A8.2.3
Gestión de Medios de almacenamiento	A8.3.1/A8.3.2/A8.3.3
Control de Acceso a Redes e Infraestructura de TI	A9.1.1/A9.1.2/A9.4.1 A9.4.2/A9.4.3/A9.4.4
Gestión de Usuarios y Perfiles Gestión de Usuarios y Perfiles en Portales Bancarios Gestión de Usuarios Privilegiados Matriz de Roles y Perfiles	A9.2.1/A9.2.2/A9.2.3 A9.2.4/A9.2.5/A9.2.6/A9.3.1
Gestión de Cifrado de Información	A10.1.1/A10.1.2
Control de Acceso a Áreas Restringidas	A11.1.1/A11.1.2/A11.1.3 A11.1.4/A11.1.5/A11.1.6
Gestión de Hardware y Software	A11.2.4
Gestión de Servicios de Tecnología	A12.1.1/A15.1.1/A15.1.2 A15.1.3/A15.2.1
Gestión de Control de Cambios	A12.1.2 A14.2.2/A14.2.3/A14.2.4 A14.2.5/A14.2.7/A14.2.8/A14.2.9 A15.2.2
Gestión de Capacidad de TI	A12.1.3/A17.2.1
Gestión de Ambientes	A12.2.1 A14.3.1
Ejecución de Backups y Restauración de Datos	A12.3.1
Gestión de Logs de TI	A12.4.1/A12.4.2/A12.4.3
Gestión de Vulnerabilidades	A12.6.1
Manual de auditoría	A12.7.1
Gestión de la Seguridad de las Redes	A13.1.1/A13.1.2/A13.1.3 A14.1.1/A14.1.2 14.1.3
Transmisión de Información a Terceros	A13.2.1/A13.2.2/A13.2.3/A13.2.4
Gestión Integral de Incidentes de Seguridad de la Información	A16.1.1/A16.1.2/A16.1.3 A16.1.4/A16.1.5/A16.1.6/A16.1.7
Continuidad del negocio	18

Tabla 11 Relación de documentos referencia y controles
Fuente: Elaboración propia

En la Tabla 11 se consolida el resultado de los 111 controles aplicables asociados a los documentos de referencia propuestos como procesos por documentar por parte del área de Tecnología Informática y el área de Seguridad de la Información con el fin de dar alcance a los controles relacionados.

Posterior a la aplicación de la lista de chequeo, se formaliza la declaración de aplicabilidad de los controles para ser presentado por el Oficial de Seguridad de la Información a la Junta Directiva de Baincol SAS, quien otorga su aval de conformidad con lo manifestado y queda como evidencia mediante Acta realizada el 26 de marzo de 2020.

Se prosigue con la conformación de una mesa de trabajo comprendida por un grupo interdisciplinario de 4 áreas de la organización. Quienes, por su

conocimiento y experiencia en el negocio y la especialidad en su respectiva área, debatieron sus diferentes puntos de vista ante cada Subdominio del estándar Internacional, a veces coincidiendo en los criterios de priorización para la implementación.

ID	CARGO	ÁREA
1	Oficial de Seguridad de la Información	Seguridad de la información
2	Jefe de Tecnología e Innovación	Tecnología Informática
3	Coordinador de Organización y métodos	Organización y Métodos
4	Auditor	Auditoría

Tabla 12 Grupo Interdisciplinario
Fuente: Elaboración propia

Se procede a instaurar una escala de prioridad la cual fue tenida en cuenta como criterio de calificación para la implementación de los controles definidos en un periodo de tiempo descrito en la Tabla 13.

CRITERIO	CALIFICACIÓN	DESCRIPCIÓN	PERIODO DE IMPLEMENTACIÓN
Alto	5	El riesgo ocasionado por la ausencia del control representa un impacto muy significativo para la organización.	Hasta 6 meses
Medio	3	El riesgo ocasionado por la ausencia del control representa un impacto representativo para la organización.	6 a 12 meses
Bajo	1	El riesgo ocasionado por la ausencia del control no representa impacto significativo para la organización.	12 a 18 meses

Tabla 13 Escala de prioridad de implementación
Fuente: Elaboración propia

Las letras representan cada una de las áreas que participaron de la mesa de trabajo y la calificación otorgada por cada una, de la siguiente manera:

A) Auditoria
B) Tecnología Informática
C) Seguridad de la Información
D) Organización y Métodos

SUB DOMINIO	CONTROL	PRIORIDAD				
		A	B	C	D	R
A.5.1	Orientación de los Ejecutivos de Nivel Corporativo para la gestión de la seguridad de la información	3	5	3	5	4
A.6.1	Organización interna	3	3	1	3	2,5
A.6.2	Dispositivos Móviles (portátiles, tables y celulares)	3	5	1	3	3
A.7.1	Antes de asumir el empleo	1	1	3	1	1,5
A.7.2	Durante la ejecución del empleo	1	5	3	1	2,5
A.7.3	Terminación y cambio de empleo	1	3	3	1	2
A.8.1	Responsabilidad por los activos de información	3	5	3	5	4
A.8.2	Clasificación de la información	3	5	5		4
A.8.3	Manejo de medios de almacenamiento removible	3	3	3	3	3
A.9.1	Requisitos del negocio para el control de acceso	5	3	3	5	4
A.9.2	Gestión de acceso de usuarios	5	5	5	5	5
A.9.3	Responsabilidades de usuarios	5	5	3	5	4,5
A.9.4	Control de acceso a sistemas y aplicaciones	5	5	3	5	4,5
A.10.1	Controles criptográficos (Encripción y cifrado de información)	1	5	1	3	2,5
A.11.1	Áreas seguras / restringidas	3	5	1	3	3
A.11.2	Equipos de cómputo, impresoras y servidores	3	5	1	3	3
A.12.1	Procedimientos operacionales y responsabilidades	5	3	3	5	4
A.12.2	Protección contra códigos maliciosos	5	5	3	3	4
A.12.3	Copias de respaldo	5	3	3	5	4
A.12.4	Registro y seguimiento de operaciones en los sistemas	5	5	5	3	4,5
A.12.5	Control de software operacional	5	3	3	3	3,5

A.12.6	Gestión de vulnerabilidades / Pruebas Ethical Hacking	5	5	5	3	4,5
A.12.7	Consideraciones sobre auditorias de sistemas de información	5	3	1	5	3,5
A.13.1	Gestión de la seguridad de las redes	5	5	3	5	4,5
A.13.2	Transferencia / Transmisión de información	5	3	5	3	4
A.14.1	Requisitos de seguridad de los sistemas de información	1	5	3	5	3,5
A.14.2	Seguridad en los procesos de desarrollo y de soporte	1	3	3	5	3
A.14.3	Uso de datos productivos en ambiente de prueba	1	3	3	5	3
A.15.1	Seguridad de la información en las relaciones con los proveedores	1	5	5	3	3,5
A.15.2	Gestión de la presentación de servicios de proveedores	1	3	3	3	2,5
A.16.1	Gestión de incidentes de seguridad de la información	5	5	5	5	5
A.17.1	Continuidad de Negocio aspectos de seguridad de la información	5	5	3	5	4,5
A.17.2	Redundancias en loa sistemas - sistemas de recuperación de desastres	5	5	3	3	4
A.18.1	Cumplimiento de requisitos legales y contractuales	5	3	3	5	4
A.18.2	Revisiones de la política seguridad de la información	5	5	3	3	4

Tabla 14 Promedio de Priorización
Fuente: Elaboración propia

La Tabla 14 refleja el resultado de promediar el valor total de cada uno de los subdominios, ubicados respectivamente en la columna R.

- Alto: Mayor o igual a 4
- Medio: Mayor o igual a 3 y menor que 4
- Bajo: menor a 3

De esta manera se consolida la información y se presenta en un gráfico de prioridad de implementación.

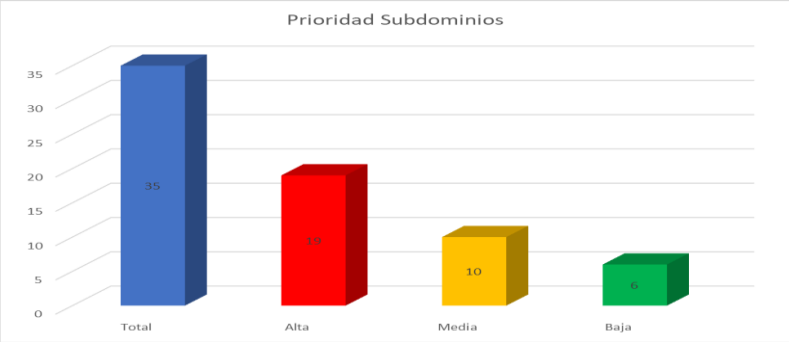


Fig. 4 Prioridad de Implementación Subdominios
Fuente: Elaboración propia

La Fig. 4 refleja el consolidado de la priorización con respecto a los subdominios del estándar internacional, esto indica que 19 de 35 subdominios fueron calificados con un nivel de implementación alto, los cuales contienen 60 de 111 controles definidos por la empresa. Esto quiere decir que el 54% de los controles aplicables a la organización se deberán implementar en un periodo máximo de 6 meses documentados a través de 19 procesos propuestos por el área de Tecnología Informática y Seguridad de la Información, sin mencionar los formatos, instructivos, manuales de usuarios, metodologías y/o matrices que resulten como anexo a cada proceso, esta información es el fundamento para establecer la fase final.

Fase III: Recomendar un plan de trabajo para la implementación de los controles aplicables para garantizar la Seguridad de la Información

El plan de trabajo propuesto para la implementación de los controles prioritarios definidos en la fase II, se realiza mediante un diagrama de Gannt donde se

establecen las actividades de documentación a desarrollar en un periodo de seis meses. Para esta última fase se tendrán en cuenta los dominios del estándar ISO/IEC 27001/2013 calificados con un rango de valor de 4 a 5, para el plan de trabajo se tendrán en cuenta los siguientes parámetros:

a) El tiempo estimado desde la documentación hasta la publicación de un proceso será de 1 semana laboral aproximadamente, consecuente con las actividades internas que demanda el proceso, este tiempo se ilustra mediante el siguiente flujo.

