UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

Diagnóstico y evaluación de cumplimiento de la norma de los controles de ISO/IEC 27001 Sistema de gestión seguridad de la información (SGSI) desde las perspectiva del AP12 Evaluar y Administrar los Riesgos de TI (Cobit 5), así como determinar el grado de alineación y nivel de madurez del SGSI en apego a la norma

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas, para optar por el grado y título de Maestría Profesional en Auditoría de Tecnologías de la Información

Natalia Hidalgo Quirós

Ciudad Universitaria Rodrigo Facio, Costa Rica

2015

Dedicatoria

A mis hijos, mis padres y a mi compañero de vida.

Agradecimientos

A Dios, por ser mi guía siempre.

A mi familia, por su comprensión, el tiempo y el apoyo que me han dado a lo largo de este proceso.

A mis compañeros, por todo su apoyo durante estos años.

Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar por el grado y título de Maestría Profesional en Auditoría de Tecnologías de la Información.

_____

Doctor Aníbal Barquero Chacón

Director Programa de Posgrado en Administración y Dirección de Empresas

_____

Doctor Sergio Espinoza Guido

Profesor Guía

Máster Marcela Ramírez Rojas

Lectora académica

Máster Óscar Jimmy Jiménez Bastos

Lector empresarial

Natalia Hidalgo Quirós

Sustentante

Contenidos

Resumen

El objetivo principal del desarrollo de esta práctica profesional fue la evaluación del Sistema Gestión de Seguridad de la Información con base en la Norma ISO 27000, de acuerdo con la normativa vigente, los entes que la rigen y la políticas asociadas a estas instituciones, valorando el nivel de madurez, para emitir un criterio, dirigido al área de Tecnologías de Información y Gerencia, sobre el nivel de madurez alcanzado en este proceso. Por motivo de confidencialidad, se ha protegido el nombre real de la institución y se hace referencia a ella como "BBB".

El BBB es una institución pública supervisada por la Superintendencia General de Entidades Financieras (Sugef), Superintendencia de Pensiones (Supen), Superintendencia General de Valores (Sugeval), Superintendencia General de Seguros (Sugese) dedicada al segmento de negocios financieros, con acceso a información confidencial de sus clientes y de los movimientos económicos que estos realizan en su entidad, por esto, es de vital importancia el manejo de su información y prevención de riesgos, o ajustarlos al nivel apetito de riesgo de la institución.

El contenido capitular consta de cuatro capítulos, que abarcan la introducción al tema propuesto, seguido de un diagnóstico de la situación actual; posteriormente, se realiza un análisis de los hallazgos obtenidos, como producto de la evaluación y, finalmente, se detallan las conclusiones y recomendaciones a la institución.

Lista de Tabla

Lista de figuras

Glosario

Activo de información: en relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13 335-1:2004[1]], cualquier cosa que tiene valor para la organización.

Archivalía: es aquella documentación que ha finalizado su trámite administrativo y es conservada, organizada y facilitada en los archivos centrales de las instituciones y en el archivo intermedio.

CISM: Certified Information Security Manager.

Cobit: Control Objectives for Information and Related Technologies.

CMDB: por sus siglas en inglés Configuration Management Data Base o base de datos de la gestión de la configuración.

Código móvil: este tipo de código es el que puede ser ejecutado en un equipo local, sin que este necesite instalación o ejecución por parte del usuario. El código móvil es un código de software que se transfiere de un computador a otro y luego se ejecuta automáticamente y lleva a cabo una función específica con poca o ninguna interacción del usuario. El código móvil se asocia con una variedad de servicios ubicados en la capa intermedia (middleware) [ISO27002:2008].

HSM: Hardware Security Module.

IPS: Sistema de prevención de intrusos (IPS, por sus siglas en inglés Intrusión Prevention System) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Isaca: International Systems Audit and Control Association.

ISO: International Organization for Standarization / International Electrotechnical Commission.

ITIL: Information Technology Infrastructure Library.

Objetivo de tiempo de recuperación (RTO, por sus siglas en inglés, recovery time objetive): el tiempo máximo permitido para la recuperación de un servicio de TI tras una interrupción. El nivel de servicio a ser provisto debe ser inferior a los objetivos de nivel de

[1] **1 Isaca**. Cobit 5: A Business Framework for the Governance and Management of Enterprise IT. [En línea] 2014. [Citado el: 16 de octubre del 2014.] http://www.isaca.org/COBIT/Pages/default.aspx

servicio. Los objetivos de tiempo de recuperación para cada servicio de TI deberían ser negociados, acordados y documentados.

Objetivo de punto de recuperación (RPO, por sus siglas en inglés, recovery point objetive): la cantidad máxima de información que puede ser perdida cuando el servicio es restaurado tras una interrupción. El objetivo de punto de recuperación se expresa como una longitud de tiempo antes del fallo. Por ejemplo, un objetivo de punto de recuperación de un día debe ser soportado por copias de seguridad diarias, y hasta 24 horas de información pueden ser perdidas. Los objetivos de punto de recuperación para cada servicio de TI deberían ser negociados, acordados, documentados y utilizados como requisitos para el diseño del servicio y los planes de continuidad de TI.

PGSI: Plan de Gestión de la Seguridad de la Información.

Prearchivalía: consiste en la documentación que se encuentre en gestión, en las diferentes unidades o secretarías de las instituciones productoras, y se organizará de acuerdo con los principios de procedencia y orden original y otros lineamientos que dicte la Junta Administrativa del Archivo Nacional o la Dirección General del Archivo Nacional. Usualmente, comprende documentos producidos en los últimos cinco años

Registros: documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas.

Trazabilidad: Capacidad para seguir la historia, aplicación o localización de todo aquello que en consideración en un sistema de gestión.

Sugef: Superintendencia General de Entidades Financieras.

Seguridad de la información: preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no repudiación y confiabilidad.

Subneteada: Dividir una red en una serie de subredes, de tal forma que cada una de ellas funcione como una red individual.

SGSI: Sistema de Gestión de Seguridad de la Información.

TI: Tecnologías de Información.

UCR: Universidad de Costa Rica.

CAPÍTULO I

Anteproyecto

1.1 Introducción

La información de las empresas es un activo más valioso, y la custodia de dicha información para que esté fuera del alcance de terceros, es una de las tareas más importantes. El acceso y la intrusión de personas ajenas a la información confidencial de la organización pueden terminar con la posición que la empresa tenga en el mercado y con la confianza que los clientes tienen puesta en la empresa. Cualquiera de las consecuencias supone un daño irreparable.

Hoy en día, son muchas las rutas por las que la información puede verse comprometida por lo que es necesario evaluar esos riesgos, aplicar los controles necesarios y establecer planes que aseguren la custodia de la información de la institución.

La seguridad que puede lograrse por medio de intermedios tecnológicos es limitada, por lo que para garantizar la custodia de la información se puede referir con un SGSI, que permite analizar y ordenar la estructura de los sistemas de información. Gracias a este sistema, se identifica los posibles riesgos, se establece las medidas de seguridad necesarias, aplicar estas medidas y disponer de controles que permitan evaluar la eficacia de las medidas tomadas. Esto conlleva una serie de ventajas como son la mejora en la imagen y relaciones con terceros, la mejora en el control de las personas, la mejora en el registro de incidencias y debilidades y la mejora en la gestión de continuidad del negocio.

El ISO 27000 aplica una arquitectura de gestión de la seguridad que identifica y evalúa los riesgos que afectan al negocio, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control y mejora continua.

Ayuda a la entidad a gestionar, de una forma eficaz, la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implantar controles desproporcionados y de un coste más elevado del necesario, por el retraso en las medidas de seguridad en relación con la

dinámica de cambio interno de la propia organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, etc.

Aunado a lo anterior, las nuevas exigencias del mercado en el que se desenvuelve, la empresa se ha interesado en orientar sus prácticas de seguridad hacia los estándares de seguridad internacionales ISO/IEC 27001 para lograr un nivel de madurez en la seguridad de la información, en línea de lo anterior, la empresa ha creado la función de Seguridad de la Información que surge de la necesidad de mejorar la gestión de la seguridad de la información dentro de la institución.

1.2 Delimitación del tema y organización

a) Delimitación del tema

Diagnóstico y evaluación de cumplimiento de la norma de los controles de ISO/IEC 27001 sistema de gestión seguridad de la información (SGSI) junto con el DS 5 Gestionar los servicios de seguridad desde las perspectiva del AP12 Evaluar y Administrar los Riesgos de TI Y AP 13 Gestionar la Seguridad (Cobit 5), así como determinar el grado de alineación y nivel de madurez del SGSI en apego a la norma.

b) Organización

Se reserva el nombre de la Institución por estatuto de confidencialidad.

Entre algunos de los servicios que ofrece, se encuentran los siguientes:

- Préstamos de toda índole.

- Tarjetas de crédito y de débito.
- Certificados a plazo
- Planes de ahorros
- Corredora de seguros
- Corredora de valores
- Fondos de inversión
- Operadora de pensiones

Misión

Impulsar el desarrollo social, la competitividad y la sostenibilidad de Costa Rica al ofrecerles a sus clientes un conglomerado financiero público de excelencia e innovación en todos sus servicios.

Visión

Ser la opción preferida en Costa Rica por ofrecer a sus clientes estándares mundiales de calidad, innovación y eficiencia en servicios financieros.

1.3 Justificación

En la actualidad, la información es una herramienta estratégica fundamental en la actividad normal de cualquier organización. Por ello, se hace indispensable la implantación

de un adecuado Sistema de Gestión de la Seguridad de la Información en la propia organización. Sin embargo, en muchas ocasiones, la implantación no se realiza llevando a cabo un proceso efectivo, eficaz ni útil para la empresa.

El establecimiento y el mantenimiento de un SGSI no solo concierne al departamento relacionado con las TIC, sino a todos y cada uno de los empleados tiene que ser consciente de qué papel poseen dentro del sistema, ya que es probable de que deban modificar, perfeccionar o rediseñar algunas de sus funciones, procesos y actitudes para el cumplimiento de un SGSI eficaz.

1.4 Finalidad

La necesidad de salvaguardar la información es prioritario para cualquier empresa y de ahí surge el presente diagnóstico, la cual se enfoca en la elaboración un Plan de Gestión de la Seguridad de la Información que le permita a la empresa en una proyección de 3 a 5 años gestionar las actividades de seguridad alineadas a las mejores prácticas en el mercado tales como la familia ISO27000, Cobit 5e ISM3; sin embargo, previo a la elaboración de este plan es necesario realizar un diagnóstico de la situación actual y nivel de madurez de la gestión actual en torno a la seguridad de la información con el objetivo de identificar los riesgos a los que está expuesto y las debilidades que necesitan ser mejoradas.

1.5 Intereses profesionales

- Implementar los conocimientos adquiridos a lo largo de la Maestría en Auditorías de Tecnologías de Información.
- Desarrollar una metodología de trabajo, eficiente y ágil para el diagnóstico de estándares y normas que puedan aplicarse para futuras evaluaciones.

- Adquirir mayor conocimiento sobre un sistema gestión de seguridad de la información y de las buenas prácticas relacionadas.

1.6 Objetivos

1.6.1 Objetivo general

- Realizar un diagnóstico y evaluación de cumplimiento de la norma de los controles de ISO/IEC 27001 sistema de gestión seguridad de la información (SGSI) junto con el DS 5 Gestionar los servicios de seguridad desde las perspectiva del AP12 Evaluar y Administrar los Riesgos de TI Y AP 13 Gestionar la seguridad (Cobit 5), así como determinar el grado de alineación y nivel de madurez del SGSI en apego a la norma.

1.6.2 Objetivos específicos

- Se realizará una revisión previa de la documentación del SGSI generada por parte la institución para obtener el contexto.
- Diagnosticar la totalidad de los ítems establecidos en la norma ISO/IEC 27001, los riesgos para DS 5 Gestionar los servicios de seguridad desde las perspectiva del AP12 Evaluar y Administrar los Riesgos de TI Y AP 13 Gestionar la seguridad (Cobit 5), para la institución, para gestionar los riesgos asociados a los hallazgos y ponerlos de acuerdo con los niveles de tolerancia aceptados por la institución.
- Emitir las recomendaciones, políticas, plantillas con respecto al diagnóstico y cumplimiento de la norma ISO/IEC 27001 y los riesgos asociados.
- Diseñar un plan de implementación de las oportunidades de mejora que sean detectadas producto de este diagnóstico.

1.7 Alcance

De acuerdo con las categorías de la norma ISO 27001 y controles de Anexo A 27002, en cumplimiento con el DS 5 Gestionar los servicios de seguridad desde las perspectiva del AP12 Evaluar y Administrar los Riesgos de TI Y AP 13 Gestionar la seguridad (Cobit 5), se llevará a cabo un diagnóstico basado en el análisis de la documentación de la seguridad existente y entrevistas con diferentes representantes de la institución, con los cuales se analizará la implementación y gestión de controles de seguridad de la información con sus respectivos procesos, personas y tecnologías que dan apoyo al control, una vez obtenida la información se tabulará y se determinarán hallazgos y oportunidades de mejora para ajustarlos y normarlos.

1.8 El marco teórico

ISO 27000

Es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI.

También, es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Cobit 5

Objetivos de Control para Información y Tecnologías Relacionadas (Cobit, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenido por Isaca (en inglés, Information Systems Audit and Control Association) y el IT GI (en inglés: IT Governance Institute), tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y, principalmente, una guía de técnicas de gestión.

Cobit es un marco de referencia para la dirección de TI, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio. Cobit permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de Cobit.

La última versión de Cobit fue liberada en Abril de 2012, esta última versión consolida e integra los marcos de trabajo Cobit 4.1, Val IT 2.0 y Risk IT, y también se basa significativamente en el marco de trabajo de aseguramiento de TI de Isaca (ITAF) y el Modelo de Negocio para la Información de Seguridad (BMIS). Sigue en línea con los marcos de trabajo y estándares como ITIL, ISO, PMBOK, PRINCE2 y FFIEC[1].

Procesos aplicables

AP12

Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.

AP13

Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

DS5

Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

1.9 El procedimiento metodológico

La metodología que se implementará para desarrollar el diagnóstico del contexto y situación actual, así como el nivel de madurez del SGSI se basa en los siguientes procesos:

1.9.1 Diseñar plantillas

El primer paso del análisis de la situación actual es diseñar las plantillas por utilizar para la recolección y análisis de la información. Para esto, se definieron las plantillas que abarcaron los requerimientos y objetivos de control establecidos en la norma ISO/IEC 27001 y DS5.

Las plantillas desarrolladas están basadas en preguntas abiertas que están alineadas a los requerimientos del ISO/IEC 27001, y a identificar los niveles de madurez de los requerimientos y controles del ISO 27001 e ISO 27002, respectivamente.

a. ***Plantilla análisis de requisitos ISO27001-*** Situación actual y nivel de madurez de los siguientes requerimientos de la norma:

- Cláusula 4 – Contexto de la organización.
- Cláusula 5 - Liderazgo.
- Cláusula 6 - Planificación

- Cláusula 7 - Soporte.
- Cláusula 8 – Operaciones
- Cláusula 9 – Evaluación del desempeño
- Cláusula 10 – Mejora continua

b. ***Plantilla análisis objetivos de control Anexo A - ISO 27001*** - Esta plantilla recolecta la situación actual y nivel de madurez de los siguientes dominios:

- 4 Contexto de la organización
- 5 Liderazgo
- 6 Planeación
- 7 Soporte
- 8 Operaciones
- 9 Evaluación del desempeño
- 10 Mejoras
- A.5 Políticas de seguridad
- A.6 Organización de la seguridad de la información
- A.7 Seguridad en los capital humano
- A.8 Gestión de activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y del entorno
- A.12 Seguridad en las operaciones
- A.13 Seguridad en las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.15 Relaciones con proveedores
- A.16 Gestión de incidentes de seguridad de la información

- A.17 Aspectos de seguridad de la información para la gestión de continuidad del negocio
- A.18 Cumplimiento.

c. DS5 Garantizar la seguridad de los sistemas

Procedimientos por valorar del DS5:

- Gestión de la seguridad de TI
- Plan de seguridad de TI
- Gestión de la identidad
- Gestión de cuentas de usuarios
- Pruebas de seguridad, vigilancia y monitoreo
- Definición de incidente de seguridad
- Protección de la seguridad
- Gestión de llaves criptográficas
- Software malicioso, prevención, detección y corrección
- Seguridad de red
- Intercambio de información sensible

ENTREVISTAR PERSONAL

Una vez que se diseñen las plantillas de recolección de información, se procederá a identificar el personal requerido para obtener la información y programar las entrevistas con este.

Para definir el personal a participar en cada una de las sesiones, debe considerarse la relación con cada ítem evaluado.

Adicional a la ejecución de las entrevistas, se consideran las solicitudes de información adicional por medio de correo electrónico, con el objetivo de aclarar puntos relacionados

con el análisis.

1.9.2 Revisar documentación existente

Como parte del análisis, se revisará la documentación proporcionada por el personal entrevistado y los requerimientos iniciales que fueron proporcionados por el personal del área de seguridad de TI. Esta información incluirá, entre otros:

- Políticas
- Directrices
- Procedimientos
- Manuales
- Estudios preliminares

1.9.3 Consolidar y analizar datos

Una vez ejecutadas las entrevistas, se consolidará la información en las plantillas respectivas y se procederá a analizar la información recopilada.

1.9.4 Generar reporte

Con la información consolidada y analizada, se procederá a generar el presente informe con las principales conclusiones y recomendaciones.

1.10 Contenido capitulario

El ordenamiento lógico de los capítulos bajo el cual estará organizado el trabajo se detalla a continuación:

Capítulo 1

Anteproyecto

Con el propósito de diagnosticar e identificar las brechas en seguridad de información y los riesgos asociados, se identificará con base en modelo de gobernabilidad de seguridad las áreas de negocio involucradas en funciones de seguridad.

Se tomara como base los objetivos y el alcance planteado.

Capítulo 2

Diagnóstico de la situación actual

En el presente capítulo se hará la valoración de las estrategias de gestión de riesgos y gestión de seguridad con base en el apetito de riesgo de la organización y recursos disponibles que respondan los requerimientos de seguridad y controles asociados.

Capítulo 3

Ejecución de la valoración

En el presente capítulo se generará la evaluación producto de la valoración al cumplimiento de la gestión de la seguridad de la información y los principales riesgos asociados a los procedimientos de la institución.

Capítulo 4

Informe final

En el presente capítulo se generara un informe de diagnóstico sobre el nivel de madurez en los procesos, gestión de la seguridad de la información, el nivel de los riesgos asociados y principales áreas afectadas.

Anexos

Se adjuntarán los anexos del trabajo.

1.11 Operacionalización de las variables

La operacionalidad de las variables aplica para los estudios de enfoques cuantitativos, por lo para el trabajo planteado no aplica.

Niveles de madurez

Con el objetivo de realizar el diagnóstico, se utilizó un modelo genérico de madurez frente a buenas prácticas de Seguridad de la Información: modelo de madurez de la gestión de seguridad de la información (Information Security Management Maturity Model ("ISM3"), por sus siglas en inglés) Dicho modelo de madurez establece un nivel de 1 a 5 de acuerdo con los criterios generales mencionados a continuación en la Figura 1:

Figura 1: Niveles de madurez

Fuente: De elaboración propia, obtenido a partir de la aplicación de la matriz denominada "Matriz ISO 27000" con base en el Anexo 1

La descripción de cada uno de los niveles se detalla a continuación en la Tabla 1:

Tabla 1: Niveles de madurez

Nivel de madurez	Nombre	Definición
1	Inicial	Existe evidencia de que la institución ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo, no existen procesos estándar. En su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración de seguridad es desorganizado.
2	Gestionado	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad a cada funcionario. Existe un alto grado de confianza en el conocimiento de los funcionarios y, por lo tanto, los errores u omisiones son probables. Los funcionarios reaccionan ante los riesgos de seguridad en más de un área de la institución, realizando procesos similares para contrarrestarlos. El conocimiento requerido para realizar estas tareas no se ha formalizado, por lo que no existe capacitación al respecto.
3	Definido	Los procedimientos del proceso se han estandarizado y

		documentado, y se han difundido por medio de entrenamiento. Sin embargo, se deja que cada funcionario decida utilizar o no estos procedimientos, y es poco probable de que se detecten desviaciones. Los procedimientos en sí, no son complejos, pero formalizan las prácticas existentes. Los procesos de tratamiento de riesgos de seguridad se han formalizado. La institución cuenta con una cultura de seguridad de la información establecida, permitiendo a los funcionarios actuar de manera consistente ante un incidente de seguridad identificado.
4	Controlado	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada. Se cuenta con indicadores o métricas de los procesos de seguridad que permiten realizar gestión de riesgos de seguridad de la información, buscando mejorar los procesos constantemente.
5	Optimizado	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. La tecnología se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la seguridad de información se adapte de manera rápida. Se gestionan los riesgos de seguridad de la información de acuerdo con buenas prácticas, logrando un nivel de seguridad elevado y adaptándose rápidamente a los cambios y tendencias en seguridad de la información.

Fuente: Obtenido a partir de Cobit 5.1 2014, Niveles de Madurez

Con base en el análisis de las entrevistas atendidas y documentación adicional, se procedió a evaluar la madurez de cada uno de los requerimientos de la norma y los dominios de control mediante el análisis de tres atributos establecidos, cada uno de los cuales se valora en una escala de 1 a 5, la cual corresponde a los niveles de

madurez detallados anteriormente. A continuación en la Tabla 2 se presenta una breve descripción de cada uno de estos atributos:

Tabla 2: Niveles de madurez para atributos

	1 Inicial / *Ad Hoc*	2 Gestionado	3 Definido	4 Controlado	5 Optimizado
Personas	•El reconocimiento sobre los asuntos y requerimientos de seguridad son evidenciados. • La gobernabilidad sobre SI existe de forma informal. • No existen recursos dedicados para atender las actividades relacionadas con SI.	• Existen roles dedicados de seguridad con un enfoque limitado. • Los roles y responsabilidad es no son formalmente asignados. • No existe una comunicación o capacitación formal sobre temas de SI.	• Existe un equipo centralizado y gobierno de seguridad de la información. • Los roles y responsabilidades sobre SI están documentados. • Sesiones de información y educación sobre sensibilización de seguridad.	• La rendición de cuentas residen en un nivel ejecutivo. • Hay métricas claras para la gobernabilidad de los sistemas, políticas y procesos de SI. • Existen indicadores individuales asociados al desempeño.	• Los ejecutivos asocian los indicadores de seguridad al desempeño operacional y financiero de la institución. • Las políticas claves son comunicadas y firmadas anualmente.
Políticas / Procesos	• Los procesos son *ad hoc*, desorganizados y no alineados. • Existen algunas declaraciones de políticas.	•Los procesos siguen un patrón regular. • Algunas actividades están incompletas o inconsistentes.	• Las políticas y procesos están bien documentadas y comprendidas. • Las políticas y procesos son comunicadas e implementadas.	• Los procesos están bajo mejora continua. • Los procesos son monitoreados y medidos. • Existen logros significativos en calidad del proceso.	• Los procesos dirigen las mejoras de calidad. • Existe un vínculo directo entre las políticas de TI y la organización.

	1 Inicial / *Ad Hoc*	2 Gestionado	3 Definido	4 Controlado	5 Optimizado
Tecnología	• Tecnologías de seguridad seleccionadas son compradas, pero no implementadas o configuradas apropiadamente. • Reportes de SI *ad hoc* o limitados.	• Tecnologías de seguridad son implementadas y configuradas. • Reportes básicos con poco detalle.	• Se implementan tecnologías de seguridad pero con poca integración.	• Tecnologías de seguridad son entregadas y configuradas de forma efectiva. • Los reportes se ejecutan frecuentemente, las oportunidades son analizadas y comunicadas.	• TI es utilizado en forma integral para automatizar el flujo de trabajo y mejorar la calidad. • Reportes sobre SI son complejos.

Fuente: Obtenido a partir de Cobit 5.1 2014, Niveles de Madurez y relacion con atributos.

Nivel de madurez deseado

El nivel de madurez deseado se estableció considerando el nivel de madurez solicitado por la normativa Cobit, el cual especifica que los procesos deben ser definidos, es decir, que se documentan y se comunican.

Para mitigar la brecha que se identifique entre el nivel de madurez actual y el deseado, se propondrá un plan de acción a corto plazo para atender riesgos urgentes, el cual tendrá un plazo de implementación de un año, y cuyo detalle puede consultar en el Capitulo, denominado “Recomendaciones, planes de acción y propuestas de mejora para mejorar en el corto plazo el SGSI de la institución actual”.

Capítulo II

Diagnóstico de la situación actual

2.1 Situación actual en el mundo

En América Latina solo 95 organizaciones han obtenido la certificación ISO 27001:2005 de Sistemas de Seguridad de la Información, mientras que a nivel mundial existen poco más de 3 000, de las cuales 46% fueron otorgadas por la empresa BSI.

Con esto se denota la importancia que está adquiriendo la información para las empresas y que, poco a poco, van alineando sus esfuerzos para la seguridad de la información, garantizando disponibilidad, confidencialidad e integridad.

El impacto de la evolución de tecnologías de virtualización y nube en las áreas de TI ha crecido a pasos titánicos. Actualmente, el 40% de las cargas de trabajo en servidores están virtualizadas, y para el 2020 se espera que esta cifra llegue al 80%. Para este mismo año la industria habrá derrochado 241 mil millones de dólares en servicios relacionados con la nube.

Ante esto, las empresas han adoptado soluciones que lejos de ser competitivas, son complejas y monolíticas; esto dificulta su escalabilidad para hacer frente al manejo de información hacia los próximos años.

Por lo tanto, contar con un esquema de gestión de información estandarizado hará que la administración sea más sencilla y controlada.

2.2 Situación en Costa Rica

En las empresas tanto de sector público como privado del sector financiero, un 70 por ciento de los altos directivos espera un cambio significativo en su departamento de TI. Los altos directivos que involucran a los directores de sistemas en la estrategia del negocio reconocen el valor de los mismos, así como los beneficios financieros de implementar una estrategia de negocio vinculada a las tecnologías de información.

Sin embargo, las instituciones, demuestran esta preocupación que va desde las capacidades del talento humano hasta la posibilidad de las mismas empresas por mantener el ritmo de aceleración.

Una encuesta realizada por la el Instituto Tecnológico de Costa Rica mostró para finales del 2014 que el 71% de las empresas cree que su organización cuenta con el nivel adecuado de habilidades y conocimientos para llevar a cabo con éxito sus prioridades de negocios pero el 89 % considera que será un desafío que estas habilidades sigan el ritmo de la innovación de Tecnologías de la Información (TI) en los próximos 1 a 2 años.

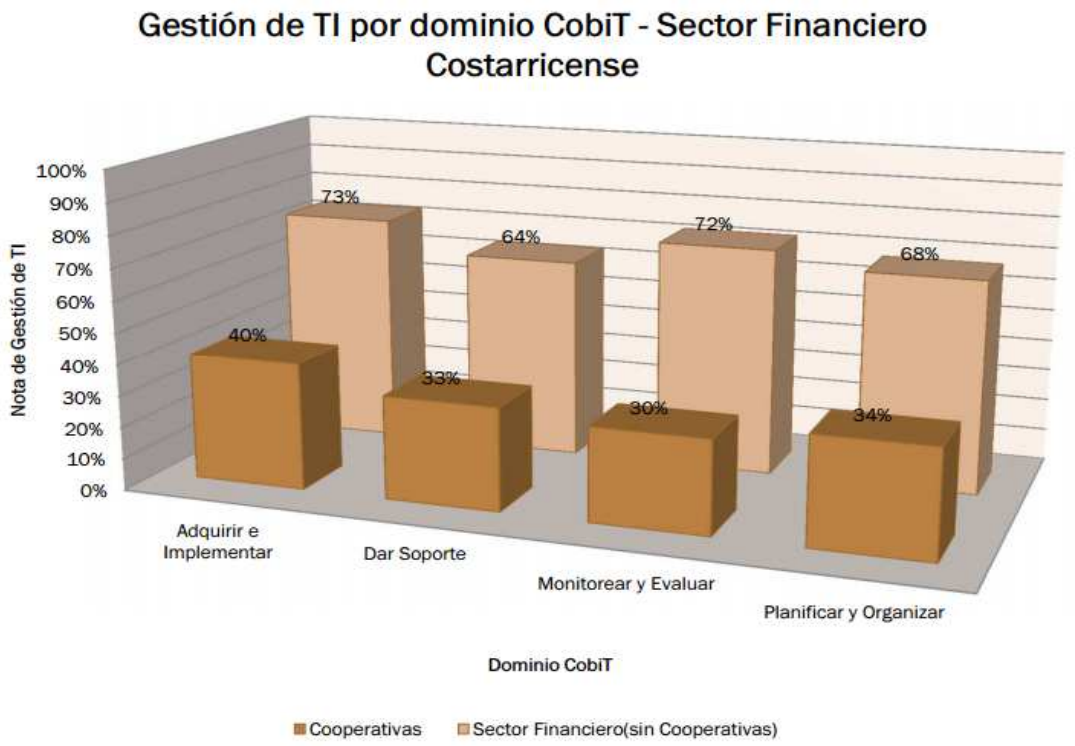
Pero el 7% de los encuestados no considera que la empresa tenga las capacidades en el área de tecnologías de la información para seguir el ritmo al mercado en los siguientes 1 a 2 años.

Para las instituciones financieras la Sugef es un ente supervisor de las operaciones de las entidades financieras costarricenses y con el fin de cumplir esas labores de supervisión, ha sido facultada para emitir normas, que contribuyan con el ejercicio de buenas prácticas bancarias.

En el año 2009, la Sugef emitió el "Reglamento sobre la Gestión de la Tecnología de Información", el acuerdo Sugef 1409 establece, que todas las entidades supervisadas deben desarrollar, implementar y mantener un marco para la gestión de tecnología de información, que se oriente al cumplimiento de las cinco áreas de enfoque del Gobierno de TI, como se citan : Alineación Estratégica, Administración del Riesgo de TI, Entrega de Valor, Gestión de Recursos y Medición del Desempeño de TI y así ajustar sus procesos de TI a los procesos descritos en Cobit.

La Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria, para el mes de julio del 2012, presentaron el estudio denominado "Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo Sugef 1409" del cual se desprenden los siguientes resultados:

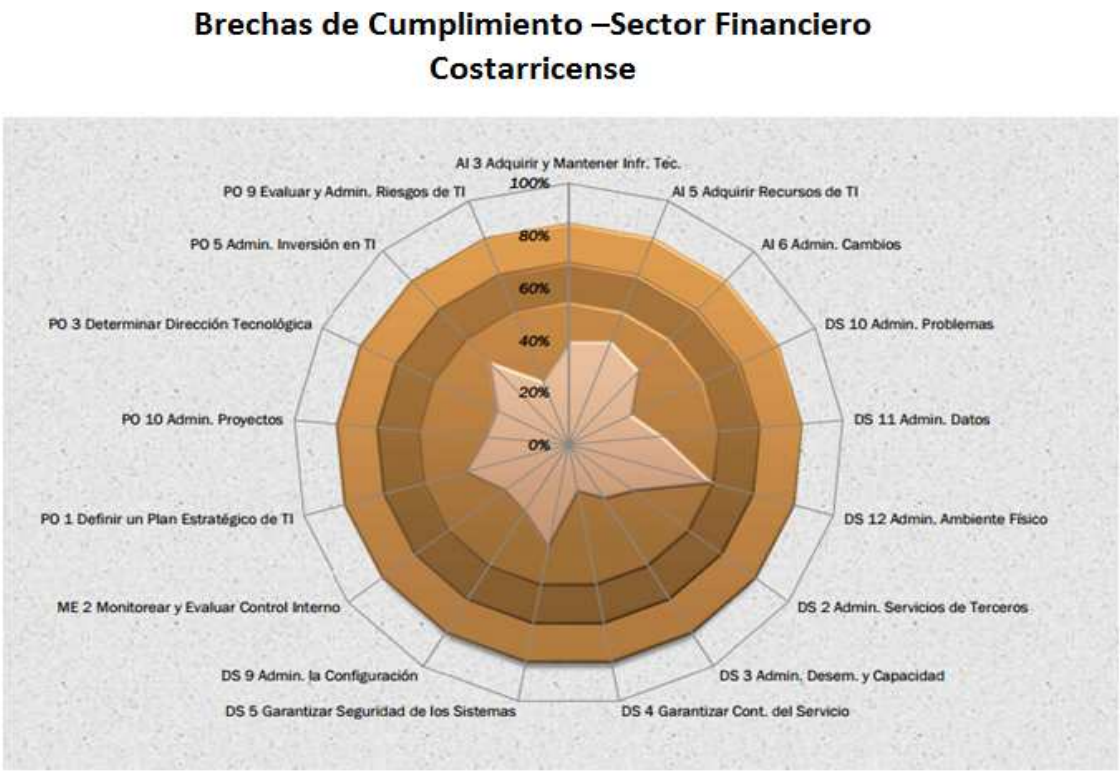
Gráfico1. Gestión de TI por dominio Cobit



Fuente: Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo Sugef 1409 y Acuerdo Sugef 14-09. Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria

Como se nota en el gráfico el sector financiero tiene una gestión de TI de nivel medio donde se evidencia que han empezado en la incorporación del acuerdo Sugef 1409, pero aún hay brechas de cumplimiento que se detallan a continuación:

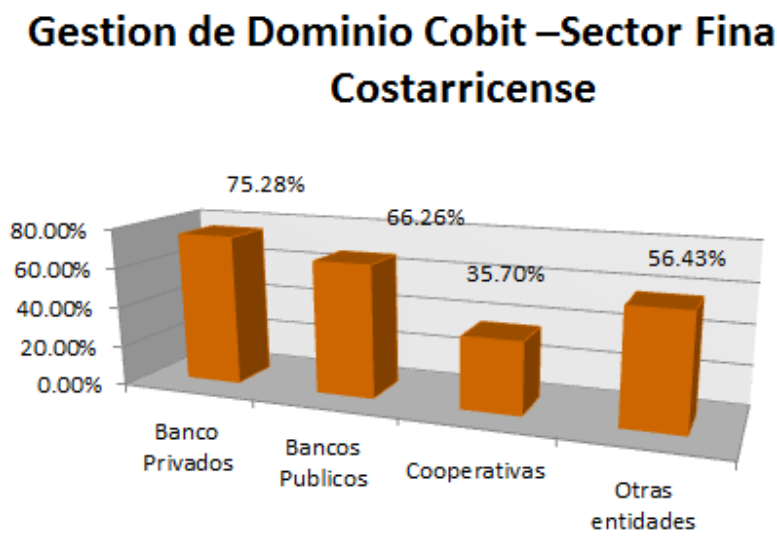
Gráfico 2, Brechas de cumplimiento



Fuente: Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo Sugef 1409 y Acuerdo Sugef 14-09. Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria

Como se nota el DS5 Garantizar la Seguridad no llega a un nivel de tres de cumplimiento como se estipula en el acuerdo, por esta razón las instituciones deben hacer un plan de trabajo para llegar a la calificación establecida.

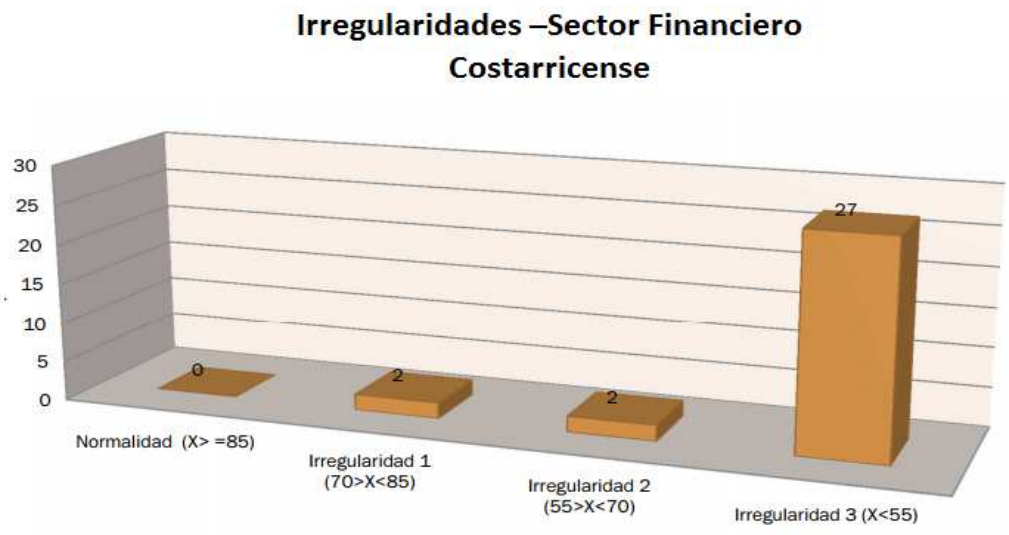
Gráfico 3, Gestión de dominio Cobit



Fuente: Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo Sugef 1409 y Acuerdo Sugef 14-09. Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria

Como se nota en el gráfico los bancos privados obtuvieron una mejor calificación que las demás instituciones, ubicándose, según nivel de irregularidad de la siguiente forma:

Gráfico 4, Irregularidades

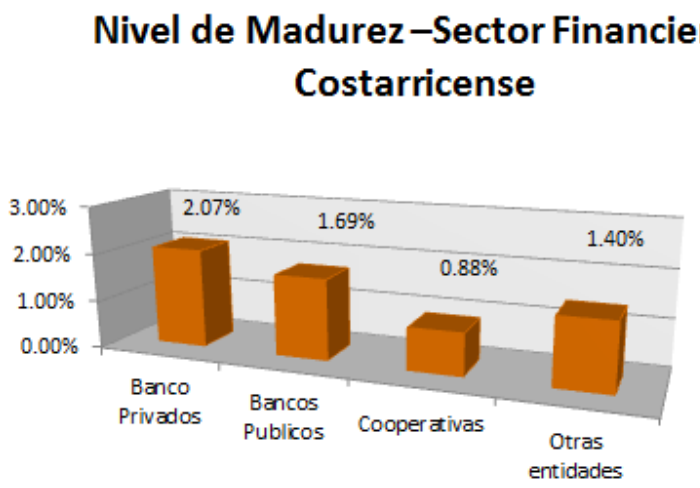


Fuente: Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo Sugef 1409 y Acuerdo Sugef 14-09. Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria.

Como se nota en el anterior gráfico los bancos públicos, cooperativas y otras entidades financieras presentan una brecha mayor de cumplimiento del Acuerdo Sugef 1409, lo que hace evidente que se tomen medidas para su conciliación.

Nótese en el siguiente grafico el nivel de madurez alcanzado por cada sector según la normativa solicitada:

Gráfico 5, Nivel de Madurez



Fuente: Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo Sugef 1409 y Acuerdo Sugef 14-09. Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria.

La banca privada obtiene una mejor calificación que va de 1- Inicial a 2- Repetible según Cobit y los demás entes solo alcanzan niveles de 0- Inexistente a 1- Inicial lo que da un panorama claro de la situación actual y real de las instituciones donde las entidades requieren un mayor esfuerzo para alcanzar un grado de evaluación de “Normal” en el corto plazo.

2.3 Diagnóstico de la situación actual en BBB

La información en todas sus formas (impresa o digital) es uno de los principales activos de cualquier organización, ya que son el medio por el cual las empresas pueden lograr la consecución de los objetivos de acuerdo con la forma en que utilizan la información. Por ello, debe garantizarse su confidencialidad, integridad y disponibilidad.

En este apartado se desarrollará un diagnóstico de la situación actual para cada uno de los requerimientos establecidos en el ISO 27001 (cláusulas de la 4 a la 10) y los controles de seguridad establecidos en el Anexo A de esta norma.