Fig. 5 Fujo de Elaboración y Publicación de documentos
Fuente: Elaboración propia

a. La implementación de los procesos en Baincol SAS, se debe realizar vez publicado y comunicado de manera formal el proceso por medio del buzón comunicaciones.
b. El seguimiento a la implementación debe ser realizado de manera trimestral posterior a la publicación.
c. La recopilación de información desconocida como matrices tendrán un tiempo definido de documentación de 1 semana laboral donde el flujo se centra en la recopilación de la información, la documentación y la revisión por el responsable del proceso. A pesar de que en este tipo de documentos no cuenta con publicación formal, debe haber una socialización con las áreas involucradas al proceso correspondiente.

PLAN DE TRABAJO		SEMANAS																																													
N°	ELABORACIÓN DE DOCUMENTOS	1		2		3		4		5		6		7		8		9		10		11		12		13		14		15		16		17		18		19		20		21		22		23	
		P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E
1	Política de Seguridad de la Información	1																																													
2	Gestión de Riesgos de Seguridad de la Información			1																																											
3	Matriz de Riesgos de SI y PdP					1																																									
4	Gestión de Activos de Información							1																																							
5	Inventario de activos de información GEMM									1																																					
6	Gestión Integral de Incidentes de Seguridad de la Información											1																																			
7	Matriz de Roles y Perfiles													1																																	
8	Gestión de Usuarios y Perfiles															1																															
9	Gestión de Usuarios Privilegiados																	1																													
10	Gestión de Usuarios en Portales Bancarios																			1																											
11	Ejecución de Backups y Restauración de Datos																					1																									
12	Aseguramiento de Infraestructura Tecnológica																							1																							
13	Control de Acceso a Redes e Infraestructura de TI																									1																					
14	Gestión de Servicio de Tecnología																											1																			
15	Gestión de Ambientes																													1																	
16	Gestión de Control de Cambios																															1															
17	Gestión de Logs de TI																																	1													
18	Gestión de la Seguridad de las Redes																																			1											
19	Gestión de Hardware y Software																																					1									
20	Gestión de Capacidad de TI																																							1							
21	Transmisión de Información con Terceros																																									1					
22	Continuidad del Negocio																																											1			
23	Gestión de Vulnerabilidades																																													1	
ACTIVIDADES EJECUTADAS			0		0		0		0		0		0		0		0		0		0		0		0		0		0		0		0		0		0		0		0		0		0		0
ACTIVIDADES PLANEADAS		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1	

Fig. 6 Plan de trabajo
Fuente: Elaboración Propia

La Fig.6 representa el plan de trabajo propuesto en 23 semanas para la estandarización de los respectivos procesos y la finalización de la etapa de planeación del presente proyecto. Este plan de trabajo permitirá realizar el control y seguimiento del avance y porcentaje de cumplimiento de acuerdo con los tiempos propuestos. El establecimiento de los controles prioritarios permitirá tener un control sobre las brechas de seguridad más importantes identificadas en la empresa Baincol SAS. No obstante, es necesario continuar con el proceso de implementación de los controles restantes con el fin de alcanzar un nivel de madurez que permita la instauración del Sistema de Gestión de Seguridad de la Información con enfoque a la mejora continua de cada uno de los procesos de la organización a través del monitoreo y evaluación del sistema.

8.2 Estandarizar los controles prioritarios en la empresa.

Esta etapa hace parte del segundo objetivo del presente trabajo y de la etapa del Hacer; tiene como propósito la estandarización de los procesos internos de la organización con el fin de dar cobertura a los controles prioritarios, previamente identificados mediante las actividades definidas por la organización a través del proceso PR-BIC-111 “Gestión de Documentos” el cual tiene por objeto: Elaborar, actualizar y socializar la información documentada por la organización, por medio del flujo descrito en la Fig.5.

Documentación: Esta actividad consiste en la documentación de cada uno de los procesos mencionados en el plan de trabajo tomando como referencia la norma internacional ISO 27002 adoptada por la organización como guía de buenas prácticas para implementar, mantener y mejorar la gestión de la Seguridad de la Información a través de controles documentados, como primer paso para la estandarización de los procesos del Sistema de Gestión de Seguridad de la Información [18] y futura integración con el Sistema de Gestión de Calidad. A pesar de que actualmente la organización no cuenta con un Sistema de Gestión de Calidad que sirva como base para la estandarización de proceso, cuenta con el proceso “Gestión de Documentos” el cual determina las directrices a tener en cuenta para la publicación y adopción de los procesos; por ello es importante denotar que la codificación, control de versiones y publicación de los documentos está a cargo del área de Organización y Métodos, previo Visto Bueno generado por cada responsable de revisión de acuerdo con el flujo ya mencionado. La publicación del documento va ligado al alcance del mismo, por ende, todas y cada una de las personas involucradas en la aplicación del proceso, son responsables de realizar la ejecución de los procedimientos definidos, así como, de llevar a cabo la implementación de los controles a partir de la fecha de emisión. Lo anterior con

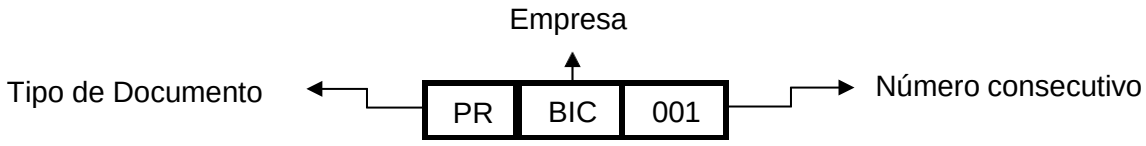
La codificación generada por el área de Organización y Métodos se lleva a cabo de acuerdo con el inventario existente y los consecutivos disponibles para asignación, de acuerdo con los siguientes parámetros definidos por la empresa, para este caso en específico fueron necesarios los siguientes:

DOCUMENTO	CÓDIGO
Manual	MN
Política	PT
Proceso	PR
Formato	FM
Planes	PN

Tabla 16. Extracto tipo de códigos
Fuente. Proceso PR-BIC-111 Gestión de Documentos BAINCOL SAS

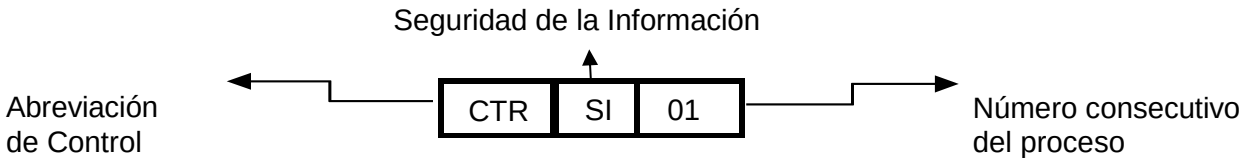
Adicionalmente, es necesario describir el código de la empresa a la cual pertenece el proceso. En casos especiales, existen documentos generados desde el Grupo Empresarial Mundo Mujer GEMM, con el fin de dar alcance a todas las empresas del Grupo (Excepto Banco Mundo Mujer). Lo anterior con el propósito de dar cobertura a temas transversales para la organización y que surtan como iniciativa para la implementación del SGSI en las demás empresas que componen el grupo.

Ejemplo de codificación:



Codificación de Controles de Seguridad de la Información:

Los controles identificados en cada documento serán codificados de la siguiente manera:



Clasificación y etiquetado de Documentos

La clasificación de los documentos se debe realizar de acuerdo con el nivel de confidencialidad de la información.

El dueño del documento debe realizar la clasificación de la información consignada y definir a quienes va dirigido teniendo en cuenta la siguiente información:

CLASIFICACIÓN	DESCRIPCIÓN
Documento Público	Son los documentos que pueden ser consultados de manera libre y sin restricciones. Ej. Política de Protección de Datos Personales, información del mapa de procesos.
Documento Privado	Es la información que debe ser usada únicamente por los funcionarios de la organización y hace referencia a: Procedimientos internos de operación, manuales o publicaciones internas. De uso exclusivo dentro de las instalaciones, su impresión es restringida y se puede usar como papel de reciclaje. Protección adecuada dado que la pérdida o fuga de ese tipo de información puede poner en riesgo procesos internos de la organización.
Documento Confidencial	Es la información más sensible relacionada con temas estratégicos del negocio y de clientes. Se refiere a la información que va dirigida exclusivamente a la dirección y las gerencias del GEMM. Debe tener una protección máxima dado que la pérdida o fuga de este tipo de información puede tener impacto a nivel económico, reputacional, legal, entre otros.
Documento Restringido	Es la documentación que debe ser usada únicamente por las áreas a las que se les ha autorizado el acceso, hace referencia a documentos que van dirigidos al personal o áreas específicas. Información que no debe salir de las instalaciones, su impresión es restringida. Sebe tener una protección adecuada dado que la pérdida o fuga de ese tipo de información puede poner en riesgo la imagen y los procesos internos de la empresa.

La etiqueta del documento clasificado como privado, restringido o confidencial deberá especificar su clasificación más el siguiente texto: “Este documento es propiedad intelectual del GEMM (exceptuando el Banco Mundo Mujer). Está prohibida su reproducción total o parcial, comercialización o divulgación sin previa autorización del propietario”.

Ejemplo de documento clasificado como Privado:

DOCUMENTO PRIVADO
Este documento es propiedad intelectual del GEMM (exceptuando el Banco Mundo Mujer). Está prohibida su reproducción total o parcial, comercialización o divulgación sin previa autorización del propietario.

La etiqueta del documento clasificado como público deberá especificar su clasificación más el siguiente texto: “Este documento es propiedad intelectual del GEMM (exceptuando el Banco Mundo Mujer)”.

Ejemplo de documento clasificado como Publico:

DOCUMENTO PÚBLICO Este documento es propiedad intelectual del GEMM (exceptuando el Banco Mundo Mujer).