Para cada uno de los requerimientos establecidos en el ISO 27001 y controles considerados en el ISO 27002, se analiza la gestión desarrollada por la institución, lo cual permite ubicar esta gestión en una escala de madurez. Por ello, se presentará por cada una de las cláusulas y controles del ISO 27001, el análisis del nivel de madurez del SGSI, según lo indicado en el marco de referencia ISM3.

Por ello, en los apartados de este documento, podrán observarse las brechas que deben subsanarse para asegurar la confidencialidad, integridad y disponibilidad de la información.

2.3.1 Proyecto de implementación del Acuerdo SUGEF 1409

En el 2014 BBB inicio el proceso de asistencia para los procesos asumidos de Cobit por las diferentes áreas para la incorporación del marco de trabajo en todos los departamentos de TI, dicho proceso termina a finales del 2015.

2.3.2 SGSI en BBB

La realización de entrevistas y aplicación de herramienta de evaluación para obtener un conocimiento de la situación actual, se obtuvieron los siguientes resultados:

- Como parte de la implementación del acuerdo Sugef 1409 el área de Seguridad de TI, está en proceso de revisión de sus procesos.

- La oficina de Riesgo de TI está en proceso de Valoración de todas las áreas del BBB.

- Las áreas de Riesgos y de TI trabajan en la concientización de mecanismos de seguridad y pautas para los usuarios y empleados.

- Existe una política formalmente aprobada, que se comunica a todos los involucrados, y se actualiza al menos una vez por año, según normativa.

- Se generan diversos tipos de informes, por ejemplo, informes de vulnerabilidades, pentest, informes solicitados de cada área para la gerencia y se generan y da seguimiento a los planes de acción correspondientes, en caso de que aplique. Se cuenta con un plan para la ejecución de pruebas de seguridad y estas son comunicadas previamente a los involucrados y dueños. Con base en los resultados de las pruebas de seguridad, se establecen análisis de brechas (planes de mitigación). El cronograma se actualiza anualmente.

- Anualmente, cada área elabora el plan de capacitación para el siguiente año, con base en las necesidades de cada área.

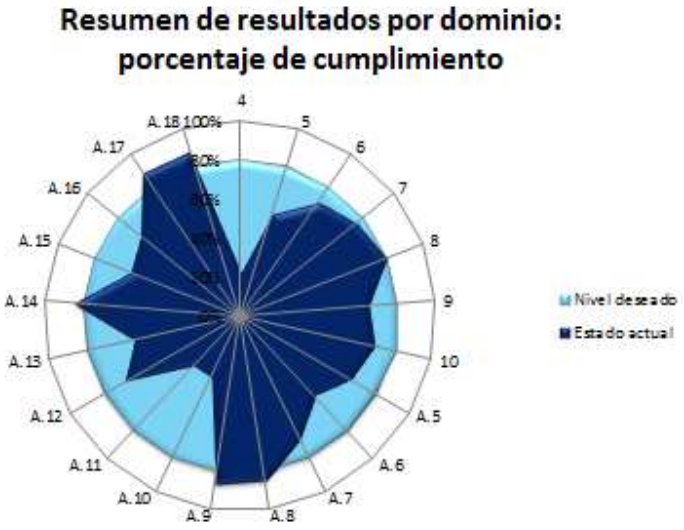
- Existe un plan anual de comunicación para la educación en materia de seguridad y riesgos para toda la institución.

- Se requiere una identificación adecuada del alcance e impacto de las acciones derivadas de la implementación del Acuerdo Sugef 14-09, así como una debida asignación de responsabilidades.

Finalmente, se observa que, en los cuatro dominios evaluados, el interés sobre la utilización de marcos de control, como la Sugef 1409 ha venido en aumento los últimos años, situación que evidencia de que la institución ha sentido la necesidad o urgencia de orientar la gestión de la tecnología de información, con este marco de trabajo Cobit y de los servicios que brindan a sus usuarios, de acuerdo con las mejores prácticas propuestas.

A continuación se muestra una serie de gráficos que resumen el nivel de madurez actual sobre las condiciones del SGSI y la cantidad de incumplimientos de acuerdo con el diagnóstico efectuado con la norma ISO/IEC 27001- 27002:2013.

Gráfico 6. Porcentaje de Cumplimiento



Fuente: De elaboración propia, obtenido a partir de la aplicación de la matriz denominada "Matriz ISO 27000" con base en el anexo 1

Gráfico 7. Nivel de Madurez

Fuente: De elaboración propia, obtenido a partir de la aplicación de la matriz denominada "Matriz ISO 27000" con base en el anexo 1

III Capítulo

Ejecución de la valoración

3 Introducción

El presente capítulo corresponde a la evaluación de los niveles de cumplimiento, madurez de los procesos, riesgos y situación evidenciada en cada una de las áreas: En esta sección se desarrollará el reporte sobre el estado de preparación del SGSI, en el cual se incluye el resumen de calificación obtenida de niveles de madurez, porcentaje de cumplimiento de los controles, análisis del contexto y las brechas existentes en el sistema.

3.1 Herramientas utilizadas

La matriz de cumplimiento está basada en preguntas abiertas que están alineadas a los requerimientos del ISO/IEC 27001 y a identificar los niveles de madurez de los requerimientos y controles del ISO 27001 e ISO 27002, respectivamente.

Matriz ISO 27001 - Esta plantilla recolecta la situación actual y nivel de madurez de los siguientes dominios:

- 4 Contexto de la organización
- 5 Liderazgo
- 6 Planeación
- 7 Soporte
- 8 Operaciones
- 9 Evaluación del desempeño
- 10 Mejoras
- A.5 Políticas de seguridad
- A.6 Organización de la seguridad de la información
- A.7 Seguridad en los capital humano
- A.8 Gestión de activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y del entorno
- A.12 Seguridad en las operaciones

- A.13 Seguridad en las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.15 Relaciones con proveedores
- A.16 Gestión de incidentes de seguridad de la Información
- A.17 Aspectos de seguridad de la información para la gestión de continuidad del negocio
- A.18 Cumplimiento.

Se utilizó como referencia la guía el The Risk IT Practitioner Guide de Isaca, The IT Assurance Guide y Information security measurement de ISO 27000.

Las plantillas en blanco utilizadas para la recolección de información pueden consultarse en el ***Anexo 2. Plantillas utilizadas.***

3.2 Resultados obtenidos por objetivo de control

A continuación la descripción de la situación actual por cláusula de la norma:

<table>
<tr><th colspan="2">Requisitos ISO 27001:2013 - Cláusula 4</th></tr>
<tr><th colspan="2">Definición según el dominio de la norma – Contexto de la organización</th></tr>
<tr><td colspan="2">Determinar los problemas externos e internos así como requisitos claros para considerar las partes interesadas. El contexto determina la política de SI, los objetivos y la forma en que la organización tendrá en cuenta el riesgo y el efecto del riesgo en su negocio y los requisitos de las partes interesadas pueden incluir los requisitos legales, reglamentarios y las obligaciones contractuales.</td></tr>
<tr><th colspan="2">Madurez</th></tr>
<tr><th colspan="2">Nivel de madurez general</th></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><th colspan="2">Situación evidenciada</th></tr>
<tr><th colspan="2">4.1 Comprender la organización y su contexto</th></tr>
<tr><td>4.1.1 Determinar los problemas internos y externos relevantes para el SGSI.</td><td>Hallazgos identificados

No se encuentra definido un documento claro, conciso y que defina explícitamente el Alcance del SGSI y que documente el análisis de la problemática interna y externa vital para entender el entorno de la organización en este caso de la institución y la situación</td></tr>
</table>

	actual. De acuerdo con la sesión obtenida con el área de Seguridad Informática no existe un documento formal que defina el alcance del SGSI, sin embargo se cuenta con un mapeo que define el alcance establecido en metas de corto, mediano y largo plazo para la gestión del SGSI. Este mapeo se encuentra en un archivo Excel, y no se encuentra, formalmente, documentado, en el sitio de seguridad.
4.2 Comprender las necesidades y expectativas de las partes interesadas	
4.2.1 Se determinan las partes interesadas	**Hallazgos identificados**
	No se encuentra definido un documento claro, conciso y que defina, explícitamente, todas las partes interesadas o involucradas en el SGSI. A pesar de que existen políticas definidas y las mismas indican el público meta, no cumple con lo estipulado en dicha cláusula. Esta cláusula determina la creación del primero de los documentos que constituyen el SGSI, los *stakeholders*.
4.2.2 Se tienen claros los requerimientos de las partes interesadas	**Hallazgos identificados**
	No se evidencia un documento claro, conciso y que defina explícitamente el Alcance del SGSI y que determine o identifique las necesidades de la organización y partes interesadas respecto a la seguridad de la información. A pesar de que existen otros documentos que justifican la implantación de políticas y controles de seguridad, los mismos no se formalizan en un documento consolidado que analice el contexto de la organización, específicamente en los requerimientos de seguridad. De acuerdo con la sesión obtenida con el área de Seguridad no existe el documento que defina el alcance del SGSI y los requerimientos explícitos de las partes interesadas. No obstante, se maneja un documento y seguimiento de políticas de seguridad que salvaguardan implícitamente el alcance de las áreas a tratar en el SGSI, sin embargo

	no es documento formalizado.
4.3 Determinar el alcance del SGSI	
4.3.1 Se determina la aplicabilidad y limitaciones del SGSI.	**Hallazgos Identificados**
	No se encuentra un documento formalmente definido que establezca la definición de la aplicabilidad y limitaciones del SGSI. A pesar de que existen políticas, normas entre otros que definen su alcance de aplicación propiamente, no hay una definición global del SGSI que se encuentre definidas No hay evidencia de la definición de la aplicabilidad y limitaciones del SGSI. A pesar de que se tiene clara que la gestión de la seguridad de la información es a nivel organizacional, en el documento del alcance se deben definir las áreas físicas, las limitaciones de la no aplicabilidad del SGSI.
4.3.2 Se considera para el alcance temas y problemáticas tanto internas como externas, los requerimientos de las partes interesadas, interacciones y dependencias entre las actividades realizadas por la organización y las actividades realizadas por otras organizaciones.	**Hallazgos identificados**
	No se encuentra un documento formalmente definido que establezca la documentación de las problemáticas internas y externas, requerimientos de los interesados en el SGSI y la relación con las actividades realizadas por la Organización y externas. A pesar de que existen políticas, normas entre otros que documentan el alcance de aplicación, no hay una definición concisa y clara sobre este punto que se encuentre definido. Existe un plan de revisión anual sobre las metas alcanzar a corto, mediano y largo plazo y que determina las actividades a realizar. Adicionalmente, se tiene un mapeo con las áreas de seguridad que van a involucrarse y gestionarse. No obstante lo anterior, no se encuentra definido en documento formal.
4.3.3 El alcance se encuentra formalmente documentado	**Hallazgos identificados**
	No se obtiene evidencia de un documento formalmente definido que establezca las políticas del SGSI. No

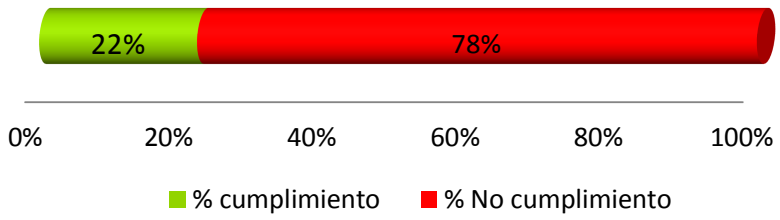
	obstante, si existen evidencia de políticas y normas de seguridad debidamente documentadas, pero las mismas no se encuentran definidas dentro de un documento de alcance del SGSI.
4.4 SGSI	
4.4.1 Se ha establecido, implementado, se da mantenimiento y se mejora continuamente el SGSI.	**Hallazgos identificados** A pesar de que no existe un documento formal que defina el alcance del SGSI, si existen políticas y normas de seguridad establecidas que rigen los controles de seguridad de la institución. Sin embargo dichas normativas aún se encuentran en proceso de actualización y la política vigente, según el control de versiones fue aprobada desde 2012. Para esta observación se toma como referencia Política Institucional de Seguridad. Además, no se determina la existencia de un proceso formal que cumpla con la aplicación de la mejora continua del SGSI con la aplicación de evaluaciones periódicas, auditorías constantes, evaluación de indicadores, entre otros. Dicha normativa se encuentra implementada y aprobada debidamente. Las funciones del área de seguridad es mantener y revisar la debida aplicación de los controles de seguridad, para garantizar la integridad, confidencialidad y disponibilidad de la información, pero la escasez del recurso humano limita que el área pueda trabajar proactivamente, por lo que no hay un adecuado monitoreo, en ocasiones, de la aplicabilidad correcta del SGSI. Como parte del proceso de evaluación, se realizó un instrumento de evaluación para determinar el nivel de cumplimiento de la normativa, sin embargo existió resistencia por parte de algunos expertos de áreas. Actualmente, no existe una métrica para la evaluación del SGSI. No hay evidencia de la definición de un

	proceso de indicadores que midan el desempeño del SGSI.

Nivel de Cumplimiento

4.1	Comprender la organización y su contexto	✖
4.1.1	Determinar los problemas internos y externos relevantes para el SGSI	✖
4.2	Comprender las necesidades y expectativas de las partes interesadas	✖
4.2.1	Se determinan las partes interesadas.	✖
4.2.2	Se tienen claros los requerimientos de las partes interesadas	✖
4.3	Determinar el alcance del SGSI	✖
4.3.1	Se determina la aplicabilidad y limitaciones del SGSI	✖
4.3.2	Alcance incluye todas las variables	✖
4.3.3	El alcance se encuentra formalmente documentado	✖
4.4	SGSI	✖
4.4.1	Se ha establecido, implementado, se da mantenimiento y se mejora continuamente el SGSI.	✖

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula 5	
Definición según el dominio de la norma – Liderazgo	
Resume los requisitos específicos para el papel de la alta dirección en el SGSI y delinea formas específicas para demostrar la gestión y su compromiso con el sistema.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
5.1 Liderazgo y compromiso	
5.1.2 Se han integrado los requerimientos del SGSI en los procesos de la organización	**Hallazgos identificados** De acuerdo con la revisión efectuada no se determina la integración de los requerimientos del SGSI a los procesos de la organización, ya que no existe un documento formal del alcance del SGSI que así los defina, por lo que los requerimientos no se encuentran alineados de acuerdo con un documento formal que así lo establezca. De acuerdo con la sesión obtenida, la implantación del SGSI claramente ha respondido con las necesidades del negocio. Sin embargo aún la alta dirección no ha abordado en algunos aspectos la atención especial sobre la gestión de la SGSI. La función

	del área de seguridad ha sido fortalecer los procesos de seguridad dentro de la organización, sin embargo por la estructura organizacional y posicionamiento jerárquico en algunos casos no ha sido factible aplicar y gestionar correctamente la seguridad y sus procesos.
5.1.3 Existen recursos suficientes para la implementación y operación del SGSI.	**Hallazgos identificados**
	De acuerdo con la información suministrada no se obtiene evidencia de documentación alguna que establezca o defina la asignación y disponibilidad de los recursos que el área de Seguridad Informática tiene para la implementación y operación del SGSI. En algunos casos si se tiene respuesta tales como en la adquisición de infraestructura o herramientas necesarias para la gestión de la seguridad de la información, en aspectos tales como recursos para la capacitación de los funcionarios del área en temas de seguridad, disponibilidad de personal especializado, recursos de apoyo para fortalecer el SGSI, entre otros, ha sido deficiente.
5.1.5 Se garantiza que el SGSI alcance sus objetivos	**Hallazgos identificados**
	De acuerdo con la revisión efectuada no hay un documento formalmente definido que establezca el alcance del SGSI, por lo que no puede determinar los objetivos del SGSI. No obstante la existencia de la política de seguridad y normas de seguridad cada una determinan el alcance hacia todas las unidades ejecutoras y funcionarios que hagan uso de las Tecnologías de Información. Sin embargo, no se determina si dicho alcance es de conocimiento a todos los involucrados, ya que no existe evidencia de

	indicadores, guías, encuestas o simulacros que pongan a prueba el cumplimiento de los objetivos de dichas políticas. De acuerdo con la sesión obtenida con el Área de Seguridad por la cantidad de recurso humano con que cuenta el área no se puede efectuar una revisión para determinar el cumplimiento de los objetivos del SGSI. No obstante, se hacen revisiones puntuales sobre algún determinado suceso de seguridad de que se haya presentado, aspecto que hace que muchas de las revisiones sean de carácter reactivo y no de una forma proactiva.
5.1.6 Se provee la dirección y el soporte necesario al personal para contribuir con el SGSI.	**Hallazgos identificados** De acuerdo con la información suministrada, las políticas y normas de seguridad llegan a ser un instrumento vital en la contribución del cumplimiento del SGSI y estas se convierten en el soporte necesario para contribuir con el cumplimiento del SGSI; sin embargo, no se denota documentación sobre la utilización de otras estrategias de comunicación fuera de las políticas que logren dar dirección y soporte al SGSI como por ejemplo el desarrollo de un programa de sensibilización o campaña de buenas prácticas en ciberseguridad. De acuerdo con la sesión obtenida con el Área de Seguridad existen pequeños espacios para brindar asesoramiento, apoyo y soporte necesario para contribuir con las buenas prácticas de seguridad. Por medio de intranet y campaña de correos con buenas prácticas proporcionan algunas herramientas que llegan a contribuir con el cumplimiento del SGSI. No obstante, no se cuenta con un plan formalmente documentado que defina lo anterior de una manera clara.

5.1.7 Se promueve la mejora continua	**Hallazgos identificados**
	De acuerdo con la revisión efectuada no se detecta la definición formal de un plan de mejora continua que determine las acciones correctivas o preventivas para la prevención de incidentes de seguridad, así como de la comunicación de las acciones y mejoras a todas las partes interesadas y el seguimiento de las mismas. De acuerdo con la sesión obtenida con el Área de Seguridad no existe un documento formal que defina y establezca el plan de mejora continua. Adicionalmente, se cuenta con charlas seguridad en los procesos de inducción y reinducción, así como la campaña efectuada por medio de las videoconferencias e intranet.
5.1.8 Se brinda soporte a otras gerencias para demostrar su liderazgo y soporte	**Hallazgos identificados**
	De acuerdo con la revisión efectuada se denota que el área de Seguridad Informática logra incentivar el cumplimiento de las políticas y normas de seguridad a toda la Institución. El tema de seguridad es un tema en el que deben colaborar toda la organización. De acuerdo con la sesión obtenida con el Área de Seguridad ejecuta el programa de sensibilización por medio de la intranet para dar soporte a todas las unidades para que velen por el cumplimiento del SGSI. No obstante, no se ha culturizado aún el tema de la seguridad de la información, puesto que para ello es necesario de que la alta dirección adopte una especial atención sobre la gestión del SGSI y lo vuelva un tema organizacional. Dentro de algunas de las consultas realizadas al personal de la organización algunos indicaron no conocer sobre las buenas prácticas de seguridad, acceso a las políticas, entre otros lo que denota que no existe un

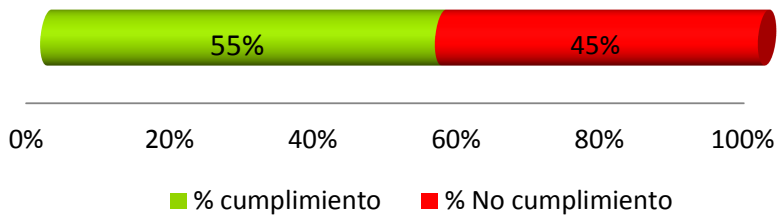
	compromiso ideal para la gestión del SGSI, esto a pesar de que el Área de Seguridad lo ha intentado.
5.2 Política	
5.2.4 La política incluye un compromiso para la mejora continua del SGSI.	**Hallazgos identificados** De acuerdo con la revisión efectuada al documento "TIC-SEG-0001-Política Institucional de Seguridad en TIC 022-21052014" si se determina en el punto 5. Divulgación y el compromiso de la actualización periódica del contenido de las políticas para alinearse a los nuevos controles de seguridad de la información. Además, existe un comité especializado para discutir los temas y decisiones relevantes en seguridad de la información para la institución; sin embargo, no se tiene evidencia de documentación generada de las sesiones de dicho comité. Esto debe ser un proceso periódico que debe efectuarse cada vez que: 1. Ocurran grandes incidentes de seguridad. 2. Posterior a una auditoría de TI sin éxito. 3. Frente a cambios que afectan a la estructura de la organización. De acuerdo con la sesión obtenida con el Área de Seguridad y revisión efectuada al documento de Política de seguridad Informática si se define un compromiso dentro del documento sobre la periódica actualización, para orientar el adecuado uso de las TI. No obstante, se evidencia de que el enunciado deja un poco abierto, y no establece en que momento especifico revisar la política, dándose un posible escenario de que la misma sea revisada cuando algún funcionario tenga disponibilidad.

5.2.5 La política se encuentra formalmente documentada	**Hallazgos identificados**
	De acuerdo con la revisión efectuada al documento Política Institucional de Seguridad si se cumple con este punto, no obstante la misma se encuentra en período de actualización, por lo que se detectan algunas oportunidades de mejora para cumplir con la norma, y ser debidamente aprobada y publicada por la alta dirección. De acuerdo con la sesión obtenida con el Área de Seguridad, actualmente, se encuentra publicada la política. La política carece algunos puntos necesarios, tales como la gestión de BYOD, entre otros, por lo que se requiere hacer algunas mejoras.
5.2.6 La política es comunicada dentro de la organización	**Hallazgos identificados**
	Observación referente a la documentación: De acuerdo con la revisión efectuada la "TIC-SEG-0001-Política Institucional de Seguridad en TIC 022-21052014" es comunicada a toda la organización, sin embargo no se obtiene evidencia del mecanismo de comunicación que se utiliza. De acuerdo con la sesión obtenida con el Área de Seguridad la política es comunicada por medio de la Intranet institucional y es de acceso para todos los interesados.
5.3 Roles organizaciones, responsabilidades y autoridades	
5.3.1 Los roles y la autoridad se encuentran definidos y son comunicados	**Hallazgos identificados**
	De acuerdo con la revisión efectuada a la documentación suministrada no se obtiene evidencia de la definición formal de roles y responsabilidades claves

	para la seguridad de la información y que los mismos se asignen y se comuniquen adecuadamente. De acuerdo con la sesión obtenida con el Área de Seguridad actualmente la gestión del Área de Seguridad Informática se encuentra basada en 2 niveles: Nivel I : Gerente de TI Nivel II : Área de Seguridad Informática Se requiere un mayor compromiso, apoyo y conciencia sobre la gestión de la seguridad de la información, aspecto que se vería reforzado con la creación de un comité.

Nivel de Cumplimiento

5.1	Liderazgo y compromiso	✖
5.1.2	Se han integrado los requerimientos del SGSI en los procesos de la organización.	✖
5.1.3	Existen recursos suficientes para la implementación y operación del SGSI	✖
5.1.5	Se garantiza que el SGSI alcance sus objetivos	✖
5.1.6	Dirección y soporte necesario al personal para contribuir con el SGSI	✖
5.1.7	Se promueve la mejora continua	✖
5.1.8	Se brinda soporte a otras gerencias para demostrar su liderazgo y soporte	✖
5.2	Política	✖
5.2.4	La política incluye un compromiso para la mejora continua del SGSI	✖
5.2.5	La política se encuentra formalmente documentada	✖
5.2.6	La política es comunicada dentro de la organización	✖
5.3	Roles, organizaciones, responsabilidades y autoridades	✖
5.3.1	Los roles y la autoridad se encuentran definidos y son comunicados	✖

Porcentaje de cumplimiento


Requisitos ISO 27001:2013 - Cláusula 6
Definición según el dominio de la norma – Planeación
Establecimiento de objetivos y principios rectores para el SGSI y planificar el SGSI con base en el contexto de la organización debe ser tenido en cuenta por medio de la consideración de los riesgos y oportunidades, los objetivos de la organización deben estar claramente definidos junto con los planes para alcanzarlos.
Madurez
Nivel de madurez general

Situación evidenciada

6.1 Acciones para atender riesgos y oportunidades	
6.1.2 Determinar los riesgos y oportunidades que deben atenderse para que el SGSI alcance sus objetivos, para prevenir o reducir efectos no deseados y para mejorar el SGSI de forma continua.	**Hallazgos identificados** De acuerdo con la revisión efectuada a la documentación suministrada no se detectó ningún tipo de documentación que identifique o determine los riesgos y oportunidades que pueden suscitarse en todo el proceso de alcance de objetivos del SGSI. No se denota una metodología que se enfoque en el objetivo de identificar los riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad de la información. No hay evidencia de un plan de mejora continua del SGSI. De acuerdo con la sesión obtenida con el Área de Seguridad actualmente se hacen evaluaciones anuales de los riesgos de seguridad. El año pasado se creó la Oficina de Riesgos de TI; sin embargo, aún no hay una evaluación formal del SGSI. Muchos de los controles de seguridad son aplicados en forma reactiva.
6.1.3 La organización establece planes de acción para atender los riesgos y oportunidades y como integrar e implementar estas acciones en el SGSI y evaluar su efectividad.	**Hallazgos identificados** De acuerdo con la información suministrada se obtiene evidencia de la aplicación de documentación sobre los planes de acción para la mitigación de riesgos y oportunidades detectadas, así como documentación sobre la medición o evaluación de la efectividad de las medidas correctivas.
6.2 Evaluaciones de riesgo de seguridad de la información	
6.2.1 La organización define y aplica un proceso de evaluación de riesgo de seguridad de la	**Hallazgos identificados** De acuerdo con la revisión efectuada se evidencia

información que establece y mantiene criterios de riesgos de seguridad de la información que incluyen los criterios de aceptación de riesgo y los criterios para realizar evaluaciones de riesgo de seguridad de la información.	documentación sobre la aplicación de un proceso de evaluación de riesgos ligado a seguridad de la información. Adicionalmente, se detecta la metodología de riesgos. Se realizan evaluaciones de riesgos de seguridad de la información, según petición del área, por plan de trabajo o solicitud de Junta Directiva.
6.2.2 El proceso de evaluación de riesgos de seguridad de la información asegura que la evaluaciones resultados consistentes, válidos y comparables.	**Hallazgos identificados** De acuerdo con la revisión efectuada a la documentación suministrada no se evidencia la existencia de ningún tipo de documentación asociada a la evaluación de riesgos de seguridad de la información. La Oficina de Riesgo de TI, aun no tiene calendarizada esta valoración en su plan anual, pero si podría incluirse en la lista de pendientes.
6.2.3 Se identifican los riesgos de seguridad asociados con la pérdida de confidencialidad, integridad y/o disponibilidad de la información, y se identifican los dueños de los riesgos.	**Hallazgos identificados** De acuerdo con la revisión efectuada no se evidencia documentación relacionada con la identificación de los riesgos de seguridad de la información asociados a la pérdida de integridad, confidencialidad y disponibilidad de la información, así como la identificación de los dueños de los riesgos. La Oficina de Riesgo de TI aún está trabajando en las prioridades interpuestas por la institución y pretende tenerse estos datos al finalizar el año.
6.2.4 Se analizan los riesgos de seguridad de la información y se determinan potenciales consecuencias, una probabilidad realista y los niveles de riesgo	**Hallazgos identificados** De acuerdo con la revisión efectuada se evidencia documentación relacionada el análisis de riesgos de seguridad de la información y la determinación de

	potenciales consecuencias en caso de materializarse el riesgo. De acuerdo con la sesión obtenida con el área de Riesgo de TI Seguridad aún no se han realizado evaluaciones de riesgos de seguridad de la información. Pero, si se tienen definidos indicadores de riesgos.
6.2.5 Se evalúan los riesgos para compararlos con los criterios previamente definidos y se priorizan para su tratamiento.	**Hallazgos identificados** De acuerdo con la revisión efectuada se evidencia documentación relacionada con la priorización de tratamiento para los riesgos de seguridad de la información de acuerdo con las evaluaciones de los riesgos de TI.
6.2.6 El proceso de evaluación de riesgos de seguridad de la información se encuentra documentado.	**Hallazgos identificados** De acuerdo con la información suministrada se obtiene evidencia de documentación formalmente definida sobre el proceso de evaluación de riesgos de TI que podría contemplarse como de seguridad de la información.
6.3 Tratamiento de riesgos de seguridad de la información	
6.3.1 La organización define y aplica un proceso de tratamiento de riesgo para seleccionar las opciones de tratamiento.	**Hallazgos identificados** De acuerdo con la información suministrada no se obtiene evidencia de documentación formal que defina el proceso de tratamiento de los riesgos de seguridad de la información. De acuerdo con la sesión obtenida con el Área de Seguridad y la Oficina de Riesgo de TI al no existir un proceso formal definido para la gestión de riesgos de seguridad de la información tampoco existe un proceso formal para el

	tratamiento de los riesgos.
6.3.2 Se determinan los controles que son necesarios para implementar las opciones de tratamiento seleccionadas. (con cualquier fuente)	**Hallazgos identificados** De acuerdo con la información que se corroboró no se obtiene evidencia de documentación formal que defina los controles necesarios para la implantación de las acciones correctivas. De acuerdo con la sesión obtenida con el Área de Seguridad y la oficina de Riesgos de TI al no existir un proceso formal definido para la gestión de riesgos de seguridad de la información tampoco existe un proceso formal para el tratamiento de los riesgos.
6.3.3 Se comparan los controles con seleccionados con el Anexo A para evitar cualquier omisión.	**Hallazgos identificados** De acuerdo con la revisión efectuada no se obtiene evidencia de documentación formal y definida tal y como un estatuto de aplicabilidad que justifique los controles por implantar.
6.3.4 Se genera el estatuto de aplicabilidad	**Hallazgos identificados** De acuerdo con la revisión efectuada no hay evidencia de un documento formal que defina el estatuto de aplicabilidad. Con base en la sesión obtenida con el Área de Seguridad no existe un documento formal que defina el estatuto de aplicabilidad del SGSI.
6.3.5 Se formula un plan de tratamiento de riesgos	**Hallazgos identificados** De acuerdo con la revisión efectuada no se determina la existencia de documentación formal que defina el plan de tratamiento de riesgos.

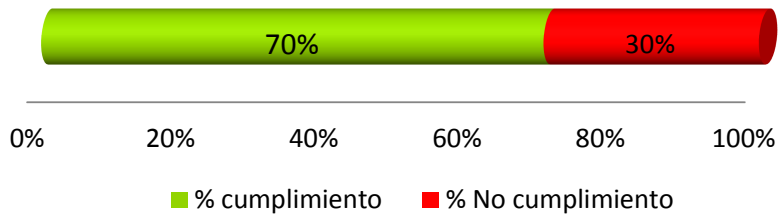
6.3.6 Se obtiene la aprobación de los dueños de los riesgos para el plan de tratamiento y aceptación del riesgo residual.	**Hallazgos identificados** Se corroboró de acuerdo con la información suministrada la existencia documentación relacionada con el plan de tratamiento de riesgos y, por lo tanto, los procesos de aprobación al tratamiento de los riesgos.
6.3.7 Se documenta el proceso de tratamiento de riesgos	**Hallazgos identificados** Se corroboró de acuerdo con la información suministrada la existencia de documentación relacionada con el plan de tratamiento de riesgos para las valoraciones.

Nivel de cumplimiento

6.1	Acciones para atender riesgos y oportunidades	✗
6.1.2	Riesgos y oportunidades que se deben atender en el SGSI	✗
6.1.3	Planes de acción	√
6.2	Evaluaciones de riesgo de seguridad de la información	√
6.2.1	Definición y aplicación de un proceso de evaluación de riesgo	√
6.2.2	Resultados consistentes, válidos y comparables	√
6.2.3	Identifica riesgos de seguridad asociados a la pérdida de CID.	✗
6.2.4	Se analizan riesgos de seguridad de la información	√
6.2.5	Se evalúan riesgos de seguridad para compararlos con los criterios definidos	√
6.2.6	El proceso de evaluación de riesgos se encuentra documentado	√
6.3.1	Definición y aplicación de un proceso de tratamiento de riesgo	✗
6.3.2	Se determinan los controles que son necesarios para implementar las opciones de tratamiento seleccionadas	✗

6.3.3	Se comparan los controles con seleccionados con el Anexo A para evitar cualquier omisión	✗
6.3.4	Se genera el estatuto de aplicabilidad	✗
6.3.5	Se formula un plan de tratamiento de riesgos	✗
6.3.6	Se obtiene la aprobación de los dueños de los riesgos para el plan de tratamiento y aceptación del riesgo residual	√
6.3.7	Se documenta el proceso de tratamiento de riesgos	√

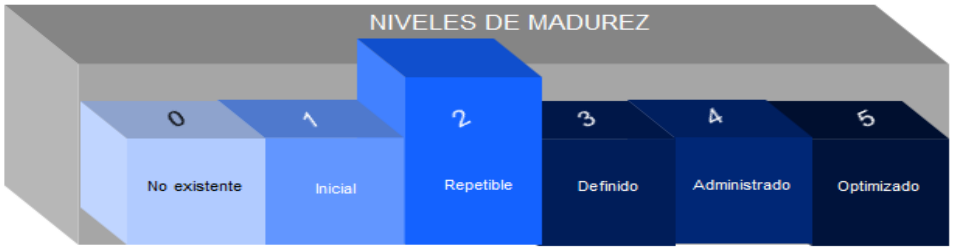
Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula 7

Definición según el dominio de la norma – Soporte

Lo necesario para establecer, implementar, mantener y mejorar continuamente un SGSI, así como los requerimientos de recursos o competencias de las personas involucradas, conocimiento, comunicación y requisitos para la gestión de documentos, donde se da más énfasis en el contenido en lugar del nombre.

Madurez
Nivel de madurez general

Situación evidenciada
7.1 Recursos

7.1.1 La organización determina y provee los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.	**Hallazgos identificados** De acuerdo con la revisión efectuada no se determinó documentación formal y definida sobre los procedimientos y recursos necesarios para el establecimiento, implementación y mejora continua del SGSI. En este punto es necesario contar con documentación formal que defina el procedimientos para el establecimiento, implementación, mejora continua y los recursos necesarios (RH, económico, tecnológico, otros) para el SGSI que son apoyados por la alta dirección. De acuerdo con la sesión efectuada, se ha incentivado en el tema del valor agregado que genera la gestión de la seguridad, la necesidad de asignar recursos suficientes para la implantación y operación del SGSI. En algunos casos, si se tiene respuesta, tales como en la adquisición de infraestructura o herramientas necesarias para la gestión de la seguridad de la información, capacitación de los funcionarios del área en temas de seguridad, disponibilidad de personal especializado,

	recursos de apoyo para fortalecer el SGSI, entre otros ha sido adecuado. Dentro del programa de capacitación para el año 2014 el personal no se ha capacitado en temas de seguridad pertinentes para el área.
7.2 Competencia	
7.2.1 La organización determina las competencias necesarias del personal; asegura que el personal es competente en aras de su educación, entrenamiento o experiencia; toma acciones para adquirir las competencias necesarias y retiene evidencia documentada como evidencia.	**Hallazgos identificados** De acuerdo con la revisión efectuada hay evidencia de la existencia de documentación formal que determine las competencias necesarias del personal involucrado en la gestión del SGSI y el perfil requerido, así como planes de capacitación internos entre otros. De acuerdo con la sesión efectuada con el Área de Seguridad y la Área de RH se obtuvo lo siguiente. El área de seguridad cuenta únicamente con 6 personas para la atención a nivel país de las funciones de la seguridad, escenario que no es el más idóneo para la organización actualmente. A pesar de que el personal del área de seguridad cuenta con vasta experiencia en la gestión de las TIC, el perfil profesional cuenta con especializaciones profesionales en el ámbito de seguridad de la información y los mismos cuentan con una amplia experiencia en el tema, por la iniciativa que los mismo han mostrado por la gestión de la seguridad de la información. Adicionalmente, para el año 2014 se han efectuado ningún tipo de capacitación para los funcionarios del área.
7.3 Sensibilización	

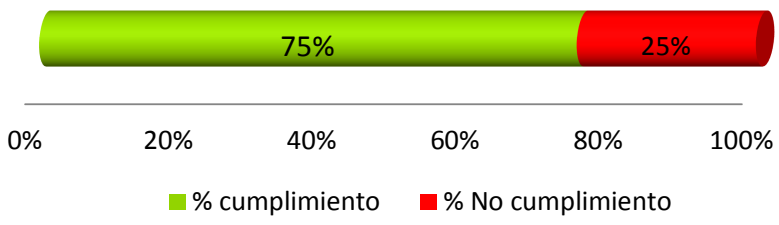
7.3.1 El personal que trabaja para la organización conoce sobre la política de seguridad de la información; sobre su aporte a la efectividad del SGSI y las consecuencias de no cumplir con los lineamientos del SGSI.	**Hallazgos identificados** De acuerdo con la revisión efectuada a la documentación suministrada no se obtiene evidencia de la definición formal de un programa de awareness o sensibilización sobre la seguridad de la información, adicionalmente no hay evidencia de un parámetro para la medición de la efectividad del programa de sensibilización. A pesar de que en los documentos Política de Seguridad se menciona un apartado sobre el tema de concientización, sin embargo no se obtiene evidencia del cumplimiento de dicho punto. De acuerdo con la sesión obtenida con el Área de Seguridad actualmente el área provee a la organización en el tema de sensibilización comunicados sobre temas relevantes sobre las buenas prácticas de seguridad de la información y además de correos que proporcionan mensajes de concientización. Si existe formalmente un documento sobre un plan de sensibilización en materia de seguridad de la información, y se indicó que el mismo se realiza como una práctica habitual.
7.4 Comunicación	
7.4.1 La organización ha determinado la necesidad de establecer comunicaciones internas y externas relacionadas al SGSI, esto incluye qué comunicar, cuando hacerlo, a quién comunicarlo, quién debe comunicarlo y el proceso por el cuál la comunicación será realizada.	**Hallazgos identificados** De acuerdo con la revisión efectuada se evidencia la existencia de documentación formal que define el mecanismo de comunicación interna, externa, su aplicabilidad y responsables de la comunicación. De acuerdo con la revisión efectuada, actualmente se tiene mapeado un manual de procedimientos que indique qué comunicar, cuando hacerlo, a quién

	comunicarlo, quién debe comunicarlo y el proceso por el cual la comunicación será realizada. Procedimiento formalizado.
7.5 Información documentada	
7.5.1 El SGSI incluye la información documentada según es requerida por el estándar ISO27001 y aquella información que la organización considere como necesaria documentar y adicionar.	**Hallazgos identificados** De acuerdo con la revisión efectuada la organización cuenta con una serie de documentación entre ellas alguna documentación formal como políticas, normas internas, guías de configuración, sin embargo se carece de otra documentación necesaria que debe estar en el SGSI y que, actualmente, no se tiene, por ejemplo, el documento para el Alcance del SGSI, procedimientos (que al menos no se evidencian en la documentación suministrada), entre otros. Se recomienda posterior al resultado de esta matriz de evaluación de cumplimiento con el estándar ISO 27001:2013 evaluar los documentos faltantes y tomar en consideración su debida aplicación. Hay carencia de procedimientos, guías, manuales que logren establecer la formalidad de los procesos. Por lo tanto, actualmente, se cuenta con documentación a nivel de políticas y normas de seguridad, adicionalmente de algunas guías o estándares realizados; sin embargo, se carece de una estructura formal de la normativa y diseño de los procesos del área de seguridad.
7.5.3 Control de información documentada	
7.5.3.2 La organización posee actividades designadas (Según sea aplicable) para la distribución, obtención, acceso y uso de la	**Hallazgos identificados** De acuerdo con la revisión efectuada en la

documentación; para el almacenamiento y preservación y de la documentación; para el control de cambios, retención y desecho de la documentación.	documentación suministrada Política Institucional de Seguridad y otros, contienen un control de versiones manual que indica los cambios realizados. Se corrobora que existen tipos de control de versión automatizado por medio del sitio que centraliza la documentación, así como el establecimiento para el desecho o eliminación de la documentación. De acuerdo con la sesión obtenida con las áreas de Procesos existe actualmente la definición de procedimientos para la normativa de documentación que define la creación, mantenimiento, aprobación, control y publicación de la normativa.
7.5.3.3 La organización contempla para estas actividades toda aquella documentación externa que es requerida para la planeación y operación del SGSI.	**Hallazgos identificados** De acuerdo con la revisión efectuada no se evidenció la existencia de documentación formal que defina las directrices para la documentación de origen externo requerida en el uso para la planeación y operación del SGSI. En este control se recomienda contar con documentación formal (procedimientos, instructivo, política) que defina y establezca los lineamientos para el manejo de documentación de origen externo. (Este punto es crucial determinar el alcance del SGSI, puesto que si es organizacional, se debe cubrir a todas las áreas que guardan relación con el manejo de documentación de origen externo, por ejemplo, en el manejo de proyectos tercerizados). No existe la definición de lineamientos para la documentación de carácter externo actualmente.
Nivel de Cumplimiento	