A continuación, se relaciona los procesos elaborados durante la actividad de documentación con la respectiva codificación otorgada:

Item	Nombre del proceso propuesto	Nombre final	Código
1	Política de Seguridad de la Información	Política de Seguridad de la Información	PT-GEMM-009
2	Gestión de Riesgos de Seguridad de la Información	Gestión de Riesgos de Seguridad de la Información	PR-BIC-073
3	Matriz de Riesgos de SI y PdP	Matriz de Riesgos de SI y PdP	Sin Código
4	Gestión de Activos de Información	Gestión de Activos de Información	PR-BIC-067
5	Inventario de activos de información GEMM	Inventario de activos de información GEMM	FM-GEMM-028
6	Gestión Integral de Incidentes de Seguridad de la Información	Gestión de Incidentes de Seguridad de la Información	PR-BIC-056
7	Matriz de Roles y Perfiles	Matriz de Roles y Perfiles	FM-GEMM-034
8	Gestión de Usuarios y Perfiles	Gestión de Usuarios y Perfiles	PR-BIC-018
9	Gestión de Usuarios Privilegiados	Gestión de Usuarios Privilegiados	PR-BIC-057
10	Gestión de Usuarios en Portales Bancarios	Gestión de Usuarios y Perfiles en Portales Bancarios	PR-BIC-008
11	Ejecución de Backups y Restauración de Datos	Ejecución de Backups y Restauración de Datos	PR-BIC-050
12	Aseguramiento de Infraestructura Tecnológica	Aseguramiento de Infraestructura Tecnológica	PR-BIC-085
13	Control de Acceso a Redes e Infraestructura de TI	Control de Acceso a Redes e Infraestructura de TI	PR-BIC-108
14	Gestión de Servicio de Tecnología	Manual de Gestión de Servicios de TI	MN-BIC-006
15	Gestión de Ambientes	Gestión de Ambientes	PR-BIC-081
16	Gestión de Control de Cambios	Gestión de Control de Cambios	PR-BIC-054
17	Gestión de Logs de TI	Gestión de Logs de TI	PR-BIC-071
18	Gestión de la Seguridad de las Redes	Gestión de la Seguridad de Redes de Comunicación	PR-BIC-082
19	Gestión de Hardware y Software	Gestión de Hardware y Software	PR-BIC-072
20	Gestión de Capacidad de TI	Gestión de la capacidad de infraestructura de TI	PR-BIC-110
21	Transmisión de Información con Terceros	Intercambio de Información con Terceros	PR-BIC-070
22	Continuidad del Negocio	Plan de Continuidad del Negocio	PN-GEMM-001
23	Gestión de Vulnerabilidades	Gestión de Vulnerabilidades	PR-BIC-083
24	Teletrabajo	Teletrabajo-Trabajo en casa	PR-BIC-068

Tabla 17. Relación de Procesos documentados y codificados
Fuente. Elaboración propia

Revisión - responsable del Proceso: En este caso, el área de Seguridad de la Información y el área de Tecnología Informática tendrán la responsabilidad de validar que el proceso cuente con la directrices y procedimientos acordes a la actividad del negocio y alineados directamente con los controles sugeridos por el Anexo A del Estándar Internacional ISO 27001. La aprobación de los documentos será evidenciada a través de la firma de quienes revisan el documento en la primera tabla de la portada del documento.

Revisión- Área de Riesgos: La revisión realizada por el área de Riesgos a todos los procesos de la organización, se argumenta en la generación de

recomendaciones a los controles definidos para los riesgos del proceso y consignados en la matriz de riesgos operativos.

Revisión- Área de Organización y Métodos: Esta revisión es la final antes de enviar el documento a la respectiva aprobación por parte de los Gerentes de la organización, el área de Organización y Métodos tiene como responsabilidad validar que los procesos cumplan con los parámetros establecidos para su publicación, en materia de estructura y contenido general.

Aprobación Gerencial: Antes de la publicación para lectura y conocimiento de los documentos, las respectivas gerencias deben conocer el contenido y finalidad de la elaboración del documento y emitir su aprobación mediante firma en la tabla de la portada.

Publicación: Con las respectivas revisiones y aprobaciones por parte de las personas involucradas, el área de Organización y Métodos lleva a cabo la publicación del documento a través de correo masivo institucional dando alcance de acuerdo con el proceso. A partir de este momento cada involucrado en el proceso, deberá poner ejecución los procedimientos y controles establecidas.

Los documentos resultantes de esta etapa pertenecen al área de Seguridad de la Información y área de Tecnología Informática, no obstante, el monitoreo realizado al cronograma de documentación propuesto será liderado por el Oficial de Seguridad de la empresa Baincol, a fin de validar el cumplimiento del mismo y poder dar inicio de manera paralela al testeo de los controles asociados a los procesos de Tecnología Informática, por otro lado, el testeo de controles correspondientes al área de Seguridad de la Información serán llevados a cabo por el área de Riesgos, quienes vienen desarrollando está actividad de manera interna y continua para todos los procesos de la organización.

A continuación, se establecen los objetivos que debe cumplir cada uno de los procesos establecidos con el fin de dar alcance a los controles clasificados como prioritarios, referenciados en la norma ISO 27002.

PT-GEMM-009 Política de Seguridad de la Información: Determinar la estrategia, directrices, lineamientos y protección de los activos de información para preservar la confidencialidad, integridad y disponibilidad de estos, los cuales son parte fundamental en la ejecución de las actividades encaminadas al cumplimiento de los objetivos estratégicos de BAINCOL.

La política de seguridad de la Información de la empresa BAINCOL, contiene entre otras, políticas específicas como: Política de Escritorio Limpio, Dispositivos Móviles, Teletrabajo, entre otras.

PT-BIC-073 Gestión de Riesgos de Seguridad de la Información: Establecer la metodología para la identificación y gestión de riesgos de Seguridad de la Información y Protección de datos personales en BAINCOL.

Matriz de Riesgos de Seguridad de la Información y Protección de Datos Personales: Identificar y evaluar los riesgos de Seguridad de la Información y

Protección de Datos Personales, con el fin de establecer los controles necesarios para minimizar los riesgos inherentes al proceso.

PR-BIC-067 Gestión de Activos de Información: Identificar, clasificar y etiquetar los activos de información con el fin de valorar su nivel de importancia de acuerdo con los criterios establecidos por BAINCOL, para el adecuado manejo y gestión de los activos.

FM-GEMM-028 Inventario de activos de información: Identificar, listar, describir y clasificar cada uno de los activos de información con los que cuenta BAINCOL, con el fin de realizar la respectiva gestión de Riesgos.

PR-BIC-056 Gestión Integral de Incidentes de Seguridad de la Información: Definir los procedimientos para la gestión de incidentes de seguridad de la información, para todos los sistemas de información e infraestructura tecnológica de la empresa BAINCOL, con el fin de minimizar el impacto negativo en las actividades operacionales y la recuperación de la información para la continuidad del negocio.

FMM-BIC-034 Matriz de Roles y Perfiles: Establecer y controlar los accesos a los sistemas de información de BAINCOL con el fin de preservar la confidencialidad, integridad y disponibilidad de los datos.

Este documento contiene entre otros aspectos, la definición de los permisos vs cargo sobre: navegación Web, permisos de correo electrónico, aplicaciones, VPN, permisos de impresión, entre otros.

PR-BIC-018 Gestión de Usuarios y Perfiles: Gestionar las autorizaciones de acceso a los sistemas de información, infraestructura tecnológica y portales bancarios de la empresa BAINCOL, igualmente adelantar las actividades relacionadas con el monitoreo y control a los accesos otorgados dando cumplimiento con la Política de Seguridad de la Información.

PR-BIC-057 Gestión de Usuario Privilegiados: Estandarizar las actividades de creación, asignación y control de los usuarios privilegiados del área de Tecnología Informática, con el fin de mitigar los riesgos asociados de la empresa BAINCOL.

PR-BIC-008 Gestión de Usuarios y Perfiles en Portales Bancarios: Gestionar los accesos otorgados a los usuarios autorizados en los portales bancarios de las Entidades Financieras en las cuales la Empresa BAINCOL S.A.S., realiza transacciones electrónicas, a través de la creación, activación, modificación, inactivación o eliminación de usuarios que cuenten con roles de consulta, preparador, aprobador y permisos de modificación de cuentas asociadas; igualmente adelantar las actividades relacionadas con el ingreso de novedades en los portales bancarios para dar cumplimiento a las políticas de seguridad en el manejo de transacciones bancarias.

PR-BIC-050 Ejecución de Backups y Restauración de Datos: Garantizar el respaldo de cada uno de los activos de información de la empresa BAINCOL,

con el nivel de seguridad apropiado, estableciendo las actividades para realizar las copias de respaldo de la información almacenada en aplicaciones, infraestructura de servidores y el Firewall de la organización.

PR-BIC-085 Aseguramiento de Infraestructura Tecnológica: Establecer los lineamientos y actividades necesarias para asegurar la infraestructura Tecnológica, que proporcione confiabilidad a las operaciones de la BAINCOL.

PR-BIC-002 Control de Acceso a Redes e Infraestructura de TI: Definir los procedimientos necesarios para garantizar un adecuado control de acceso a la información a través de la red de datos corporativa e Infraestructura de BAINCOL.

MN-GEMM-006 Gestión de Servicio de Tecnología: Dar a conocer a las partes interesadas los principales servicios que se encuentran bajo la gestión y administración del área de Tecnología Informática de la empresa BAINCOL S.A.S.

PR-BIC-081 Gestión de Ambientes: Determinar los lineamientos en los ambientes de pruebas y producción con el fin de minimizar los riesgos de acceso o cambios no autorizados.

PR-BIC-054 Gestión de Control de Cambios: Establecer los lineamientos para realizar de manera planificada y segura los requerimientos que puedan afectar el normal desarrollo de la operatividad de la empresa BAINCOL, identificando los posibles riesgos asociados, con el fin de mitigar los impactos generados en materia de Seguridad de la Información.

PR-BIC-071 Gestión de Logs de TI: Establecer las actividades concernientes a elaborar, conservar y revisar regularmente los Logs acerca de actividades de usuarios, terceros, fallas y/o eventos de seguridad presentados en la infraestructura tecnológica y de redes en la empresa BAINCOL.

PR-BIC-082 Gestión de la Seguridad de las Redes: Definir los procedimientos necesarios para asegurar, controlar y monitorear el acceso a la información a través de la red corporativa del Grupo Empresarial Mundo Mujer, en adelante GEMM.

PR-BIC-072 Gestión de Hardware y Software: Establecer las actividades para mantener y actualizar el Hardware y Software de los equipos informáticos de la empresa BAINCOL, con el fin de garantizar su disponibilidad.

PR-BIC-107 Gestión de Capacidad de la Infraestructura TI: Establecer los planes de adquisición de recursos tecnológicos necesarios para soportar los requerimientos actuales y futuros de la infraestructura tecnológica de la empresa BAINCOL.

PR-BIC-070 Intercambio de Información con Terceros: Establecer los parámetros y procedimientos para el intercambio seguro de información con terceros que poseen alguna relación contractual con BAINCOL.

PN-GEMM-001 Continuidad del Negocio: Establecer los lineamientos que permitan que la empresa BAINCOL pueda recuperar sus procesos críticos en caso de un siniestro, evento de continuidad o desastre que interrumpa la normal actividad de sus operaciones.

PR-BIC-083 Gestión de Vulnerabilidades: Identificar, analizar y corregir de manera prematura, las vulnerabilidades presentadas en los activos de información pertenecientes a la empresa BAINCOL.

PR-BIC-068 Teletrabajo- Trabajo en Casa: Establecer las directrices y procedimientos para implementar de forma segura el servicio de teletrabajo o trabajo en casa, el cual permite al colaborador efectuar sus actividades en ubicaciones diferentes a las locaciones de la empresa; dando continuidad a las operaciones del negocio de BAINCOL.

Pese que este proceso no se encuentra dentro de la calificación de controles definidos como prioritarios, debido a situación sanitaria a nivel mundial con respecto al Sars Cov-2; este proceso tuvo que ser priorizado, con el fin de dar continuidad a las operaciones de la organización de manera remota.

Una vez documentados los procesos anteriormente mencionados, estos por los respectivos flujos de revisiones y aprobaciones para su posterior publicación y aplicación. Con el fin de validar los controles de manera secuencial a la formalización de los procesos, se definen los respectivos controles

8.3 Evaluar el nivel de madurez, en materia de Seguridad de la Información, en la organización mediante auditoría interna.

Esta etapa hace parte del tercer objetivo planteado del presente trabajo y de la etapa verificar del ciclo PHVA; concluye con la realización de la auditoría interna la cual es subcontratada con el fin de ser lo más objetivo posible con el resultado del mismo. Como evidencia de esta etapa, resulta el informe de auditoría generado al proceso de Seguridad de la Información basados en los niveles de madurez de la metodología GAP y referenciado en el estándar internacional ISO 27001/2013 con el objeto de realizar la comparativa del proceso de implementación de los controles prioritarios en la organización.

En esta etapa se debe tener en cuenta lo establecido por la Ley 87 de 1993 por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado, así como las previsiones de la ley 489 de 1998.

La auditoría interna determina si las políticas y procedimientos existen. También se revisa la eficacia de las políticas y procedimientos. Algunas guías generales para la auditoría incluyen:

- El cumplimiento de la política de Seguridad de la Información
- La implementación de los controles definidos
- La evaluación de la participación de los colaboradores
- El desarrollo de las responsabilidades

- La competencia y la capacitación de los colaboradores en SI
- La documentación del Sistema de Gestión de Seguridad de la Información
- La forma de comunicar la SG-SI a los trabajadores y su efectividad
- La planificación, desarrollo y aplicación de los controles de SI
- El alcance y aplicación de los controles de SI
- La supervisión y medición de los resultados
- Las acciones de mejora.

Adicionalmente, para fortalecer el avance de la implementación de los controles prioritarios se documenta el Proceso PR-BIC-077 “Monitoreo y Evaluación del SGSI”, donde se determinan directrices para el control y seguimiento del avance del presente proyecto como el inicio de la implementación del Sistema de Gestión de Seguridad de la Información, bajo la dirección del Oficial de Seguridad de la Información y Protección de Datos quien tendrá entre otras la siguiente responsabilidad:
El Oficial de Seguridad de la Información, Protección de Datos Personales y Calidad tiene la responsabilidad de realizar un informe mensual sobre la gestión de seguridad de la información y tratamiento de datos personales; este informe debe ser presentado a la Junta Directiva de la empresa de la empresa BAINCOL SAS, con el fin de soportar las decisiones, aprobar cambios y mejoras que se consideren necesarias.

El informe de gestión debe contener entre otros la siguiente información:

- Reporte de incumplimientos sobre la política de seguridad o la política de tratamientos de datos personales, incluyendo las sanciones aplicadas por estos motivos.
- Ejecución de testeo de los controles establecidos.
- Avance cronograma de documentación de procesos y controles

Auditoría del Sistema de Gestión de Seguridad de la Información

La auditoría del Sistema de Gestión de Seguridad de la Información, se realiza de acuerdo con las siguientes etapas:

Preauditoria: Esta etapa permite al ente auditor, comprender los procesos y objetivos de la empresa, con el fin de realizar un análisis general de la organización. Para ello se hace necesario enviar al ente auditor documentos organizacionales tales como: Misión y Visión de BAINCOL, Organigrama, PICs (Proceso Integral de Cargo) de las personas que conforman el área de Seguridad de la Información. Adicionalmente, se remiten documentos específicos al área, entre ellos: Política de Seguridad de la Información y los procesos documentados a la fecha. Ver tabla 17.

Plan de la Auditoría: En esta etapa se define el Objetivo, alcance, fechas y equipos que intervienen en la auditoria:

Objetivo: Evaluar la gestión de la Seguridad de la Información que realiza la empresa BAINCOL para la protección de la Información y su alineación con el

programa de Protección de Datos Personales.

Alcance: Está delimitado a evaluar a nivel de diagnóstico la gestión general del sistema de Seguridad de la Información de la empresa BAINCOL, frente a los diferentes riesgos que este posee y bajo la norma ISO 27001, teniendo en cuenta la necesidad real de la implementación de los controles sugeridos por esta norma.

Con el fin de llevar a cabo la primera auditoría del SGSI y validar el nivel de avance con respecto a la documentación de los controles del Sistema, se establece el inicio de la misma día 16 de noviembre y al 18 diciembre de 2020. Para ello la firma externa *Netx Audit & Consulting* confirma por medio de oficio formal al Oficial de Seguridad de la Información, Protección de Datos y Calidad las fechas para dar apertura a la auditoria en mención.

Equipo de trabajo: Los responsables de la organización para dar atención a los requerimientos de la Auditoría son: El Oficial de Seguridad de la Información, Protección de Datos y Calidad y la Pasante Universitaria del área.

Equipo Auditor: Se dan a conocer los integrantes por parte de la firma, quienes están comprendidos por un Auditor Líder y un Auditor de Apoyo.

Ejecución de la Auditoria: La ejecución de la auditoria da inicio mediante reunión formal de apertura en la cual participa el Gerente Administrativo y de Operaciones, el Oficial de Seguridad de la Información y Calidad, el Pasante Universitario de Seguridad de la Información. Esta etapa permite plantear la metodología, el tiempo de desarrollo de las actividades, presentación del equipo de trabajo y equipo Auditor; así como, la solicitud de los procedimientos de Seguridad y el análisis de los mismos.

Posteriormente, se lleva a cabo el análisis de la información y documentos previamente compartidos, con tal de realizar una comparativa que permita determinar la ejecución y puesta en marcha de lo descrito en la normatividad vigente.

Informe Final: El ente Auditor debe emitir un informe dirigido a la Gerencia General con copia al Oficial de Seguridad de la Información, Protección de Datos Personales y Calidad con los resultados de la auditoria, las causas y las recomendaciones emitidas.
Este documento será el punto primordial para dar inicio a la mejora continua de la implementación de los controles prioritarios definidos por la organización, no obstante, tendrá un panorama extenso teniendo en cuenta la necesidad y estructura organizacional.

Resultado obtenido: de conformidad con el resultado compartido por el ente auditor se obtiene los siguientes hallazgos:

ITEM	HALLAZGO	CAUSA	RECOMENDACIÓN
1	Fallas sobre los actuales m mecanismos de control para la extracción de información confidencial	Ausencia de medidas restrictivas para el acceso de servicios de almacenamiento en la nube y correos públicos a través de la red y equipos corporativos. Ausencia de medidas restrictivas para el monitoreo, detención y bloqueo de archivos con información confidencial a través del correo corporativo.	Establecer filtros que impidan el acceso a servicios de almacenamiento en la nube y correos electrónicos públicos a través de la red y equipos corporativos, utilizando las listas restrictivas propuestas por las herramientas de seguridad que posee BAINCOL. Establecer mecanismos para el monitoreo, detención y bloqueo de archivos de salida con información confidencial de BAINCOL a través del correo corporativo
2	Fallas sobre control de restricción y monitoreo para la instalación de programas no autorizados	Fallas en la configuración de controles preventivos para la instalación de programas. Puesta en operación de controles de monitoreo de software.	Evaluar la correcta configuración y funcionamiento de los controles preventivos de instalación de software en los distintos laptop y desktop de la compañía, que permita garantizar el correcto funcionamiento del control, sugerimos efectuar pruebas sobre el 100 de la población identificando la causa raíz del mal funcionamiento en algunos equipos. Sugerimos poner en marcha el control CTR SI 075 pata todo tipo de licenciamiento utilizado por BAINCOL por lo menos una vez año
3	Optimización del control de monitoreo del proveedor del servicio de Datacenter	Desconocimiento del correcto funcionamiento de este tipo de controles.	Teniendo en cuenta la criticidad del servicio ofrecido, recomendamos ejecutar de forma consistente el control CTR SI 052, permitiendo tener claridad del ambiente del control del proveedor en función de su servicio de datacenter, dicha evaluación debe contener: Evaluación del último período de auditoría, en lo posible cubrimiento de enero a diciembre de cada año. Evaluación del auditor independiente idóneo para la realización de este tipo de trabajos. Evaluación general del ambiente de control según lo descrito en el reporte (Evaluación del control interno)
4	Fallas sobre la identificación de activos de información y su gestión de riesgos	Madurez de la gestión de seguridad de la información.	Sugerimos actualizar el actual inventario de activos de información en conjunto con las áreas usarías contemplando entre otros los siguientes aspectos Incluir la identificación y análisis de activos de información sensibles para el GEMM como los intangibles, los servicios y equipos auxiliares Identificar por cada activo de información la base de datos de información personal con la que éste se relaciona en caso que aplique, e indicar las observaciones que apoyen el fortalecimiento de la gestión de datos personales Es importante exista una alineación entre los activos de información, el inventario de bases de datos y el Registro Nacional de Bases de Datos. Optimizar la referenciación entre las distintas pestañas del inventario de activos de información según su relación entre activos, a continuación algunas recomendaciones: Es requerido una vez realizado el análisis de riesgos para cada una de los activos considerados como críticos establecer los diferentes controles que apoyen a la mitigación tanto a nivel de probabilidad como de impacto partiendo de Controles ya establecidos según implementación