7.1	Acciones para atender riesgos y oportunidades	✗
7.1.1	La organización determina y provee los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.	✗
7.2.1	La organización determina las competencias necesarias del personal.	√
7.3	Sensibilización	√
7.3.1	El personal que trabaja para la organización conoce sobre la política de seguridad de la información;	√
7.4	Comunicación	√
7.4.1	La organización ha determinado la necesidad de establecer comunicaciones internas y externas relacionadas al SGSI	√
7.5	Información documentada	✗
7.5.1	El SGSI incluye la información documentada según es requerida por el estándar ISO27001.	✗
7.5.3	Control de información documentada	√
7.5.3.2	La organización posee actividades designadas (según sea aplicable) para la distribución, obtención, acceso y uso de la documentación;	√
7.5.3.3	La organización contempla para estas actividades toda aquella documentación externa que es requerida para la planeación y operación del SGSI.	✗

Porcentaje de cumplimiento



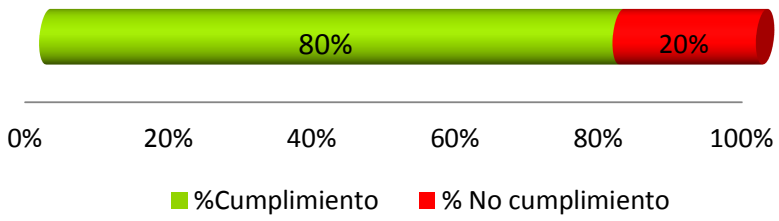
Requisitos ISO 27001:2013 - Cláusula 8	
Definición según el dominio de la norma – Operaciones	
Las organizaciones deben planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información debe llevarse a cabo valoraciones de riesgo de SI a intervalos planificados y la implementación de un Plan de Tratamiento de Riesgos de SI.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
8.1 Planificación y control operativo	
8.1.1 La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con la seguridad de información	**Hallazgos identificados** De acuerdo con la información suministrada no hay evidencia de una estructura de procesos implementado en el control del SGSI tanto durante su fase de construcción y los diferentes ciclos del PDCA en años sucesivos. No obstante, existen políticas y normas que incentivan las buenas prácticas y los

	lineamientos respectivos para la salvaguarda de la seguridad. De acuerdo con la revisión efectuada, actualmente, no se tienen definidos los procesos del Área de Seguridad. Sin embargo, se planea para el año 2015 iniciar con este proyecto de documentar y levantar los procesos del Área de Seguridad.
8.2 Las evaluaciones de riesgo de la seguridad de la información	
8.2.1 La organización realiza evaluaciones de riesgo cuando ocurran cambios significativos o en intervalos planificados.	**Hallazgos identificados** De acuerdo con la información obtenida, si existe evidencia de documentación sobre la ejecución de evaluaciones de riesgos de planificadas, o bien, cuando haya ocurrido algún cambio significativo y que haya ocasionado algún tipo de impacto negativo en la plataforma tecnológica. La oficina de Riesgo de TI está trabajando en diferentes valoraciones asignadas por su plan de trabajo.
8.2.2 La organización conserva las evaluaciones de riesgo de forma documentada.	**Hallazgos identificados** De acuerdo con la evidencia obtenida existe documentación formal sobre anteriores evaluaciones de riesgos sobre seguridad de la información realizadas,
8.3 Tratamiento de los riesgos de seguridad de la información	
8.3.1 La organización debe de poner en práctica el plan de tratamiento de riesgos y conservar la documentación respectiva	**Hallazgos identificados** De acuerdo con la información suministrada se observa la existencia de la aplicación de un plan de tratamiento de riesgos y que, además, conserva la documentación respectiva de la aplicación del tratamiento.

Nivel de Cumplimiento

8.1	Planificación y control operativo	✗
8.1.1	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con la seguridad de información	✗
8.2	Las evaluaciones de riesgo de la seguridad de la información	√
8.2.1	La organización realiza evaluaciones de riesgo cuando ocurran cambios significativos o en intervalos planificados.	√
8.2.2	La organización conserva las evaluaciones de riesgo de forma documentada.	√
8.3	Tratamiento de los riesgos de seguridad de la información	√
8.3.1	La organización debe de poner en práctica el plan de tratamiento de riesgos y conservar la documentación respectiva.	√

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula 9

Definición según el dominio de la norma – Evaluación de desempeño

Auditorías internas y revisión por la dirección de métodos claves de la revisión del rendimiento del SGSI y herramientas para su mejora continúa.
Madurez
Nivel de madurez general

Situación evidenciada
9.1 Monitoreo, medición, análisis y evaluación

9.1.1 La organización debe evaluar el rendimiento y la eficacia de la SGSI	**Hallazgos identificados** De acuerdo con la información suministrada se evidencia la existencia del procedimiento de indicadores. Esté documento establece las métrica de calidad para el Área de Seguridad. No obstante, no se evidencia relación alguna entre lo definido en los beneficios esperados del funcionamiento del SGSI ya que no existe un documento como tal que los defina (definición de objetivos del SGSI), por lo que dicho proceso debe estar totalmente alineado con los objetivos a lograr en el SGSI. En esta cláusula lo que se establece es cómo se analizará si dichos objetivos se están o no cumpliendo. De acuerdo con la sesión obtenida con el Área de Seguridad al no existir un proceso formal y definido para la gestión de riesgos, no hay una evaluación clara sobre el panorama del SGSI. La definición de los procesos del Área de

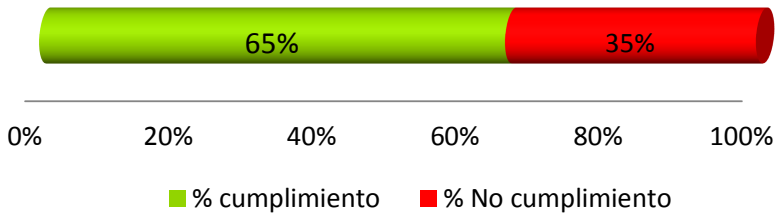
	Seguridad deben definir indicadores que puedan evaluar el cumplimiento de cada uno para con el SGSI. Actualmente, para cada año manejan el cumplimiento de metas y las cuáles son medidas por medio de los indicadores definidos en el plan de trabajo del Área.
9.3 Revisión gerencial	
9.3.1 La alta gerencia debe revisar el SGSI que debe incluir: - Estatus de las acciones tomadas en la reunión anterior - Cambios Internos y Externos - Comentarios sobre el desempeño - No conformidades y Acciones correctivas - Seguimiento y medición - Resultados de la Auditoria - Cumplimiento de los Objetivos - Retroalimentación de las partes Interesadas - Resultados de las evaluaciones de riesgo y planes de tratamiento - Oportunidades de mejora continua - Se necesitan los resultados de revisión por la dirección	**Hallazgos identificados** De acuerdo con la información suministrada no se obtiene evidencia de documentación formal en donde la alta gerencia revise periódicamente el SGSI. De acuerdo con la sesión obtenida con el Área de Seguridad y revisión del panorama de la gestión del SGSI en la organización, la alta dirección adquiere un compromiso con el SGSI en la aprobación de normativa, y en el apoyo de la creación del comité de seguridad institucional. No obstante, no hay compromiso de la alta dirección en efectuar tareas puntuales sobre: - Revisión del estado de las acciones tomadas en la reunión anterior en relación al SGSI. - Cambios Internos y Externos que afecten la seguridad de la información - Comentarios sobre el desempeño del SGSI - No conformidades y acciones correctivas detectadas en el SGSI - Seguimiento y medición del SGSI - Resultados de la Auditoria interna sobre el SGSI

	- Cumplimiento de los Objetivos del SGSI. - Realimentación de las partes Interesadas. - Resultados de las evaluaciones de riesgo y planes de tratamiento - Oportunidades de mejora continua al SGSI

Nivel de Cumplimiento

9.1	Monitoreo, medición, análisis y evaluación	X
9.1.1	La organización debe de evaluar el rendimiento y la eficacia de la SGSI	X
9.3	Revisión gerencial	X
9.3.1	La alta gerencia debe revisar el SGSI	X

Porcentaje de cumplimiento



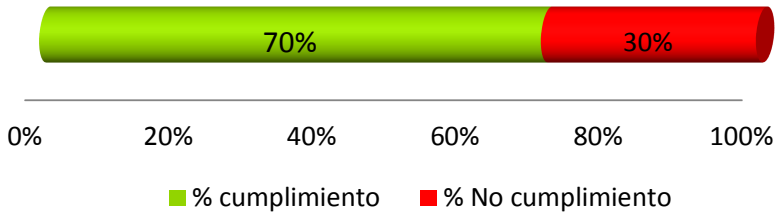
Requisitos ISO 27001:2013 - Cláusula 10	
Definición según el dominio de la norma – Mejoras	
Las no conformidades de los SGSI tienen que ser tratadas junto con las acciones correctivas para asegurarse de que no vuelvan a ocurrir.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
10.2 Mejora Continua	
10.2.1 La organización debe mejorar continuamente el SGSI	**Hallazgos identificados** De acuerdo con la información suministrada no se evidencia la existencia de un plan de mejora continua del SGSI o un proceso formal que establezca la frecuencia de la mejora continua del plan. De acuerdo con la sesión obtenida con el Área de Seguridad, actualmente se tiene un mapeo con las actividades a realizar a corto, mediano y largo plazo y que forma parte del proceso de mejora para el Área de Seguridad. Adicionalmente, con el Comité de Seguridad Informática Institucional se valoran temas que lleguen a implementar mejoras en el aspecto de la normativa del SGSI. Sin embargo, no hay definido un plan formal y documentado sobre la mejora continua del SGSI que

	describa las actividades, responsabilidades, canales de acción, tiempos, entre otros, para la mejora continua del SGSI.

Nivel de cumplimiento

10.2	Mejora continua	✗
10.2.1	La organización debe mejorar continuamente el SGSI	✗

Porcentaje de cumplimiento



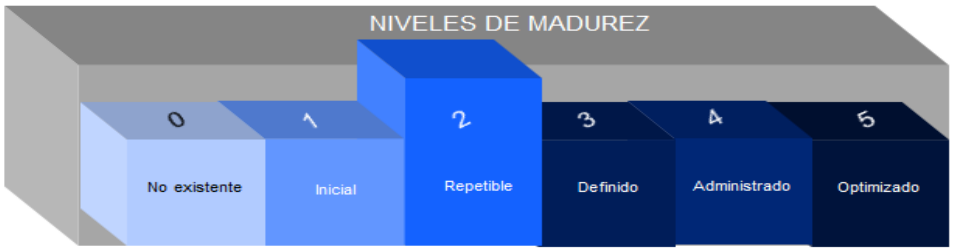
Requisitos ISO 27001:2013 - Cláusula A.5

Definición según el dominio de la norma – Política de seguridad

Se requiere que los responsables del nivel gerencial aprueben y publiquen un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según corresponda. El nivel gerencial debe poner de manifiesto su compromiso y establecer el enfoque de la organización con respecto a la gestión de la seguridad de la información. La política debe ser comunicada a todos los usuarios de la organización de manera pertinente, accesible y comprensible

Madurez

Nivel de madurez general



Situación evidenciada	
5.1 Dirección de la Alta Gerencia para la Seguridad de la Información	
5.1.1 Políticas de Seguridad de la Información	**Hallazgos cumplidos** De acuerdo con la revisión del documento Política Institucional de Seguridad se concluye lo siguiente: - Si se define claramente el compromiso de la organización en la aplicación y publicación de las políticas de seguridad, se encuentre alineada bajo distintos estándares, entre ellos el ISO 27001. Se recomienda generar a partir de la versión 2013 de la norma ISO27001. La política actual en vigencia se encuentra comunicada por medio de la intranet institucional. Si se encuentra establecido en el documento Política Institucional de Seguridad la definición de la seguridad de la información, no obstante se debe realizar la aclaración entre la diferencia de los conceptos de seguridad de la información y seguridad informática. Si se evidencia la definición de los objetivos y principios para orientar todas las actividades relacionadas con la seguridad de la información. La política se ve apoyada por el documento de procedimientos que son un conjunto de reglas que dan apoyo y amplían el contenido de cada una de las políticas de seguridad

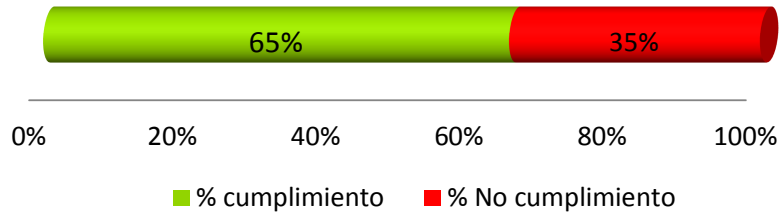
	y son de carácter más operativo. El contenido carece de políticas como el manejo del BYOD, seguridad física y ambiental, entre otros, por lo que se debe ajustar para acatar los lineamientos de la norma y actualizar en algunos otros puntos. No obstante existen acciones de mejora que se detallen en la columna de observaciones. De acuerdo con la revisión realizada actualmente se encuentra publicada la política de seguridad de la información aprobada. A la fecha aún no se ha modificado la política, sin embargo se encuentra, actualmente en dicho proceso y la misma no ha sido publicada.
5.1.2 Revisión de las políticas de seguridad de la información	**Hallazgos cumplidos**
	De acuerdo con la información suministrada el documento Política Institucional de Seguridad " se encuentra en un período de actualización para ajustarla a la realidad de la institución. En el proceso de revisión la política tiene un control de versión del documento en forma manual. Actualmente, se encuentra en vigencia la política aprobada en el 2007, y no se obtiene evidencia de alguna modificación y/o actualización a la fecha. No se observa la definición de un procedimiento formal para la actualización de las políticas de seguridad información. De acuerdo con la revisión efectuada y sesión obtenida con el Área de Seguridad actualmente se encuentra publicada la política que fue aprobada. A la fecha, la misma no ha recibido revisión alguna. Actualmente se encuentra en proceso de elaboración y actualización de la política alineada las buenas prácticas y estándares como ISO27001 - ISO27002. No hay un período

	determinado para dar revisión a la política actualmente.

Nivel de cumplimiento

5.1	Dirección de la Alta Gerencia para la Seguridad de la Información	✖
5.1.1	Políticas de Seguridad de la Información	✖
5.1.2	Revisión de las Políticas de Seguridad de la Información	✖

Porcentaje de cumplimiento



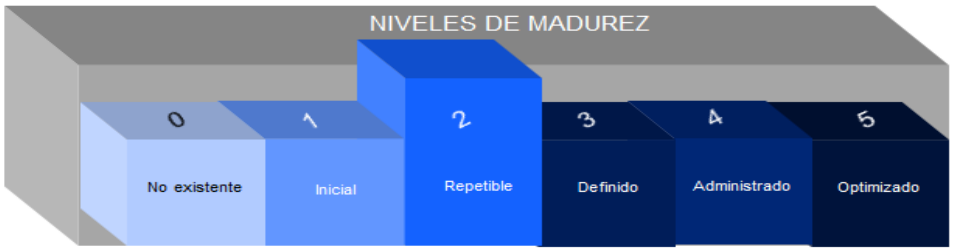
Requisitos ISO 27001:2013 - Cláusula A.6

Definición según el dominio de la norma – Organización de seguridad

Establecer un marco de gestión para iniciar y controlar la aplicación y el funcionamiento de seguridad de la información dentro de la organización.

Madurez

Nivel de madurez general



Situación evidenciada	
A6.1 Organización interna	
6.1.1 Roles y responsabilidades de Seguridad de la Información	**Hallazgos identificados** De acuerdo con la información suministrada en el documento Política de Seguridad si se obtiene evidencia de la definición de las responsabilidades en la gestión de la seguridad de la información y aplicación de los lineamientos, sin embargo no lo define de manera clara y concisa en un apartado del documento exclusivo. De acuerdo con la sesión obtenida con el Área de seguridad actualmente la gestión del área de seguridad informática se encuentra basada en 3 niveles: Nivel I : Jefatura del área de Seguridad Nivel II : Arquitectos de Seguridad Informática Nivel III : Analistas de Seguridad Informática La estructura jerárquica de la organización conllevó a crear el 3er nivel, ya que se requería un mayor compromiso, apoyo y conciencia sobre la gestión de la seguridad de la información, aspecto que se ha visto reforzado con la creación del comité.
6.1.2 Segregación de funciones	**Hallazgos identificados**

	De acuerdo con la información suministrada no se obtiene evidencia de la estructura de segregación de las funciones en la organización, para reducir las oportunidades para la modificación o mal uso de los activos de la organización no autorizado. (Se puede corroborar en algunos procesos de sistemas de información la segregación de funciones, por ejemplo). De acuerdo con la revisión efectuada y sesiones obtenidas con las diferentes áreas, el BBB mantiene una estructura definida sobre las funciones y alcances de cada uno de los departamentos. A nivel de la gestión de accesos del personal con los sistemas de información se carece de un mecanismo inadecuado de comunicación para la deshabilitación o habilitación de estos, ya que, actualmente, puede darse el caso de que algún funcionario cambia de rol o función dentro de la misma organización y si la Jefatura no lo comunica, se dejaría a dicho usuario con los accesos y privilegios iniciales, aspecto que podría estar afectando e incumpliendo con una adecuado segregación de funciones en el aspecto lógico de la administración de sistemas institucionales.
6.1.3 Contacto con las autoridades	**Hallazgos identificados**
	De acuerdo con la revisión efectuada no se determinó evidencia de documentación formal que establezca los procedimientos para el manejo de los contactos con las autoridades indicadas para obtener apoyo en el caso de los incidentes de seguridad de la información (OIJ, bomberos, policía, autoridades gubernamentales, otros). De acuerdo con la sesión obtenida con el área de Seguridad actualmente existe un contacto con el Mocitt

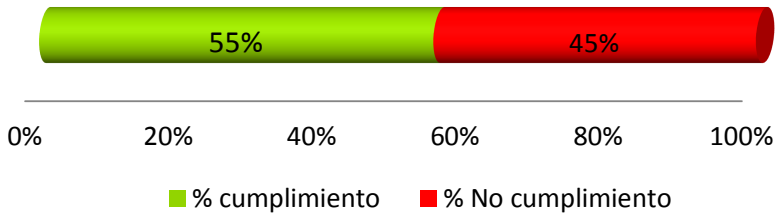
	y el OIJ, sin embargo el contacto es informal y no se encuentra formalizado un convenio como tal que así lo establezca.
6.1.4 Contacto con grupos de interés especial	**Hallazgos identificados**
	De acuerdo con la información suministrada no se observa documentación formal que defina el contacto con entes apropiados en la gestión de la seguridad de la información que mantengan a la organización en constante comunicación con los grupos de interés especial u otros foros especializados en seguridad y con entes o asociaciones profesionales en seguridad de la información, por ejemplo (Inteco, España, OWASP, otros). De acuerdo con la sesión obtenida con el Área de Seguridad, actualmente, se maneja un convenio con el CSIRT del ICE en donde existe un convenio formal, pero que se encuentra orientado hacia temas más de servicio y no tanto de la gestión de la Seguridad. Adicionalmente, se cuenta con convenio informal con Intel.
6.1.5 Seguridad de la información en la gestión de proyectos	**Hallazgos identificados**
	De acuerdo con la evidencia suministrada la organización cuenta con una metodología para administración de proyectos, sin embargo debido a falta de evidencia/documentación no se observa si la gestión de la seguridad de la información es aplicable al desarrollo de cualquier tipo de proyecto determinando aspectos, tales como: a) los objetivos de seguridad de la información se incluyen en los objetivos del proyecto.

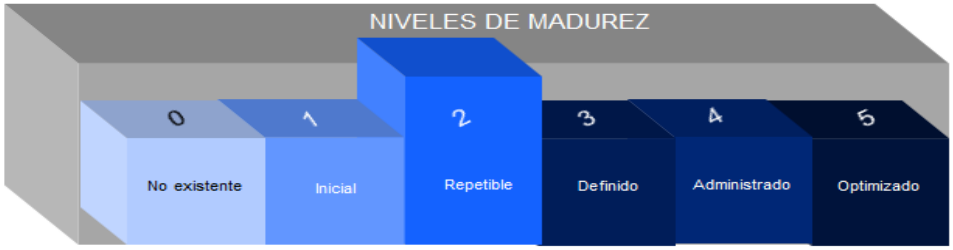
	b) incluir una evaluación de riesgos de seguridad de información identificados en el proyecto. c) seguridad de la información es parte de todas las fases de la metodología del proyecto aplicado. d) implicaciones de seguridad de información deben ser dirigidas y revisados con regularidad en todos los proyectos. e) las responsabilidades de seguridad de la información deben ser definidos y asignados a los roles específicos definidos en la metodología de gestión de proyectos. De acuerdo con la sesión obtenida con el Área de Proyectos existe una metodología propia organizacional para la gestión de proyectos en el área de TI que se basa en el PMI básicamente. Dicha metodología es genérica y dentro de su contenido no hay nada definido que inste a involucrar el tema de seguridad de la información en la gestión de proyectos, no obstante las prácticas y necesidades en muchos de los proyectos hace requerir que se involucre al personal de seguridad; no obstante, esto depende siempre del tipo de proyecto. Por ejemplo, en los casos de un proyecto de desarrollo de software si se contempla, tomando en cuenta los riesgos que desde el punto de vista de seguridad de la información la organización está expuesta. El tema de seguridad de la información no se involucra en todas las fases de la metodología, se menciona que únicamente en la fase de ejecución y control, no así en la fase de inicio. La metodología de gestión de proyectos no involucra

	dentro de su contenido revisar y monitorear la gestión de la seguridad de la información, pero en proyectos, tales como desarrollo de software si se ejecuta. No se definen los roles y responsabilidades en el manejo de la seguridad de la información en la gestión de proyectos; sin embargo, si se hace en los proyectos de desarrollo de software.
6.2 Dispositivos móviles y teletrabajo	
6.2.1 Política de dispositivos móviles	**Hallazgos identificados**
	De acuerdo con la información suministrada no hay evidencia dentro del documento "TIC-SEG-0001-Política Institucional de Seguridad en TIC 022-21052014" los lineamientos o pautas sobre el manejo de Dispositivos Móviles, adicionalmente, no hay evidencia de existencia de documentación formal que defina los procedimientos para la gestión de los dispositivos móviles. De acuerdo con la sesión obtenida con el Área de Seguridad la gestión de BYOD forma parte del mapa de ruta a cumplirse para el período 2018, para lo que se tiene planeado contratar una consultoría externa que gestione el tema. Actualmente, se cuenta con Intel un convenio, por contar con estrategias para la gestión de BYOD. Existe evidencia de un procedimiento formal para el teletrabajo con una serie de lineamientos establecidos por lo cual la prueba es satisfactoria.
Nivel de cumplimiento	

6.1	Organización interna	
6.1.1	Roles y responsabilidades de Seguridad de la Información	√
6.1.2	Segregación de funciones	√
6.1.3	Contacto con las autoridades	✗
6.1.4	Contacto con grupos de interés especial	✗
6.1.5	Seguridad de la información en la gestión de proyectos	✗
6.2	Dispositivos móviles y teletrabajo	✗
6.2.1	Política de dispositivos móviles	✗

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula A.7	
Definición según el dominio de la norma – Gestión de los Capital Humano	
Las responsabilidades en materia de seguridad deben estar incluidas en los manuales de funciones y reflejarse en los procesos de selección y manejo de acciones del personal, y su cumplimiento monitoreado como parte del desempeño del individuo como empleado. Los candidatos por ocupar los puestos de trabajo deben ser adecuadamente seleccionados, especialmente si se trata de tareas críticas. Todos los funcionarios y usuarios externos a las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad (no-revelación).	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
A 7.1 Previo al empleo	
7.1.1 Verificación de antecedentes	**Hallazgos identificados**
	De acuerdo con la evidencia realizada a los documentos Política de Seguridad se documentan lineamientos sobre la verificación de antecedentes. De acuerdo con la revisión efectuada de los documentos del Área de Capital Humano el procedimiento actual para el ingreso de personal a la institución es realizar las debidas pruebas psicológicas, médicas y de capital humano. Estas pruebas toman criterios cualitativos de las personas. Todo este estudio se almacena en un

	expediente de acceso exclusivo de capital humano.
7.1.2 Términos y condiciones del empleo	**Hallazgos identificados**
	De acuerdo con la revisión si se obtiene evidencia sobre documentación formal que defina claramente los términos y condiciones del empleo de acuerdo con los requisitos de seguridad y que los mismos sean de conocimiento del empleador en su totalidad al ingresar a la institución. De acuerdo con políticas de contratación durante el proceso de inducción se brinda todos los detalles sobre los deberes y responsabilidades del empleado con la organización. Dicha inducción cubre un programa que contempla proporcionar detalles sobre la estructura organizacional, el apegó a la ética institucional, temas de motivación, relaciones del trabajo, seguridad de la información, entre otros.
A 7.2 Durante el empleo	
7.2.1 Responsabilidades de gestión	**Hallazgos identificados**
	De acuerdo con la información suministrada se obtiene evidencia de documentación en donde la gestión del SGSI y la alta dirección, proporcione las pautas de seguridad, motive y establezca canales de denuncia sobre la gestión de la seguridad de la información a los empleados de la organización antes de iniciar sus labores y acceder a los recursos de la organización. Se obtiene evidencia de documentación que defina como debe instruirse al nuevo empleado sobre las políticas y normas de seguridad, sobre aspectos de concienciación en seguridad de la información, pero no de como procederá a denunciar eventos o incidentes de seguridad que sean detectados. La alta dirección debe

	liderar todo el proceso, ya que es la que conoce los riesgos del negocio y las obligaciones con los asegurados, mejor que nadie. Además, es la única que puede introducir los cambios de mentalidad, de procedimientos y de tareas que requiere el sistema. De acuerdo con Área de Capital Humano, por medio del proceso de inducción se brinda el conocimiento necesario a los nuevos empleados sobre las políticas y lineamientos en materia de seguridad, adicionalmente el Área de Seguridad Pública en la Intranet, la política de acceso para todos los interesados, adicionalmente en los correos y videoconferencias que se realizan. No obstante, durante el empleo se consultó la existencia de un plan de concienciación/sensibilización en materia de seguridad de la información. Actualmente, el Área de Seguridad realiza varios esfuerzos en la ejecución de capacitaciones, estas con cierta frecuencia y en donde se hace la invitación a todo el personal; sin embargo, el público meta siempre ha sido personal de índole técnica. Adicionalmente con cierta frecuencia por medio de la intranet se realizan comunicados sobre las buenas prácticas en la gestión de la seguridad de la información.
7.2.2 Conciencia, educación y entrenamiento de Seguridad de la Información	**Hallazgos identificados**
	De acuerdo con la información suministrada se obtiene evidencia de la implementación de un programa de concienciación que capacita al personal sobre los riesgos de seguridad de la información y promueve las buenas prácticas en el uso seguro y responsables de las TIC. Se menciona la aplicación de un programa de concienciación y en el contenido de dichos documentos no es claro y definido el procedimiento para la

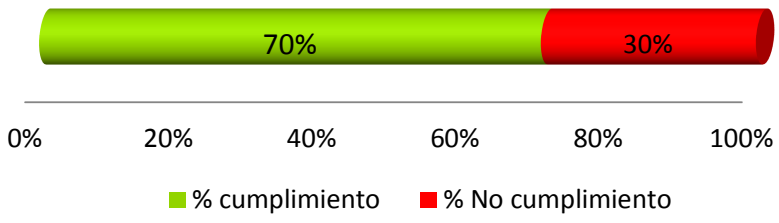
	ejecución. Se obtuvo evidencia de documentación sobre la aplicación de charlas, talleres o aplicación de estrategias para proporcionar sensibilización en este tema.
7.2.3 Proceso disciplinario	**Hallazgos identificados**
	De acuerdo con la revisión efectuada no se encuentra evidencia de documentación que establezca el procedimiento del proceso disciplinario contra los empleados que hayan violado las políticas de seguridad de la información. Este proceso debe ser notificado y de previo conocimiento para todo el personal de la organización. De acuerdo con la sesión obtenida con el Área de Seguridad, actualmente no hay proceso formal que defina la aplicación de este control específicamente para casos en los que se hayan violado los lineamientos en el manejo de la seguridad de la información. Los procesos disciplinarios no tienen un manejo adecuado.
A 7.3 Terminación y Cambio de Empleo	
7.3.1 Término de responsabilidades o cambio de empleo	**Hallazgos identificados**
	De acuerdo con la revisión efectuada en la documentación suministrada no se obtiene evidencia de la definición de un proceso formal que defina el procedimiento por seguir para los términos de responsabilidades o en casos en que se realice un cambio de empleo. De acuerdo con la información en intranet en caso de que exista salida de personal o cambio dentro de la misma organización cada jefatura le corresponde realizar el debido proceso de comunicación en este caso por ejemplo para la des

	habilitación de accesos a los sistemas institucionales, áreas físicas, otros. No existe documentación formal que defina el procedimiento para la terminación de empleo o cambio de trabajo.

Nivel de cumplimiento

7.1	Previo al empleo	√
7.1.1	Verificación de antecedentes	√
7.1.2	Términos y condiciones del empleo	√
7.2	Durante el empleo	√
7.2.1	Responsabilidades de gestión	√
7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	√
7.2.3	Proceso disciplinario	X
7.3	Terminación y cambio de empleo	X
7.3.1	Término de responsabilidades o cambio de empleo	X

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula A.8	
Definición según el dominio de la norma – Gestión de activos	
Para cumplir con este dominio de la norma ISO/IEC 27001, la organización debe considerar entre otros: Se deben identificar los activos de información de los procesos de la BBB, clasificarlos y designar propietarios para todos los activos de información. Se debe asignar la responsabilidad por analizar los riesgos de los activos de información y por el mantenimiento de los controles apropiados. La rendición de cuentas por los activos ayuda a garantizar que se mantenga una adecuada protección. En último término, el propietario designado del activo debe rendir cuentas por el control y adecuado nivel de riesgo de los activos de información de los procesos a su cargo.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
A 8.1 Responsabilidad de los activos	
8.1.1 Inventario de activos	**Hallazgos identificados**
	De acuerdo con la evidencia suministrada en los documentos de políticas y normas de seguridad se menciona en el lineamiento para la responsabilidad por la gestión de los activos de información y se detecta la

	existencia de documentación que establece un inventario explícito de los activos organizacionales clasificados (procesos de negocio o servicios, datos e información, aplicaciones de software, equipos informáticos, personal interno y externo, redes de comunicaciones, soporte de información, equipos auxiliares que soportan los sistemas, instalaciones) y al que se le de mantenimiento una vez al año. De acuerdo con la revisión efectuada y sesión obtenida con el área de Seguridad y entre otras consultas se lleva un control de licencias, activos físicos y lógicos. Estos activos están asignados por unidad ejecutora.
8.1.2 Propiedad de activos	**Hallazgos identificados**
	De acuerdo con la evidencia suministrada si se detecta un inventario de los activos y que el mismo contiene la asignación del responsable o propietario del activo. Esta información es revisada una vez al año con solicitud formal a los jefes de oficinas para su cotejo.
8.1.4 Devolución de activos	**Hallazgos identificados**
	De acuerdo con la información suministrada se obtiene evidencia de un proceso formalmente definido y documentado para la devolución de activos del personal que sale de la organización. Actualmente, este proceso se encuentra definido, y no se encuentra normado en la política institucional
A8.2 Clasificación de la información	
8.2.1 Clasificación de la información	**Hallazgos identificados**
	De acuerdo con la información suministrada, se observa

	el procedimiento de Procedimiento de Clasificación y Etiquetado de la Información. Como oportunidad de mejorar al procedimiento actual debe darse un mayor alcance al procedimiento descrito adicionando por ejemplo activos de información como las grabaciones, fotografías que son información y deben estar en forma explícita definidas en el documento. Adicionalmente entre otros detalles si se especifica el nivel de clasificación de la información, no obstante no se detalla el procedimiento sobre cómo procede a clasificarse la información de acuerdo con los requisitos legales, valor de la información, criticidad, sensibilidad, integridad, disponibilidad y confidencialidad. Aunque existe una frecuencia de revisión para determinar cambios en la clasificación de la información de acuerdo con el ciclo de vida de esta, no toda se revisa. Se carece del procedimiento para acceder a la información de acuerdo con su nivel de clasificación.
8.2.2 Etiquetado de la información	**Hallazgos identificados**
	De acuerdo con la información suministrada, se observa el procedimiento Procedimiento de clasificación y etiquetado de la información, sin embargo es necesario que se cumpla con lo siguiente: El etiquetado debe de reflejar el sistema de clasificación establecido ya sea en formato físico o electrónico. El etiquetado debe de reflejar el sistema de clasificación establecido en la clasificación de información (8.2.1). Las etiquetas deben ser fácilmente reconocibles en los documentos. La asignación de responsables de la información de

	estar documentada. Para el manejo y acceso con terceros debe ser reconocible la etiqueta del nivel de clasificación para evidenciar la garantía de confidencialidad y manipulación de la información, por lo que el procedimiento debe aclarar este punto. El procedimiento debe orientarse y definirse de cómo se accede a la información, según su clasificación. La salida de información de los sistemas debe ser clasificada como sensible o crítica, o bien, llevar una etiqueta de clasificación apropiada. De acuerdo con la sesión obtenida con el Área de Seguridad, actualmente, la organización cuenta con un proceso formal para la clasificación de la información, sin embargo no se evidencia así en la práctica.
8.2.3 Manejo de activos	**Hallazgos identificados**
	De acuerdo con la revisión efectuada si hay evidencia de documentación formal que defina el procedimiento para el manejo de los activos, para orientarlos a que deben ser desarrollados e implementados de acuerdo con el esquema de clasificación de la información aprobado por la organización.
A 8.3 Manejo de medios	
8.3.1 Gestión de medios removibles	**Hallazgos identificados**
	De acuerdo con la información suministrada en las políticas si se evidencia las pautas o lineamientos institucionales para la gestión de medios removibles. Sin embargo, se determinan algunas oportunidades de

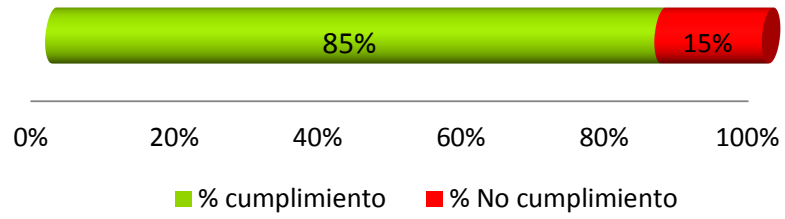
	mejora para adicionar tal y como, por ejemplo, la aplicación de controles de cifrado para los medios extraíbles que manejan información organizacional, en donde su clasificación es restringida o privada, además de limitar el manejo de información de acuerdo con el esquema de clasificación en dispositivos extraíbles, aspecto que no se evidencian en los lineamientos. Adicionalmente, no se evidencian lineamientos sobre el manejo de información corporativa en medios extraíbles y móviles de carácter personal. De acuerdo con la sesión obtenida con el encargado de servidores y AD, actualmente, la institución no tiene normado la deshabilitación de los puertos USB, esto más que todo por un tema de adaptación de los usuarios. No existe un procedimiento que establezca el control para la destrucción y desecho de información de medios removibles. Además, no se cuentan con lineamientos para la transferencia de información a través de medios removible como los USBs, dispositivos móviles, CDs, discos duros externos, entre otros. Adicionalmente, no se evidencian lineamientos sobre el manejo de información corporativa en medios extraíbles y móviles de carácter personal.
8.3.2 Eliminación de medios	**Hallazgos identificados**
	De acuerdo con la información suministrada existe una política para el procedimiento para la destrucción y desecho de la información. Sin embargo, hace más énfasis a discos duros y no a otros dispositivos.
8.3.3 Transporte de medios físicos	**Hallazgos identificados**
	De acuerdo con la revisión efectuada no se obtiene

	evidencia de documentación formal que defina los lineamientos o pautas para el proceso de transferencia de información en medios físicos por ejemplo CDs, medios USB, discos duros, dispositivos móviles, laptops, entre otros para que sea de acceso único a los entes autorizados. De acuerdo con la sesión obtenida con el Área de Seguridad no existen lineamientos para el traslado de información institucional en medios extraíbles institucionales y personales.

Nivel de cumplimiento

8.1	Responsabilidad de activos	√
8.1.1	Inventario de activos	√
8.1.2	Propiedad de activos	√
8.1.4	Devolución de activos	√
8.2	Clasificación de la información	√
8.2.1	Clasificación de la información	√
8.2.2	Etiquetado de la información	√
8.2.3	Manejo de activos	√
8.3	Manejo de medios	✗
8.3.1	Gestión de medios removibles	✗
8.3.2	Eliminación de medios	√
8.3.3	Transporte de medios físicos	✗

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula A.9

Definición según el dominio de la norma – Control de acceso

Para cumplir con este dominio de la norma ISO/IEC 27001, la organización debe considerar, entre otros:

Las instalaciones y equipos de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con controles de seguridad y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones, así como los controles ambientales necesarios. La protección provista debe ser proporcional a los riesgos identificados.

Madurez

Nivel de madurez general

Situación evidenciada	
A9.1 Requerimientos de Negocio para el control de acceso	
9.1.1 Política de control de acceso	**Hallazgos identificados**
	De acuerdo con la revisión efectuada a Política de Seguridad Informática sí existe un apartado de políticas que definen el control de acceso. No obstante, no se determinó lo siguiente: - No se evidencian lineamientos sobre la revocación de los accesos en caso, por ejemplo, de cese de funciones, pensionados, vacaciones inmediatamente deben eliminarse o deshabilitarse todos los accesos, según corresponda. -No se evidencia la existencia de un canal de comunicación entre los responsables de la gestión de accesos y el área de CH, para determinar las salidas de la institución. De acuerdo con la revisión de políticas se determinó lo siguiente: - Actualmente existe un procedimiento definido formalmente para la solicitud de accesos. Esto se da por medio de una solicitud a la mesa de ayuda. - De acuerdo por lo indicado por el Área de CH, la revocación de accesos de personal retirado, vacaciones, incapacitado, otros se da por medio de la indicación de cada jefatura con la unidad de soporte. CH no se involucra en este proceso. - No se aplica un proceso de mantenimiento de las

	cuentas de funciones en los sistemas institucionales. - Se realizan cambios en roles solo por petición no por control.
A9.2 Gestión de accesos de usuario	
9.2.1 Registro y baja del usuario	**Hallazgos identificados**
	De acuerdo con la información suministrada se evidencia la aplicación de éste punto en la norma de seguridad informática Sin embargo, puede adicionarse oportunidades de mejora para cumplir con los controles que establece la norma para este punto. -Debe estar alineada con la política para el etiquetado y clasificación de la información. - No se evidencian lineamientos sobre la revocación de los accesos en caso por ejemplo de cese de funciones, pensionados, vacaciones inmediatamente se deben eliminar o deshabilitar todos los accesos según corresponda. -No se evidencia un procedimiento formal que defina dar mantenimiento o revisión a la gestión de los accesos periódicamente. -No se evidencia la existencia de un canal de comunicación entre los responsables de la gestión de accesos y el Área de CH, para determinar las salidas de la institución. De acuerdo con la sesión obtenida con el área de Seguridad y Área de CH no hay un proceso formal para la comunicación en la deshabilitación de accesos de los usuarios. No obstante, para la asignación de accesos se

	sigue el procedimiento por medio de la mesa de ayuda. No existe una desactivación inmediata de los identificadores o usuarios que dejan la compañía, y no se cuenta con una formalidad en las revisiones periódicas de los usuarios.
9.2.2 Gestión de privilegios	**Hallazgos identificados**
	De acuerdo con la información suministrada se evidencia la aplicación de este punto en la norma de seguridad informática Sin embargo, puede adicionarse oportunidades de mejora para cumplir con los controles que establece la norma para este punto, tales como por ejemplo: - Controles de acceso adecuados a nivel de seguridad física no se especifican. - Mantenimiento del registro central de los derechos de acceso de todos los sistemas no se evidencia. - Revisiones periódicas de acceso no se evidencia en la documentación dicha frecuencia. De acuerdo con la sesión obtenida con el área de Seguridad y CH, no hay un proceso formal para la comunicación en la deshabilitación de accesos de los usuarios. No obstante, para la asignación de accesos se sigue el procedimiento por medio de la mesa de ayuda. No existe una desactivación inmediata de los identificadores o usuarios que dejan la compañía, y no se cuenta con una formalidad en las revisiones periódicas de los usuarios.