			del SGSI y recomendaciones de la norma ISO 27001 siempre y cuando sean aplicables Controles de mayor detalle requeridos para controlar la integridad, confidencialidad y disponibilidad de la información personal procesada por el activo de información evaluado, dichos controles son muy específicos para cuidar los datos personales e igualmente pueden ser automáticos (de aplicación o manuales (operativos)
5	Optimización de controles sobre el SGSI	Madurez de la gestión de seguridad de la información.	Recomendamos efectuar una revisión de detalle sobre el actual inventario de controles declarados en el SGSI, específicamente sobre los 50 controles descritos en el Anexo 4 de este mismo informe, permitiendo tomar los correctivos que sean necesarios para la optimización del sistema de gestión de seguridad de la información (SGSI). Un paso importante para el 2021 como parte de la mejora continua y luego de la definición, documentación e implementación de controles, es la ejecución de testeo sobre los controles declarados en el SGSI, para el cual recomendamos realizar una revisión por grupo de controles de forma mensual y por lo menos dos pruebas de cada control al año según sea requerido Es importante el SGSI deje evidencia de los distintos testeos realizados, las observaciones encontradas y los planes de acción atendidos para la mejora de los controles

Tabla 18. Relación de Hallazgos de Auditoria
Fuente. Elaboración propia

De acuerdo con la información anterior y los hallazgos identificados por Auditoria, es posible precisar que los hallazgos 1,2,3 de la tabla 18. Son específicos para algunos dominios tal como se relaciona en la siguiente tabla:

Hallazgo	Dominio/Subdominio
1	A.12 Seguridad de las operaciones
2	A.12 Seguridad de las operaciones
3	A. 15 Relación con los proveedores A. 17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio
4	A. 8 Gestión de Activos
5	Numeral 10 ISO 27001 Mejora

Fig. 19 Relación de Hallazgos con los Dominios/Subdominios de la ISO 27001/2013
Fuente. Elaboración Propia

Teniendo en cuenta la relación anterior, es posible diferir que los hallazgos identificados por auditoría corresponden a controles prioritarios determinados por la organización, los cuales cuentan con puntos de mejora y para lo cual se emiten las recomendaciones pertinentes, con el fin de fortalecer los controles y llegar a la calificación objetivo definida al inicio del proyecto. Para ello es necesario corregir los hallazgos identificados mediante la fase del Actuar donde, adicionalmente, se realizará el respectivo plan de Acción.

8.3.1 Desarrollar el Plan de Acción

Esta etapa es pieza clave para el cierre del presente trabajo y corresponde a la etapa del Actuar del ciclo PHVA, ya que, se definen las acciones a tomar con el fin de corregir y mejorar cada uno de los hallazgos de la auditoria.

En esta fase se detalla el plan de acción, por el cual se describe la manera de llegar al nivel objetivo o superarlo, para ello es necesario que la organización inicie la implantación de mejoras identificadas por parte de la auditoría o por sí mismos, estableciendo una cultura de mejora continua.

Plan de Acción: Esta etapa permite conocer y definir el plan de acción ante los hallazgos identificación por el equipo auditor. Para ello, se definen las actividades y los responsables requeridos para dar cumplimiento a cada una de las acciones correctivas dispuestas.

ITEM	HALLAZGO	PLAN DE ACCIÓN	RESPONSABLE
1	Fallas sobre los actuales mecanismos de control para la extracción de información confidencial	1. Se establecerán los filtros a través de directorio activo que impidan el acceso no autorizado a los servicios de almacenamiento en la nube y correos electrónicos públicos en los equipos corporativos, a través de la red interna y externa. 2. Se establecerán mecanismos básicos para el monitoreo, detención y bloqueo de archivos de salida con información confidencial del GEMM a través del correo corporativo utilizando las políticas de seguridad disponibles para el licenciamiento disponible de O 365.	Oficial de Seguridad de la Información y Calidad / Jefe de Tecnología e Innovación
2	Fallas sobre control de restricción y monitoreo para la instalación de programas no autorizados	1. Se implementará un doble control a través de la política de directorio activo y la funcionalidad de ejecución de procesos de instalación de cylance que permita garantizar el correcto funcionamiento del control de instalación de software.	Oficial de Seguridad de la Información y Calidad / Jefe de Tecnología e Innovación
3	Optimización del control de monitoreo del proveedor del servicio de Datacenter	1. Anualmente en el mes de abril se ejecutará la evaluación del proveedor Claro en función de su servicio de datacenter, para ello se solicitará el reporte ISAE 3402 y se procederá a enviar el respectivo informe a la Jefatura de TI, esto partiendo que el reporte es suministrado por Claro en el mes de marzo.	Oficial de Seguridad de la Información y Calidad
4	Fallas sobre la identificación de activos de información y su gestión de riesgos	1. Se actualizará el proceso PR BIC 067 Gestión de activos de información y el Inventario de Activos de Información de acuerdo con las recomendaciones recibidas por la Auditoría. 2. Se modificará la metodología de Clasificación de los Activos de Información, incluida en el PR BIC 067, efectuando una priorización de los activos. 3. Se actualizará el proceso el PR BIC 073 Gestión de riesgos de seguridad de la información con el fin de que contemple los controles del sistema. 4. Se efectuará la evaluación de riesgos detallada por cada activo de información. 5. Se definirá para los activos Datos de información una pestaña de clasificación de la información de acuerdo con los criterios sugeridos.	Oficial de Seguridad de la Información y Calidad
5	Optimización de controles sobre el SGSI	1. Se efectuará una revisión detallada sobre el actual inventario de controles declarados en el SGSI. 2. Se ejecutará el testeo sobre los controles declarados en el SGSI, realizando una revisión por grupo de controles de forma mensual y dos pruebas de cada control al año según sea requerido.	Oficial de Seguridad de la Información y Calidad

Tabla 20. Relación Plan de Acción
Fuente. Elaboración propia

A partir del diagnóstico, se pretende alcanzar el nivel 3 en madurez de la organización en materia de Seguridad de la información, dando cumplimiento a 60 controles prioritarios de 111 aplicables a la organización y 19 subdominios de 35 establecidos por el anexo A. del estándar internacional ISO 27001/2013; acreditados a través de 23 documentos formales de acuerdo con lo establecido por la organización.

Como resultado de la primera auditoría realizada a la implementación de los controles prioritarios de la ISO 27001/2013 en BAINCOL, el ente auditor emite mediante informe seccionado en 3 partes:

- Objetivos y Alcance
- Informe Ejecutivo
- Resumen Ejecutivo,

Los hallazgos identificados durante la actividad y emite las sugerencias respectivas en pro de la mejora continua del sistema de gestión y la evolución en el nivel de madurez corporativo. Para ello describe mediante gráfica comparativa el resultado general de los dominios de la norma con respecto al promedio del nivel multiindustria nacional.

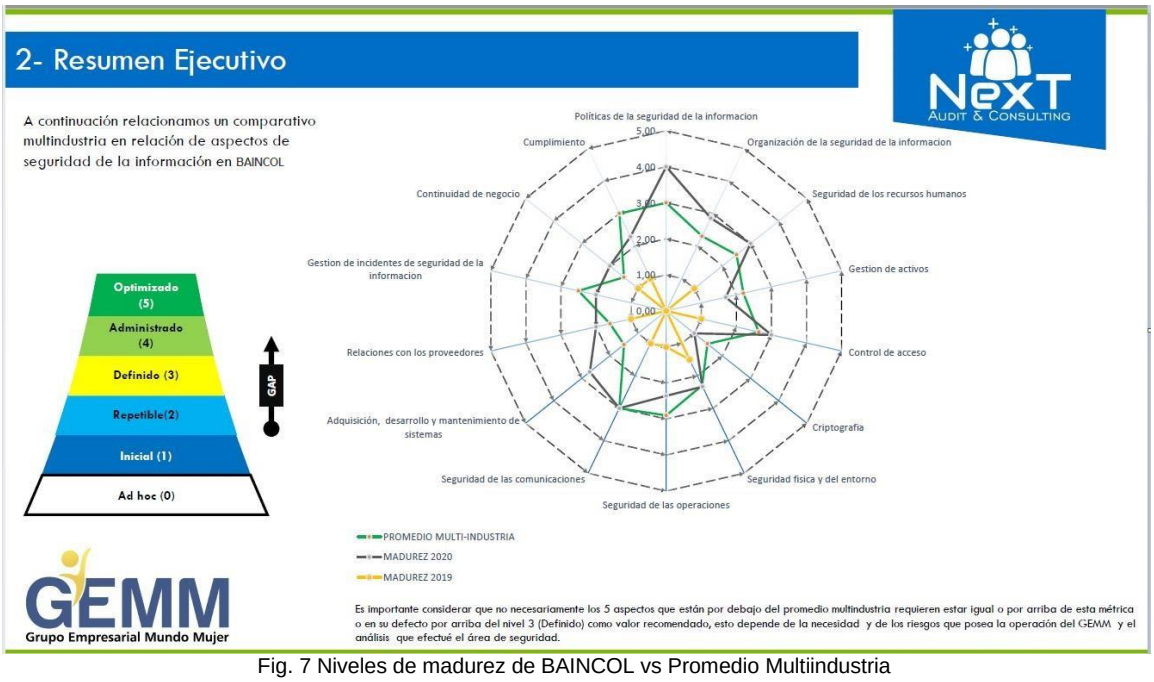


Fig. 7 Niveles de madurez de BAINCOL vs Promedio Multiindustria
Fuente: Informe de Auditoria NEXT Audit & Consulting

El análisis de la Fig. 7 se llevará a cabo en relación con los controles prioritarios definidos en la fase del diagnóstico del presente proyecto; no obstante, la calificación objetivo aplica para todos los dominios de la norma.