9.2.3 Gestión de derechos de acceso con privilegios especiales	**Hallazgos identificados**
	De acuerdo con la información suministrada se evidencia la aplicación de éste punto en la norma de seguridad informática. Sin embargo se puede adicionar oportunidades de mejora para cumplir con los controles que establece la norma para este punto como, por ejemplo, no se evidencian lineamientos y procedimientos que definan la gestión de derechos de accesos de los usuarios con privilegios especiales, tales como administradores de base de datos, redes y comunicaciones, controlador de dominio, accesos a centro de datos, áreas restringidas, entre otros. De acuerdo con la sesión obtenida con el Área de Seguridad y Área de CH no hay un proceso formal para la comunicación en la deshabilitación de accesos de los usuarios. No obstante, para la asignación de accesos se sigue el procedimiento por medio de la mesa de ayuda. No existe una desactivación inmediata de los identificadores o usuarios que dejan la institución, y no se cuenta con una formalidad en las revisiones periódicas de los usuarios.
9.2.4 Revisión de derechos de acceso de usuarios	**Hallazgos identificados**
	De acuerdo con la información suministrada no se evidencia la aplicación de este punto en la política y norma de seguridad informática, ni se obtiene evidencia de procedimientos que definan la revisión periódica de los accesos de los usuarios. De acuerdo con la sesión obtenida con el área de seguridad no se cuenta con un proceso formal definido para la revisión y el mantenimiento de los accesos y privilegios en las

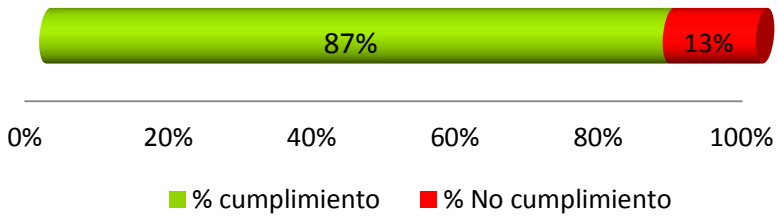
	aplicaciones institucionales definido con una frecuencia.
9.2.5 Eliminación o ajuste de derechos de acceso	**Hallazgos identificados**
	De acuerdo con la información suministrada no se evidencia de procedimientos que definan la revisión periódica de la eliminación de accesos. De acuerdo con la sesión obtenida con el Área de Seguridad y consultas realizadas con el CH el mecanismo de comunicación para la revocación o eliminación de los accesos se efectúa por medio de cada Jefatura quien le comunica al Área de Soporte encargada de la deshabilitación. Sin embargo, actualmente, no hay control para asegurar que los accesos y privilegios se mantienen correctamente.
A9.3 Responsabilidades del Usuario	
9.3.1 Uso de información de autenticación secreta	**Hallazgos identificados**
	De acuerdo con la información suministrada, en el documento Política de Seguridad si se evidencia un apartado que define las obligaciones y prácticas a seguir en el uso de información confidencial. Además, si se advierte sobre la no divulgación de la información confidencial a terceros, se hace mención también sobre la gestión de contraseñas y la longitud mínima, además de los ejemplos sobre cómo crear contraseñas robustas, el debido cambio en el inicio de sesión la primera vez, entre otros. Además, gestiona y tiene normado lineamientos sobre la no divulgación de la información confidencial a terceros, la gestión de contraseñas, entre otros.
A9.4 Control de acceso de Sistemas y Aplicaciones	
9.4.1 Restricción de acceso a la información	**Hallazgos identificados**

	De acuerdo con la información suministrada, existe en los documentos Política de Seguridad un apartado sobre los lineamientos que establece lo relacionado con cuentas de usuarios, perfiles, permisos en los diferentes módulos y componentes de aplicaciones. Adicionalmente, existen políticas para el control de accesos a la red, dominio, y un procedimiento para la clasificación y etiquetado de la información. No obstante, en la política de control de accesos se determinan acciones correctivas indicadas en puntos anteriores. De acuerdo con la sesión obtenida con el Área de Seguridad a nivel de restricción de acceso a los sistemas institucionales, los mismos son gestionados por medio del *Active directory*. Lo que no existe, actualmente, es un control o monitoreo frecuente sobre el mantenimiento de los accesos a la información. Además, para acceder a la red institucional, de igual forma, deben realizarse una serie de permisos para habilitar la navegación. Adicionalmente y valorado en controles anteriores se encuentra en proceso de elaboración el procedimiento para la clasificación y etiquetado de la información mismo que debe normar los lineamientos para el acceso a la información de acuerdo con el nivel de categorización de esta.
Resumen	
Nivel de cumplimiento	

9.1	Requerimientos de negocio para el control de acceso	√
9.1.1	Política de control de acceso	√
9.2	Gestión de accesos de usuario	√
9.2.1	Registro y baja del usuario	√

9.2.2	Gestión de privilegios	√
9.2.3	Gestión de derechos de acceso con privilegios especiales	√
9.2.4	Revisión de derechos de acceso de usuarios	√
9.2.5	Eliminación o ajuste de derechos de acceso	X
9.3	Responsabilidades del usuario	X
9.3.1	Uso de información de autenticación secreta	√
9.4	Control de acceso de sistemas y aplicaciones	√
9.4.1	Restricción de acceso a la información	√

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula A.10

Definición según el dominio de la norma – Criptografía

Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad , autenticidad y / o integridad de la información.

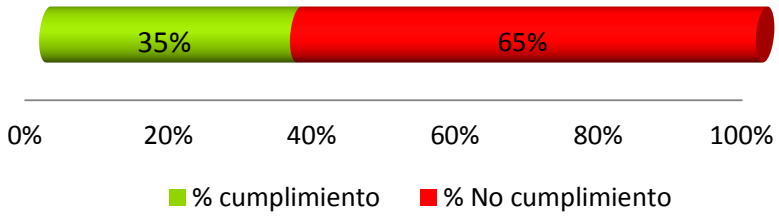
Madurez

Nivel de madurez general

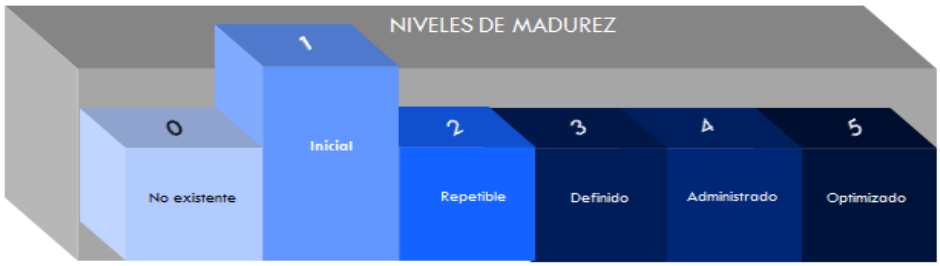
Situación evidenciada	
A10.1 Controles Criptográficos	
10.1.1 Política en el uso de controles criptográficos	**Hallazgos identificados**
	De acuerdo con la información suministrada no se tiene evidencia de documentación formal que defina los lineamientos sobre el uso de controles criptográficos para la protección de la información. De acuerdo con la sesión obtenida con el Área de Seguridad, el uso de controles criptográficos no se gestiona actualmente. La gestión sobre el uso de controles criptográficos se encuentra dentro del nuevo PETI.
10.1.2 Gestión de llaves	**Hallazgos identificados**
	De acuerdo con la información suministrada, a pesar de que existe la Política de Seguridad Informática que determinan los lineamientos sobre las gestión de password a nivel de usuario, no así se determina un documento o apartado dentro de las políticas o normas sobre la gestión de claves de cifrado con el uso de técnicas criptográficas. De acuerdo con la sesión obtenida con el Área de Seguridad, el uso de controles criptográficos no se gestiona actualmente. La gestión sobre el uso de controles criptográficos se encuentra dentro del nuevo PETI.

Nivel de cumplimiento		
10.1	Controles criptográficos	✗
10.1.1	Política en el uso de controles criptográficos	✗
10.1.2	Gestión de llaves	✗

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula A.11
Definición según el dominio de la norma – Seguridad Física y del Entorno
Para cumplir con este dominio de la norma ISO 27001, el acceso a la información debe ser controlado de acuerdo con los requerimientos del negocio. Para esto, deben tenerse en cuenta las políticas de acceso y la autorización para el acceso a la información.
Madurez
Nivel de madurez general



Situación evidenciada	
A11.1 Áreas seguras	
11.1 Perímetro de seguridad física	**Hallazgos identificados**
	De acuerdo con la información suministrada en el documento de Políticas de Seguridad si se menciona en el lineamiento sobre la seguridad física y ambiental; sin embargo, el contenido de los lineamientos no sustentan directrices para la aplicación de las medidas y buenas prácticas en materia de seguridad física y ambiental. De acuerdo con la sesión obtenida con el Área de Seguridad si se cuenta con lineamientos definidos para áreas con manejo de información sensible, tales como el centro de datos, áreas como redes y soporte únicamente se accede con acceso electrónico entre otros pisos críticos. No obstante, las demás dependencias de la institución no necesariamente cumplen con estos controles. Existe una guía de mejores prácticas en los centros de procesamiento de datos que norma todos los lineamientos respecto al perímetro de seguridad física. Adicionalmente si se utiliza un registro de entrada y salida del personal que está de visita en la organización, sin embargo las visitas también entran sin identificarse, sin badge y los mismos funcionarios les abren las puertas, sin preguntarles el motivo de la visita o a donde van.

	Se realizó una visita el centro de datos y donde se determinó lo siguiente: - *Racks* abiertos sin ningún tipo de cerradura. - Existen cámaras visibles y ubicadas en sitios estratégicos para determinar quién está accediendo algún equipo, sin embargo no dan un panorama total del lugar. - Se carecen de controles para restringir realizar la toma de fotografías o grabar vídeos. - Hay cables en los dispositivos ubicados en los *racks* sin etiquetar, los mismos pueden ser manipulados y cambiados de lugar sin que nadie se percate.
11.1.2 Controles físicos de entrada	**Hallazgos identificados**
	De acuerdo con la información suministrada se evidencia documentación formal que norma la seguridad física, además se detecta los lineamientos en seguridad física para las áreas que contienen información crítica para la organización, entre otros. A pesar de que el documento de políticas de seguridad si lo mencionan, el contenido no es claro, explícito sobre los controles físicos de entrada. De acuerdo con la sesión obtenida y revisión a distintos lugares no se evidencian estrictos controles de entrada adecuados. Durante las visitas realizadas se logró vulnerar el control de acceso principal a la organización logrando acceder a cualquier área de la organización, porque los guardas de seguridad no consultan sobre la visibilidad del gafete institucional. Al centro de datos logró ingresarse acompañado de un funcionario con acceso autorizado; sin embargo, en dicha visita se vulneró el

	control para el registro de acceso manual.
11.1.3 Seguridad de oficinas, cuartos y facilidades	**Hallazgos identificados**
	De acuerdo con la información suministrada se evidencia documentación formal que norma la seguridad física para oficinas, salas e instalaciones. De acuerdo con la sesión obtenida y revisión a distintos lugares no se evidencian estrictos controles de entrada adecuados. Durante las visitas realizadas logró vulnerarse el control de acceso principal a la organización logrando acceder a cualquier área de la organización, porque los guardas de seguridad no consultan sobre la visibilidad del gafete institucional. Al centro de datos logró ingresarse acompañado de un funcionario con acceso autorizado; sin embargo, en dicha visita, se vulneró el control para el registro de acceso manual.
11.1.5 Trabajo en áreas seguras	**Hallazgos identificados**
	De acuerdo con la información suministrada se encuentra evidencia del control que norma los lineamientos para las áreas de trabajo seguras (centro de datos, áreas de acceso restringido con equipos críticos, otros) y que establece los lineamientos de seguridad. De acuerdo con la información obtenida de la revisión efectuada al centro de datos (área segura) se evidenciaron carencia de controles para este tipo de áreas.
11.1.6 Áreas de entrega y carga	**Hallazgos identificados**
	De acuerdo con la información suministrada se evidencia documentación formal que norma los lineamientos y establece el procedimiento para las áreas de entrega y carga para que solo sean de acceso del personal autorizado. De acuerdo

	con la sesión obtenida con el Área de Seguridad si existen áreas de carga y descarga, pero únicamente en lo que respecta a las zonas críticas o restringidas. Se notó, además, por ejemplo, el ingreso de personal externo con material inmobiliario en un área de no descarga. No se evidenció documentación que norme el lineamiento para los mecanismos de carga y descarga.
11.2 Equipo	
11.2.1 Instalación y protección de equipo	**Hallazgos identificados**
	De acuerdo con la información suministrada se obtiene evidencia suficiente que satisfaga esté punto. Adicionalmente, hay evidencia de documentación formal que norma o establece el procedimiento de protección de los equipos, tales como protección contra amenazas ambientales, daños físicos, robo y/o hurto, entre otros. A pesar de que se cuenta con una guía para la implantación de las mejores prácticas en la gestión de los centros de datos de datos, la. Al menos en la visita realizada al centro de datos no se obtuvo evidencia de la prohibición de algún tipo de alimento, dispositivo extraíble, lo que provocaría fuga de información o daño.
11.2.2 Servicios de soporte	**Hallazgos identificados**
	De acuerdo con la información suministrada si se evidencia documentación formal que define los lineamientos sobre la protección contra fallas de energía y otras interrupciones esto con los lineamientos en la UPS. De acuerdo con la sesión obtenida con el área de Servicios técnicos y encargados del Centro de datos cada unidad es responsable de la gestión, mantenimiento y revisión de los equipos de TI que tienen a

	cargo, por lo que la aplicación e implementación de un programa de revisión, mantenimiento y verificación es de cada área, ya que los cambios e innovación se hacen según el POA. Existe una guía de configuración segura de los equipos; sin embargo, es una guía de recomendaciones y buenas prácticas. Por ejemplo, con el tema de los Windows XP la organización aún cuenta con bastantes equipos, por lo que no se determina un plan de capacidad y de prevención para determinar este tipo de riesgos.
11.2.3 Seguridad en el cableado	**Hallazgos identificados**
	Si se determina documentación referente a los lineamientos sobre la seguridad en el cableado de red. De acuerdo con la revisión efectuada existe una adecuada separación entre los cables de alimentación de energía y de comunicaciones, una adecuada protección e instalación del cableado en todas las sucursales.
11.2.4 Mantenimiento de equipos	**Hallazgos identificados**
	A pesar de que existe documentación que define apartados sobre el adecuado mantenimiento de los equipos, documentos de sobre el estudio de códigos maliciosos que disponen las buenas prácticas por seguir en el mantenimiento de la infraestructura tecnológica. De acuerdo con la sesión obtenida existe un programa de mantenimiento que se efectúa cada tres meses. Sin embargo, al respecto no se tiene un control sobre las demás unidades o sitios de la institución. Dentro de las políticas y normas no se define la frecuencia para la realización del mantenimiento por lo que queda a discreción de cada área, no obstante si se incentiva a la ejecución de los programas de mantenimiento. No hay un proceso definido formalmente para la realización de un

	mantenimiento preventivo y correctivo.
11.2.5 Retiro de activos	**Hallazgos identificados**
	De acuerdo con la información suministrada se obtiene evidencia de documentación que defina los lineamientos o control para el retiro de equipo, manejo de información o software. Actualmente no hay un estricto control sobre el retiro de activos de la organización. La seguridad física no aplica el estricto control de solicitud de los permisos, boleta de salida de equipos, solicitud del gafete institucional, entre otros.
11.2.6 Seguridad en el equipo	**Hallazgos identificados**
	De acuerdo con lo corroborado no se evidencia documentación que defina los lineamientos sobre la seguridad que debe ser aplicada a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de los sitios de la organización. No existe la definición y aplicación de este control dentro de los actuales procesos de la gestión de la seguridad de la información.
11.2.7 Eliminación segura o reutilización del equipo	**Hallazgos identificados**
	De acuerdo con lo corroborado no se evidencia documentación que defina los lineamientos sobre la eliminación segura de información de los equipos en todas las unidades de almacenamiento. De acuerdo con la sesión obtenida con el Área de Seguridad actualmente se carece de un procedimiento para el control de la eliminación segura de información.
11.2.8 Equipo de usuario desatendido	**Hallazgos identificados**

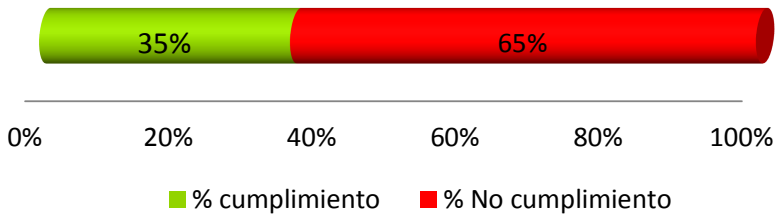
	De acuerdo con la revisión efectuada a las políticas y normas de seguridad si se detecta la evidencia de lineamientos que definan el procedimiento para que los usuarios conozcan las prácticas a efectuar cuando son desatendidos. De acuerdo con la sesión obtenida con el Área de Seguridad actualmente no se manejan políticas para gestionar el riesgo de contar con equipo desatendido. En algunas de las visitas a oficinas se notaron debilidades en este control.
11.2.9 Política de escritorio limpio y pantalla limpia	**Hallazgos identificados**
	De acuerdo con la revisión efectuada las políticas y normas de seguridad se detecta la evidencia de documentación formal que defina la política de escritorio limpio y de pantalla limpia.

Nivel de cumplimiento

11.1	Áreas seguras	✗
11.1.1	Perímetro de seguridad física	✗
11.1.2	Controles físicos de entrada	✗
11.1.3	Seguridad de oficinas, habitaciones y facilidades	✗
11.1.5	Trabajo en áreas seguras	✗
11.1.6	Áreas de entrega y carga	√
11.2	Equipo	✗
11.2.1	Instalación y protección de equipo	√
11.2.2	Servicios de soporte	✗
11.2.3	Seguridad en el cableado	√
11.2.4	Mantenimiento de equipos	✗
11.2.5	Retiro de activos	✗
11.2.6	Seguridad en el equipo	✗
11.2.7	Eliminación segura o reutilización del equipo	✗

11.2.8	Equipo de usuario desatendido	X
11.2.9	Política de escritorio limpio y pantalla limpia	√

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula A.12

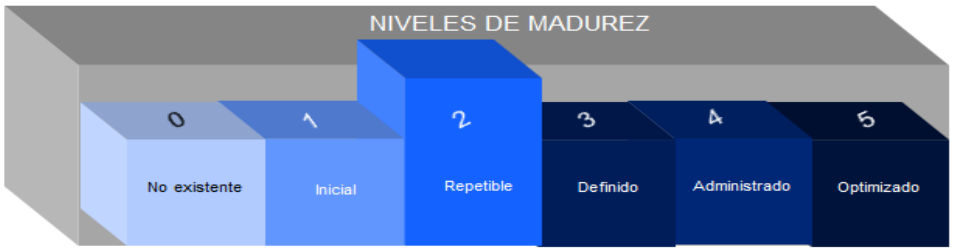
Definición según el dominio de la norma – Seguridad en las operaciones

Para cumplir con este dominio de la norma ISO 27002, dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios.