En la Fig.7 se puede apreciar los niveles de madurez de la empresa BAINCOL frente al promedio registrado por las empresas industriales Colombianas de lo cual podemos concluir lo siguiente:

Es posible evidenciar que los dominios de A. 8 Gestión de Activos y A.12 Seguridad de las Operaciones, los cuales hacen parte de los dominios prioritarios para implementación, se encuentran por debajo de la calificación objetivo definida por la organización, así como, del nivel promedio multiindustria, los cuales hacen parte de los hallazgos y recomendaciones emitidas por el equipo auditor con un nivel de madurez de 2,2 y 1,8 respectivamente Adicionalmente, se puede validar que el dominio A. 16 Gestión de Incidentes de Seguridad de la Información, se encuentra en un nivel de madurez 2 sin embargo, no es posible evaluar la eficacia del proceso documentado debido a la ausencia de Incidentes en la organización durante el periodo auditado.

A manera de llevar a cabo de manera exitosa el desarrollo del plan de acción, es necesario contar con el apoyo del área de Tecnología Informática de BAINCOL SAS para la implementación de las recomendaciones técnicas emitidas en los hallazgos 1 y 2. Por otro lado, para la remediación de los hallazgos 3,4 y 5, es necesario contar con el personal del área de Seguridad de la Información para dedicar su esfuerzo al cierre de las recomendaciones a los dominios ya mencionados, con el propósito de cumplir con todas las actividades en un periodo máximo de 4 meses a partir de la emisión del informe final de auditoria.

Validación cierre de hallazgos

Posterior a la implementación del plan de acción definido durante la etapa del Actuar, se lleva a cabo una sesión de trabajo con el equipo auditor a fin de evidenciar la ejecución de los planes de acción propuestos y la efectividad de los mismos en las fechas propuestas.

Actividades de Cierre para el Hallazgo 1 y 2:
Con el fin de mitigar la instalación de software sin autorización por parte de los colaboradores del GEMM, en el Directorio Activo de la Infraestructura Tecnológica se crea con una Política que solo permite realizar las instalaciones a los usuarios que se encuentren en el grupo Administrator_desktop. Los permisos de inclusión al grupo mencionado, deben ser solicitados por el área de Tecnología Informática a través de la mesa de servicio y suministrados por el área de Seguridad de la Información, para la atención de requerimientos específicos; esta se encuentra desplegada sobre toda la Unidad Organizativa del BAINCOL.

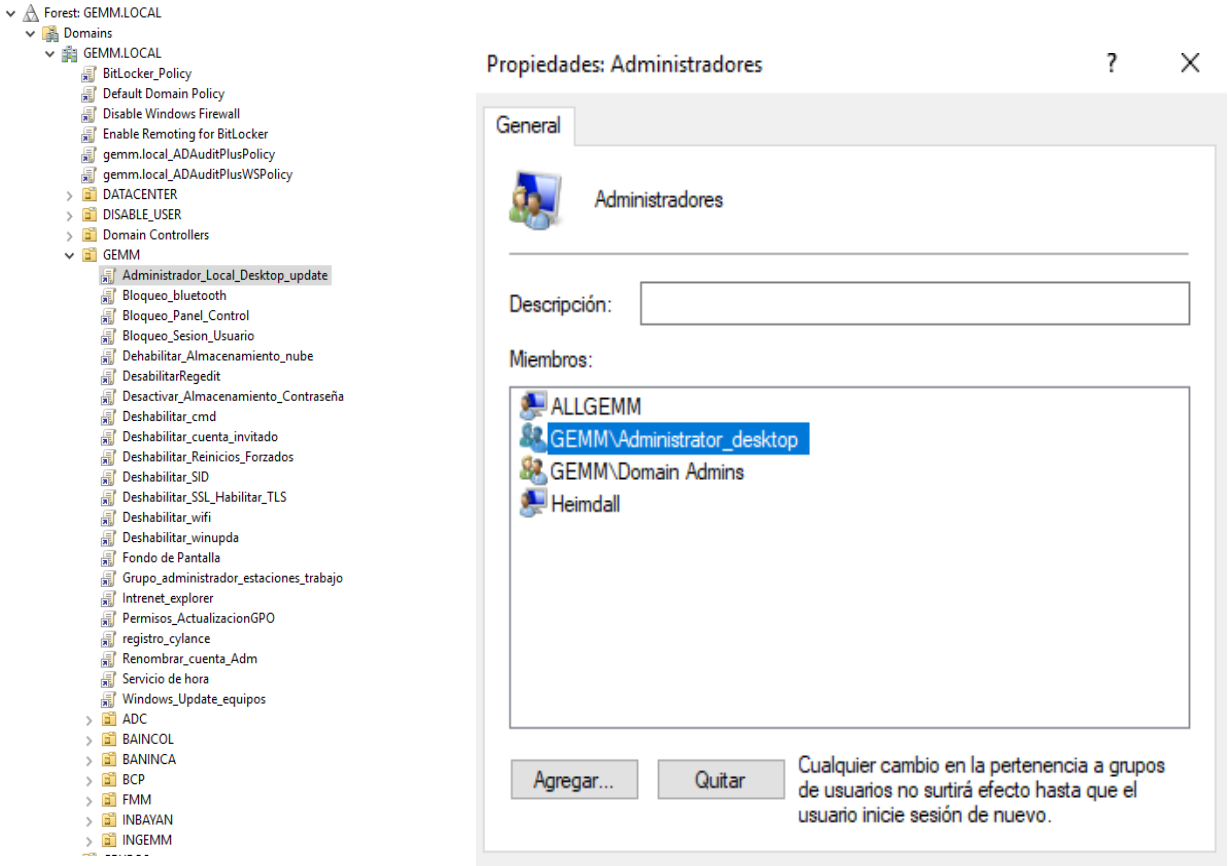


Fig. 8 Política de Administrador_desktop
Fuente: Directorio Activo Baincol

A través del Antivirus gestionado por la organización, se generan políticas para segregar diferentes permisos sobre los servidores y equipos de red con el fin de restringir el uso de dispositivos de almacenamiento tales como: DVD, CD, USB, etc. Mediante políticas sobre la navegación Web se prohíbe el acceso a correos gratuitos, personales y/o almacenamientos de nube con el fin de minimizar la extracción no autorizada de información.

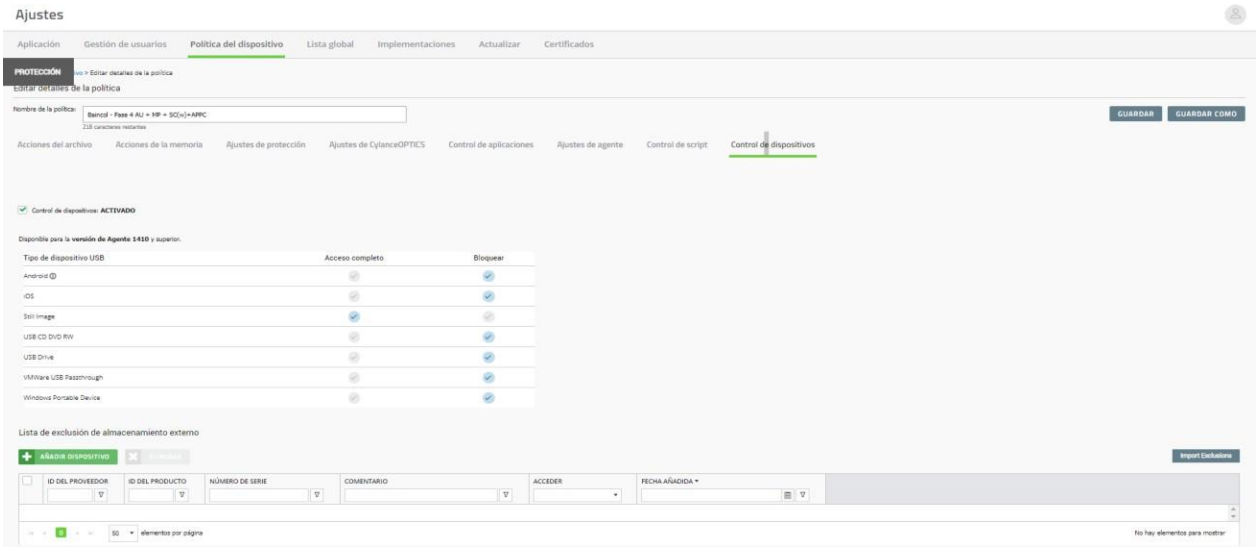


Fig. 9 Política de restricción dispositivos de almacenamiento
Fuente: Antivirus Baincol

Por medio del licenciamiento Office 365, se crean las etiquetas de clasificación de correos, para la identificación y control de salida de información, de acuerdo con los criterios ya definidos y mencionados en el numeral 8.2 del presente trabajo: Documento Público, Documento Privado, Documento Restringido. Evidencia de remediación:

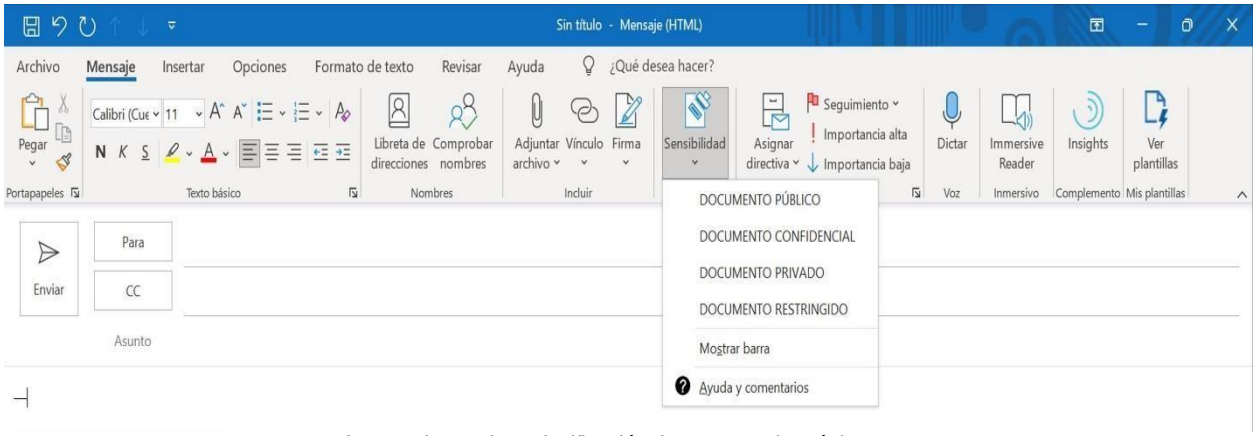


Fig. 10 Etiquetado y Clasificación de Correos electrónicos
Fuente. Microsoft Office 365

Actividades de Cierre para el Hallazgo 3:
La organización a través del Oficial de Seguridad de la Información y Protección de Datos, solicita como parte de la evaluación de proveedores, proveedores el informe llamado ISAE () a los proveedores críticos, considerados así, debido a los servicios que prestan y/o la información que gestionan. Este informe detalla los lineamientos de seguridad llevados a cabo por el proveedor y sus planes de contingencia ante los posibles riesgos.

Actividades de Cierre para el Hallazgos 4:
Para este hallazgo fue necesario actualizar el proceso PR-BIC-067 Gestión de Activos de Información, en el cual se unifica el proceso PR-BIC-073 Gestión de Riesgos de Seguridad de la Información, con el fin de definir la metodología para gestionar los riesgos asociados a cada tipo de activo identificado, del mismo modo, se realiza la actualización e inclusión de los activos de información siguiendo las recomendaciones del ente auditor, para lo cual se definen la identificación de los activos de información, por sujeto. Posteriormente se realiza la priorización los mismos y la identificación de los activos de información que contienen datos personales.

Actividades de Cierre para el Hallazgo 5:
Como plan de remediación a este hallazgo, se lleva a cabo una revisión detallada de los 111 controles aplicables a la organización y documentados a través de los 23 procesos referidos en el presente proyecto, para lo cual se adoptan las recomendaciones de Auditoría con el objeto de realizar la consolidación de controles de acuerdo con su naturaleza, objetivo y periodicidad. De esta manera se optimiza el proceso de monitoreo al Sistema de Gestión de Seguridad de la Información, sin desatender ningún control sugerido por la norma y aplicable a la organización.

Anexo Informe Final:

Posterior a la evaluación del plan de acción, el ente auditor genera un informe anexo al informe inicial, donde integra las evidencias recopiladas durante la respectiva validación. No obstante, durante el periodo de remediaciones se continua con el proceso de madurez de todos los controles establecidos en el SGSI a fin de mejorar el nivel de madurez referido en el informe de Auditoria.

Como resultado del plan de acción y bajo el acompañamiento del ente Auditor se genera la segunda versión del Diagnóstico GAP implementado en el primer objetivo del presente proyecto, para lo cual de acuerdo con las evidenciados entregadas y la evaluación de los controles, se representa la siguiente información:

N°	Dominio	Interlocutores	Calificación Actual	Calificación Objetivo
A.5	A5. Políticas de Seguridad de la Información	Oficial de Seguridad - Todas las áreas	4,00	3,00
A.6	A6. Organización de la Seguridad de la Información	Oficial de Seguridad	3,57	3,00
A.7	A7. Seguridad en los Recursos Humanos	Coordinadora de Recursos Humanos	3,71	3,00
A.8	A8. Gestión de Activos	Oficial de Seguridad y Jefe de TI	3,30	3,00
A.9	A9. Control de Acceso	Gerente Administrativo y de Operaciones	3,57	3,00
A.10	A10. Criptografía	Jefe de Técnología e Innovación	2,00	3,00

A.11	A11. Seguridad Física y del entorno	Gerente Administrativo y de Operaciones	3,54	3,00
A.12	A12. Seguridad en las Operaciones	Oficial de Seguridad y Jefe de TI	3,81	3,00
A.13	A13. Seguridad en las Comunicaciones	Oficial de Seguridad y Jefe de TI	3,57	3,00
A.14	A14. Adquisición, desarrollo y mantenimiento de sistemas de información	Jefe de Técnología e Innovación	2,64	3,00
A.15	A15. Relación con Proveedores	Gerente Administrativo y de Operaciones	3,40	3,00
A.16	A16. Gestión de incidentes de seguridad de la información	Oficial de Seguridad y Jefe de TI	3,29	3,00
A.17	A17. Gestión de la Continuidad del Negocio	Oficial de Seguridad - Todas las áreas	3,00	3,00
A.18	A18. Cumplimiento	Área Jurídica	3,25	3,00
			3,33	

Tabla 21. Promedio de calificación por dominio- Cuestionario Anexo A5. ISO/IEC 27001- Año 2021
Fuente: Elaboración Propia.

En la Tabla 20. Se pueden evidenciar la calificación obtenida por cada uno de los dominios y el promedio general del Anexo A de la ISO 27001 posterior a la implementación de los controles prioritarios durante el ciclo de mejora continua.

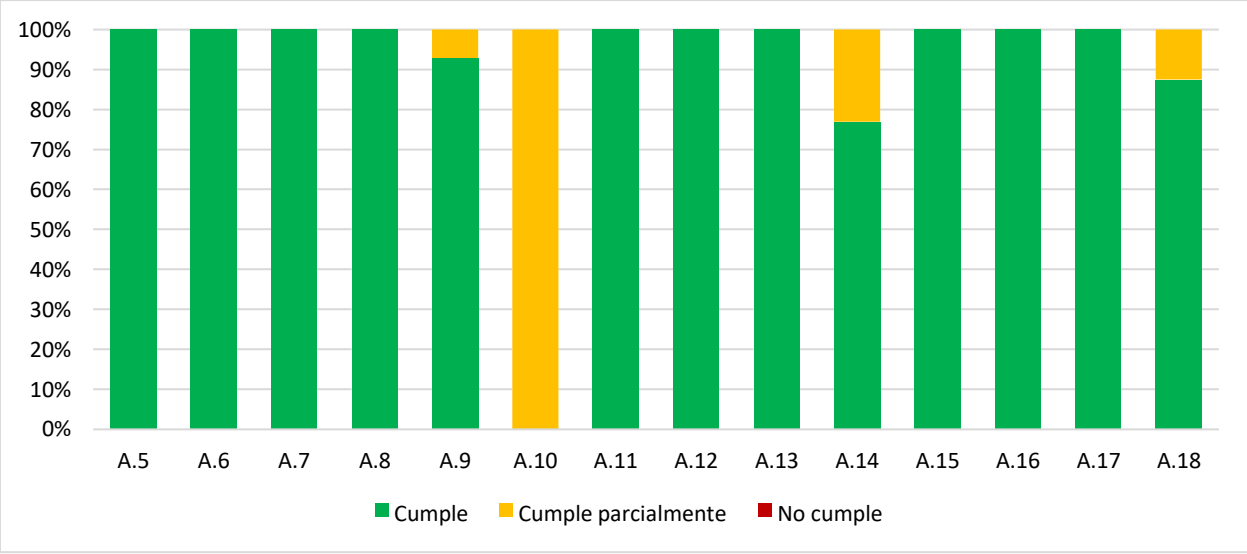


Fig.8 Niveles de cumplimiento Anexo A. ISO/IEC 27001 – Año 2021
Fuente: Elaboración propia

En la Fig.8 podemos validar el nivel de cumplimiento de los dominios del Anexo A de la ISO 27001 indicando como calificación objetivo el nivel 3 de madurez con respecto a la metodología GAP. Entre ellos, podemos destacar el dominio A.10 el cual la organización cumple parcialmente, debido a que el grado de exigencia de este criterio no es considerado relevante para la organización acorde con su actividad económica.

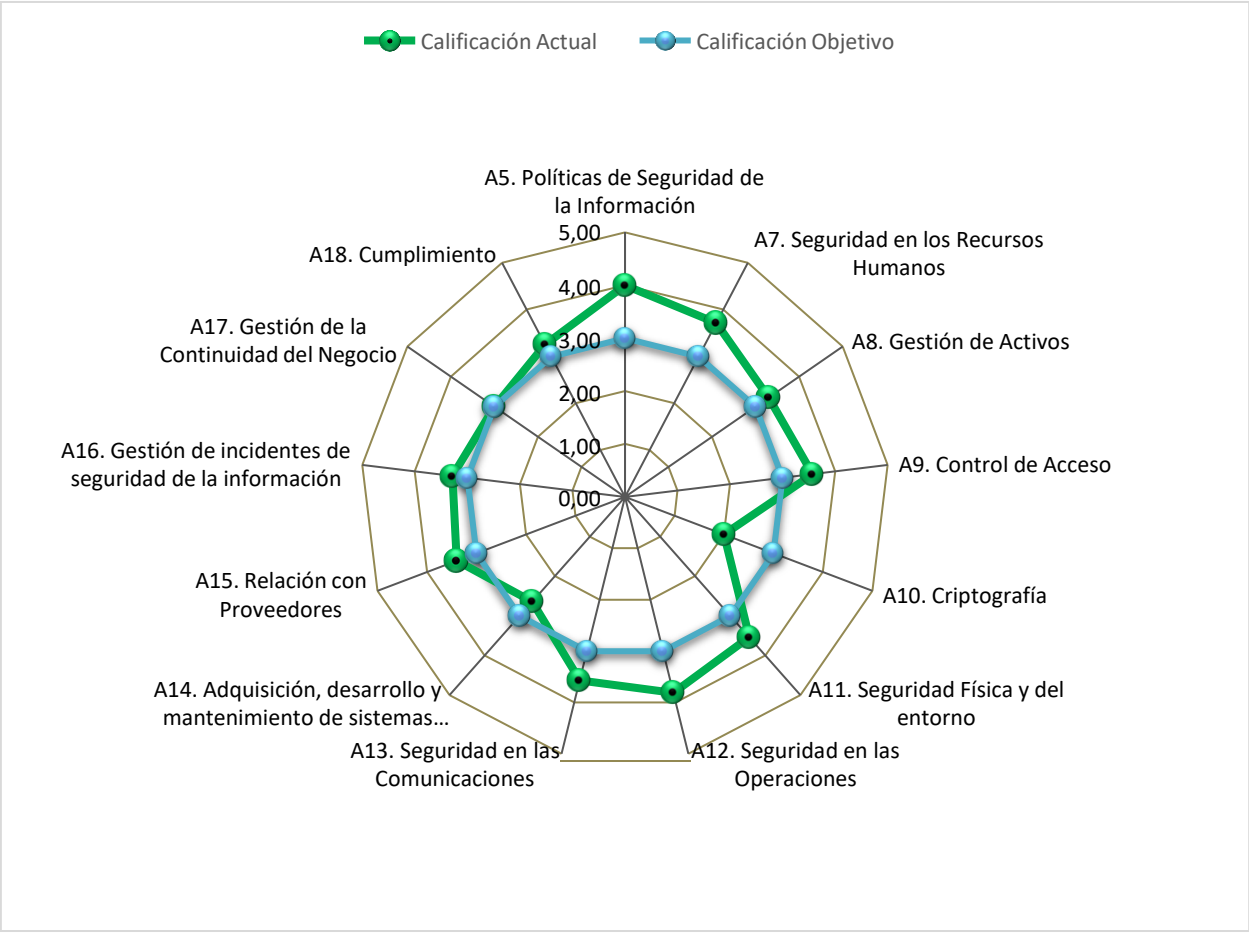


Fig. 9. Brechas Dominios Anexo A. 27001- Año 2021
Fuente: Elaboración propia

Gracias a la Fig. 9 se puede visualizar el nivel alcanzado por la organización posterior a la implementación de los controles prioritarios a través de la metodología PHVA, dejando como evidencia del nivel de madurez a la fecha de verificación.

9 CONCLUSIONES

El diagnóstico realizado en la empresa Baincol SAS, permitió determinar que actualmente la organización no cumple con los controles de seguridad de la información sugeridos por la ISO/IEC 27001/2013, reflejados en el nivel de madurez frente a la calificación objetivo definida, la cual se encuentra en 0,18 puntos de 3 esperados por la organización. lo que se denomina un nivel de madurez “No existente” detectando brechas de seguridad de la información asociadas a cada uno de los 35 dominios de la norma.

Mediante la “Declaración de aplicabilidad” fue posible justificar la exclusión de 3 controles sugeridos por la norma: 9.4.5 Control de Acceso a Códigos Fuente de Programas, 11.2.6 Áreas de Despacho y Carga y 14.2.6 Ambiente de Desarrollo Seguro. Lo que quiere decir que el 97,4 % de los controles de la norma son aplicables vs 2,6% excluidos por la organización.

El proceso PR-BIC-111 Gestión de Documentos, fue pieza clave en la estandarización de los procesos, ya que, fue referente documental para implementación y socialización de cada uno de los documentos elaborados.

Como resultado de esta fase, se implementaron 24 documentos los cuales contienen 62 controles de 60 propuestos en la etapa del planear, cada proceso cuenta con el respectivo código y versión generado desde el área de Organización y métodos haciendo parte de manera activa del ciclo PHVA del SGSI, como implementación inicial de los controles sugeridos por la norma.

La evaluación posterior a la implementación de los controles prioritarios del Anexo A de la ISO 27001, logra reflejar un promedio general de 3.3 con respecto a 0.18 puntos obtenidos durante la etapa de Diagnóstico, posicionando la organización en el nivel de madurez “Definido”; alcanzando y superando, para casos específicos, la calificación objetivo planteada inicialmente.

Es importante ratificar la importancia de la implementación de los controles de la norma a través del ciclo PHVA, evidenciando el crecimiento y madurez posterior a la implementación de todas sus fases, en pro del mantenimiento y la mejora continua.
Debido a la situación sanitaria mundial ya conocida por todos, el plan de trabajo del presente proyecto se llevó a cabo en un tiempo mayor al dispuesto inicialmente, a fin de cumplir con las fases del Verificar y Actuar como se dispuso en el objetivo general.

10 RECOMENDACIONES

Con el fin de mejorar el nivel de madurez del Sistema de Gestión de Seguridad de la Información, se recomienda evaluar los numerales generales de la ISO 27001 como parte del cumplimiento de sistema.

Parte del crecimiento del nivel de madurez del Sistema de Gestión de Seguridad de la Información recae sobre el grado de exigencia que la organización esté dispuesta a asumir para cada reinicio del ciclo PHVA, por lo cual se deberá replantear la calificación objetivo con respecto al resultado obtenido en este proyecto.

Es importante mantener le ejecución de los controles implementados y la validación de la eficacia de los mismos, así mismo, la reevaluación de los riesgos inherentes y residuales, generados de la gestión de los riesgos de Seguridad de la Información, con el fin de preservar la Integridad, disponibilidad y confidencialidad de la información.

BIBLIOGRAFIA

[1] López, A. (s/f). *Glosario. Iso27000*.es. Recuperado el 15 de septiembre de 2021, de https://www.iso27000.es/glosario.

[2] ISO 27001:2013; (28 de 01 de 2015). Recuperado de https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/.

[3] Moreno, j. (2016) *Implementación del Sistema de Gestión de Seguridad de la Información del Ministerio de Defensa Nacional en el Proceso de Talento Humano, Tesis de pregrado*. Institución Universitaria Politécnico Grancolombiano, Bogotá.

[4] Villamil, M. (2017) *Diagnóstico y Planificación de la Implementación del Modelo de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional de Cundinamarca – Car*. Tesis especialización. Universidad Católica de Colombia, Bogotá.

[5] Restrepo, J. (2017) *Diagnóstico del Estado Actual de la Seguridad de la Información basado en la Norma ISO 27001:2013, de la Institución Educativa Técnico Industrial Sede Mercedes Pardo De Simmonds de la Ciudad de Popayán*. Tesis Especialización, Universidad Abierta y a Distancia UNAD, Popayán.

[6] ISO 27001. 2020. *Implementar ISO 27001 Paso A Paso - 1 Como Hacer Un Análisis Previo*. [online] Available at: https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/.

[7] Icontec. (2013). Norma Técnica Colombiana NTC-ISO-IEC 27001 *Sistemas de Seguridad de la Información*, Requisitos, Bogotá D.C, Bogotá.

[8] Icontec. (2015). Guía Técnica Colombiana GTC-ISO-IEC 27002 *Código de práctica para controles de Seguridad de la Información*, Bogotá D.C, Bogotá.

[9] Incontec. (2012). Guía de implementación de un Sistema de Gestión de Seguridad de la Información, Bogot,a D.C, Bogotá.

[10] Tiempo, C., 2020. *En 2019 Se Reportaron Más De 28.000 Casos De Ciberataques En Colombia*. [online] El Tiempo. Available at: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790.

[11] RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 2017. *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000*. [online] (22), pp.73-88. Available at: https://dx.doi.org/10.17013/risti.22.73-88.

[12] 2020. [online] Available at: https://www.mintic.gov.co/gestionti/615/articles 5482_G8_*Controles_Seguridad.pdf*.

[13] Blogsgsi.blogspot.com. 2020. *Pilares De La Seguridad Informática Y De La Información*. [online] Available at: http://blogsgsi.blogspot.com/2016/07/normal-0-21-false-false-false-es-co-x_27.html

[14] Cardenas, M. (2015) *Análisis y diagnóstico al sistema de gestión de seguridad de la información de la red VOIP en el área de sistemas del nivel central de la defensoría del pueblo*. Esp. Seguridad Informática, Cundinamarca, UNAD, Bogotá.

[15] G. Villegas, G. Aguas, F. (2015) *Diagnóstico de seguridad de la información para la unidad administrativa especial para la consolidación territorial – UACT*. Esp. Seguridad de la Información, Cundinamarca, IUPG, Bogotá.

[16] Congreso de Colombia, 2020. Ley 1581 (17, octubre, 2012). *Por la cual se dictan disposiciones generales.*

[17] Portafolio, 2020. *En 2020, SIC puso multas por $7.580 millones*. [online]. Available at: https://www.portafolio.co/economia/por-incumplimiento-en-proteccion-de-datos-personales-sic-puso-multas-a-empresas-por-7580-millones-548649.

[18] López, A. (s/f). *Home. Iso27000*.es. Recuperado el 8 de septiembre de 2021, de http://www.iso27000.es

[19] ISO27002*:*Buenas prácticas para gestión de la seguridad de la información. (2016, diciembre 30). Ostec.blog. https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/.

[20] Congreso de Colombia. (1993). *Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones*, Bogotá D.C, Bogotá.