El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.

Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

Madurez

Nivel de madurez general	
	
A 12.1 Procedimientos Operaciones y Responsabilidades	
12.1.1 Documentación de procedimientos operacionales	**Hallazgos cumplidos**
	De acuerdo con la información suministrada se evidencia documentación formal sobre documentación en la aplicación de procedimientos operacionales que ayuden en la gestión del SGSI así como el Área de Apoyo para la creación de la documentación, metodología, procesos y lineamientos.
12.1.3 Gestión de la capacidad	**Hallazgos identificados**
	De acuerdo con la revisión efectuada se detecta la existencia de tanto del área encargada como de la documentación formal que define el desarrollo de un plan para la administración de la capacidad y el desempeño de la plataforma tecnológica.
12.1.4 Separación de desarrollo , pruebas y producción	**Hallazgos identificados**
	De acuerdo con la revisión efectuada se cumple en el Ciclo de Desarrollo de Sistemas con los tres ambientes necesarios para el cumplimiento de este punto.
A 12.2 Protección de Malware	

12.2.1 Controles	**Hallazgos identificados**
	Si se determina documentación referente a los lineamientos sobre los controles y manejo contra malware. De acuerdo con la revisión efectuada existe una adecuada gestión en los controles existentes.
A 12.3 Backups	
12.3.1 Información de respaldo	**Hallazgos identificados**
	De acuerdo con la revisión efectuada se obtiene evidencia de procedimientos y lineamientos en los procesos de respaldo de los datos así como todo un proceso previo de solicitud de la información a respaldar con temas como frecuencia, dueño de los datos, fechas, puntos de respaldo, sitio seguros para su mantenimiento, tamaño y según la clasificación dada por la institución para los datos por respaldar se establecen periodos de retención.
A12.4 Registro y monitoreo	
12.4.1 Registro de eventos	**Hallazgos identificados**
	De acuerdo con la revisión efectuada se obtiene evidencia de procedimientos que insten sobre la habilitación de la configuración de los registros de eventos, además del uso de indicadores y métricas de seguridad que permitan evaluar la consecuencia de los objetivos de seguridad establecidos. Con los registros pueden evaluarse la eficacia y éxito de los controles de seguridad implantados. Actualmente, no se tienen activas todas las bitácoras o

	pistas de auditoría. Hoy se tienen únicamente bloqueo de cuentas, login, cierre de sesión, acceso a objetos o bitácoras, pero solo para algunos sistemas.
A12.5 Control de Software Operacional	
12.5.1 Instalación de software en sistemas operacionales	**Hallazgos identificados**
	De acuerdo con la revisión efectuada se evidencia documentación explicita sobre el procedimiento para la instalación de software, que tipo de software deben contener los equipos, quienes pueden instalar software, como procede a solicitarse la instalación de algún software, entre otros. De acuerdo con la sesión obtenida con el Área de Seguridad y con las visitas realizadas existe una lista de software autorizado. En caso de requerir algún tipo de software nuevo debe realizarse todo un proceso de estudio para aprobar el nuevo software. No obstante, en algunas áreas, esto no se cumple y algunos usuarios cuentan con permisos de administrador y en donde se detectan software no autorizado.
A12.6 Gestión de vulnerabilidades técnicas	
12.6.1 Gestión de vulnerabilidades técnicas	**Hallazgos identificados**
	De acuerdo con la información corroborada, se evidencia información relacionada con la gestión de vulnerabilidades técnicas a los sistemas de información, así como un procedimiento definido, formalmente, para la realización de escenarios de identificación de vulnerabilidades técnicas. De acuerdo con la sesión obtenida con el Área de Seguridad, actualmente, la

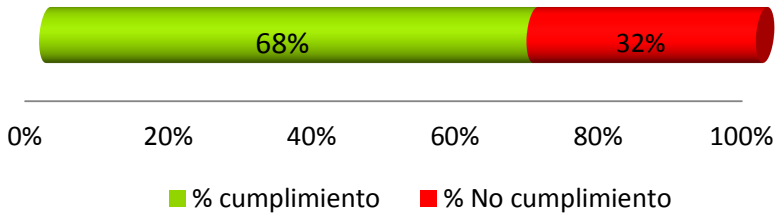
	gestión sobre vulnerabilidades a la plataforma se realiza siempre. Es un proceso definido que se realiza cada 4 meses y que forma parte de los procesos críticos del área de seguridad.
12.6.2 Restricciones en la instalación de software	**Hallazgos identificados**
	De acuerdo con la revisión efectuada a la Política de seguridad Informática. El Área de Seguridad maneja un estándar de software autorizado, existe todo un flujo diseñado para la gestión del software autorizado. Los usuarios en las oficinas no cuentas con los permisos de instalación de software. No obstante, en algunas revisiones efectuadas a otras dependencias, estas no cumplen con lo anterior y existen usuarios que poseen cuentas con privilegios de administrador, y no tienen restricciones para la instalación de software.

Nivel de cumplimiento

12.1	Procedimientos Operacionales y Responsabilidades	√
12.1.1	Documentación de procedimientos operacionales	√
12.1.3	Gestión de la capacidad	√
12.1.4	Separación de desarrollo, pruebas y producción	√
12.2	Protección de malware	√
12.3	Backups	√
12.4	Registro y monitoreo	✗
12.4.1	Registro de eventos	✗
12.5	Control de software operacional	✗
12.5.1	Instalación de software en sistemas operacionales	√
12.6	Gestión de vulnerabilidades técnicas	✗
12.6.1	Gestión de vulnerabilidades técnicas	√

12.6.2 Restricciones en la instalación de software

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula A.13

Definición según el dominio de la norma – Seguridad en las Comunicaciones

Para cumplir con este dominio de la norma ISO 27002, Garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas. Debería establecerse el informe formal de los eventos y de los procedimientos de escalada.

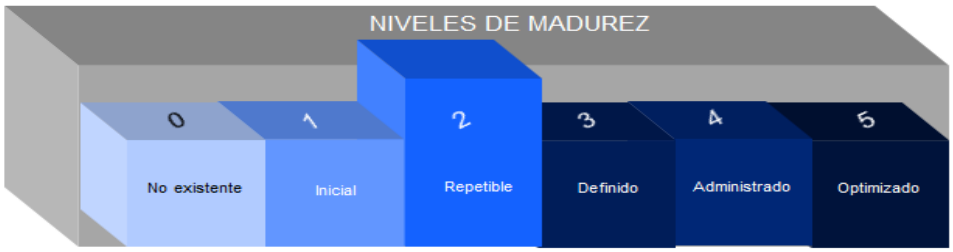
Todos los empleados, contratistas y terceros deberían estar al tanto de los procedimientos para informar de

los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos

Organizacionales. Se les debería exigir que informen de cualquier evento o debilidad en la seguridad de información lo más rápido posible y al punto de contacto designado.

Madurez

Nivel de madurez general



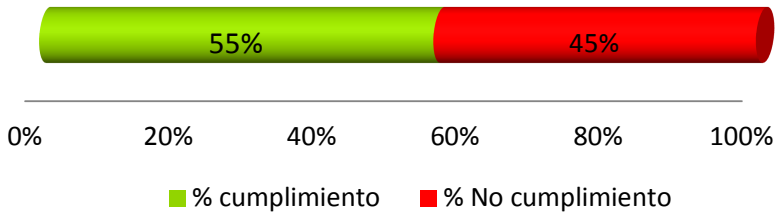
Situación evidenciada	
A 13.1 Gestión de la seguridad en redes	
13.1.2 Controles	**Hallazgos identificados**
	De acuerdo con la documentación si se evidencia de documentación formal y la aplicación de controles de seguridad, los cuales son revisados en un monitoreo constante 24/7. Existe una segregación de red dentro de la institución para no permitir accesos no autorizados.
A 13.2 Transferencia de información	
13.2.1Políticas y procedimientos para la transferencia de información	**Hallazgos identificados**
	De acuerdo con la revisión efectuada se evidencia documentación relacionada sobre procedimientos o lineamientos para la transferencia de información. De acuerdo con la revisión efectuada, no existe dentro de la política de seguridad informática los lineamientos para la transferencia o intercambio de información en los canales de comunicaciones; sin embargo, el control es delegado a los responsables de tal fin con el uso de buenas prácticas.
13.2.3 Mensajería electrónica	**Hallazgos identificados**
	De acuerdo con la información suministrada se obtiene evidencia sobre medidas aplicadas a los servicios de

	mensajería electrónica por ejemplo no existen chats internos. No obstante si existen medidas para medios como el correo electrónico. No se permiten servicios como las redes sociales, entre otros. Actualmente, la organización utiliza el servicio Skype como chat oficial interno.

Nivel de cumplimiento

13.1	Gestión de seguridad en redes	√
13.2	Transferencia de información	X
13.2.1	Políticas y procedimientos para la transferencia de información	X
13.2.3	Mensajería electrónica	√

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula A.14

Definición según el dominio de la norma – Adquisición, Desarrollo y Mantenimiento de Sistema

Para cumplir con este dominio de la norma ISO 27002, debe garantizarse que la seguridad es parte integral de los sistemas de información.

Dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios.

El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información. Todos los requisitos de seguridad deberían identificarse en la fase de recolección de requerimientos de los requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

Madurez

Nivel de madurez general

Situación evidenciada

A14.1 Requerimientos de seguridad de Sistemas de Información

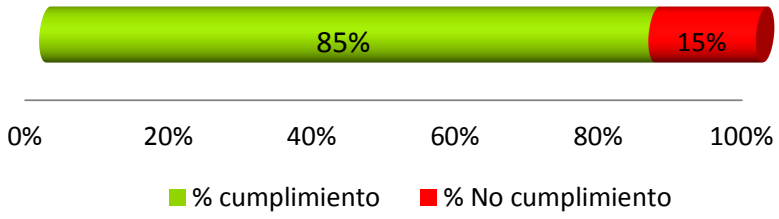
14.1.1 Análisis y especificación de requerimientos de seguridad	**Hallazgos identificados**
	De acuerdo con la información solicitada se obtiene evidencia de documentación formal que defina el análisis y especificación de requerimientos de seguridad para los nuevos y existentes sistemas de información. De acuerdo con la sesión obtenida con el Área de Seguridad, actualmente los requerimientos en sistemas de información en materia de seguridad de la información se proporciona, por lo que el proceso de requerimientos de seguridad sí se desarrolla.

A14.2 Seguridad en el proceso de desarrollo y soporte	
A14.2.1 Política de desarrollo seguro	**Hallazgos identificados**
	Se evidencia en el documento de políticas de seguridad un apartado sobre los lineamientos para el desarrollo de sistemas de información. De acuerdo con la sesión obtenida con el área de Seguridad, durante ninguna fase del ciclo de vida de los desarrollos de sistemas se incorpora a la Área de seguridad para valorar y gestionar el manejo de la seguridad como parte de las prácticas de desarrollo seguro. Sin embargo, es parte del procedimiento de desarrollo de sistemas de TI.
14.2.2 Procedimientos de control de cambios	**Hallazgos identificados**
	Se evidencia el documento Procedimiento para la gestión de cambios y formulario para cambios. El cual incorpora toda una metodología para gestionar los cambios tanto normales como de emergencia adicionalmente se tienen indicadores.
14.2.7 Desarrollo tercerizado	**Hallazgos identificados**
	De acuerdo con la evidencia en los documentos de políticas y normas de seguridad se evidencian los lineamientos para el desarrollo de sistemas de acuerdo con las políticas o estándares de seguridad institucional en el desarrollo de proyectos de software tercerizados. De acuerdo con la revisión efectuada y sesión obtenida con el Área de Seguridad los lineamientos para el desarrollo tercerizado se realiza de acuerdo con lo estipulado tanto en el cartel de la licitación, y adicionalmente las normas de seguridad así lo estipulan, no obstante no se observa que a los terceros contratados para el desarrollo tercerizado se les haga saber lo estipulado en las normas de seguridad en lo estipulado para el desarrollo, mantenimiento y actualización de sistemas de información.

	Aunque si se lleva un control del proyecto donde estos temas deben revisarse.
14.2.8 Pruebas de seguridad del sistema	**Hallazgos identificados**
	De acuerdo con la información suministrada no se observa información relacionada sobre la aplicación de pruebas de seguridad en el desarrollo de sistemas antes de ser puestos en producción. No se evidencia la metodología de desarrollo sobre la ejecución de las pruebas de seguridad a los nuevos y/o modificados sistemas de información. De acuerdo con la sesión obtenida con el Área de Seguridad no se realizan pruebas de seguridad del sistema, al menos al área de seguridad informática no se toma en cuenta.
14.2.9 Pruebas de aceptación del sistema	**Hallazgos identificados**
	De acuerdo con la información suministrada se obtiene evidencia de la definición de un programa de pruebas de aceptación y criterios establecidos para los nuevos sistemas de información, actualizaciones y nuevas versiones. De acuerdo con la sesión obtenida con el área de TI se realizan pruebas de aceptación del sistema.
A 14.3 Datos de prueba	
14.3.1 Protección de datos de prueba	**Hallazgos identificados**
	De acuerdo con la información suministrada no se obtiene evidencia de la definición de la protección sobre los datos de prueba que van a ejecutarse para el testeo del nuevo desarrollo. De acuerdo con la sesión obtenida con el área de TI no hay definidos actualmente controles para la protección de los datos de prueba para los sistemas de información que se encuentran próximos a salir a producción.
Nivel de cumplimiento	

14.1	Requerimientos de seguridad de Sistemas de Información	√
14.1.1	Análisis y especificación de requerimientos de seguridad	√
14.2	Seguridad en el proceso de desarrollo y soporte	√
14.2.1	Política de desarrollo seguro	√
14.2.2	Procedimientos de control de cambios	√
14.2.7	Desarrollo tercerizado	√
14.2.8	Pruebas de seguridad del sistema	√
14.2.9	Pruebas de aceptación del sistema	√
14.3	Datos de prueba	✗
14.3.1	Protección de datos de prueba	✗

Porcentaje de cumplimiento



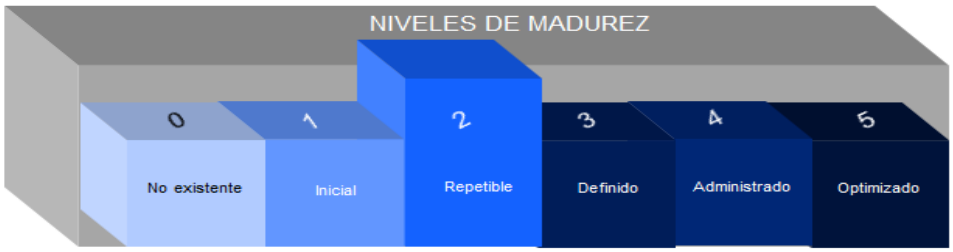
Requisitos ISO 27001:2013 - Cláusula A.15

Definición según el dominio de la norma – Relaciones con Proveedores

Para gestionar las relaciones con los proveedores y estipular la correcta administración de los recursos contratados.

Madurez

Nivel de madurez general



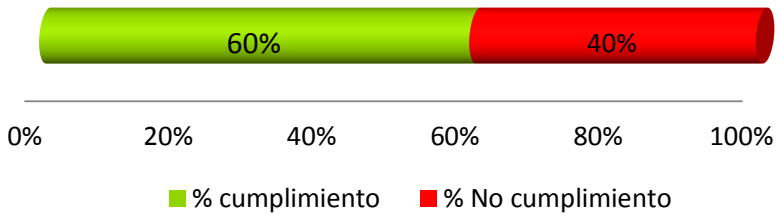
Situación evidenciada	
A15.1 Seguridad en relaciones con el proveedor	
15.1.2 Atención de tópicos de seguridad dentro de los acuerdos con proveedores	**Hallazgos identificados** De acuerdo con la revisión efectuada en los documentos de las políticas y normas de seguridad se definen los lineamientos para el tratamiento de la información corporativa con terceros y que define todas las pautas para que los mismos se acojan a los lineamientos de seguridad institucional. De acuerdo con la sesión obtenida con el Área de Seguridad y los lineamientos definidos en las normas y políticas de seguridad sí hay definidos lineamientos para el trato con terceros. Sin embargo, se carecen de algunas medidas o controles de seguridad necesarios para el trato con terceros. Por ejemplo, no se exigen el uso de gafete corporativo de los terceros para el acceso a las instalaciones, adicionalmente no hay un registro o control de acceso y salida de terceros a la institución.
A 15.2 Gestión de entrega de servicios de proveedor	
15.2.1 Monitoreo y revisión de servicios de proveedor	**Hallazgos identificados** De acuerdo con la documentación no se observa evidencia sobre la aplicación de un monitoreo continuo sobre los servicios del proveedor. De acuerdo con la sesión obtenida con el Área de seguridad, semanalmente existen reuniones de seguimiento sobre el proyecto en ejecución, además existe un control sobre lo definido en el cartel y los productos

	o actividades que deben ser proporcionadas en los tiempos definidos por ambas partes.

Nivel de cumplimiento

15.1	Seguridad en relaciones con el proveedor	√
15.1.2	Atención de tópicos de seguridad dentro de los acuerdos con proveedores	√
15.2	Gestión de entrega de servicios de proveedor	✗
15.2.1	Monitoreo y revisión de servicios de proveedor	✗

Porcentaje de cumplimiento

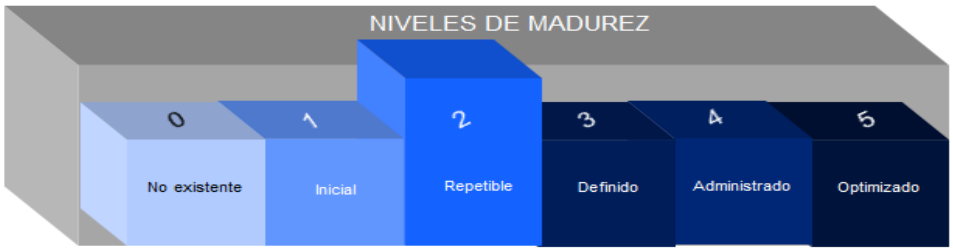


Requisitos ISO 27001:2013 - Cláusula A.16

Definición según el dominio de la norma – Gestión de incidentes

Para garantizar un enfoque coherente y eficaz para la gestión de seguridad de la información, incidentes, incluyendo la comunicación de eventos de seguridad y debilidades.

Madurez

Nivel de madurez general	
	
Situación evidenciada	
A16.1 Gestión de incidentes de seguridad de la información y mejoras	
16.1.1 Responsabilidades y procedimientos	**Hallazgos identificados**
	De acuerdo con la información suministrada se evidencia la existencia de documentación formal que define las responsabilidades y procedimientos de gestión por ser establecidos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. De acuerdo con la sesión obtenida con el Área de Seguridad, actualmente no hay definido un proceso formal para la gestión de incidentes de seguridad de la Información. El área de Seguridad maneja un flujo sobre la gestión de los incidentes, que define la clasificación y el esquema de atención, responsabilidades y roles que deberían ejecutarse.
16.1.2 Reporte de eventos de Seguridad de la Información	**Hallazgos identificados**
	De acuerdo con la información suministrada no se evidencia la existencia de documentación formal que defina el mecanismo o el procedimiento para el reporte de eventos de seguridad de la información. A pesar de que la mesa de ayuda recibe el tiquete de solicitud de atención no hay canal formalizado sobre la gestión de incidentes de seguridad de la información. No hay definidos tiempos de atención, tiempos de respuesta, no hay definidos niveles de atención, entre otros.

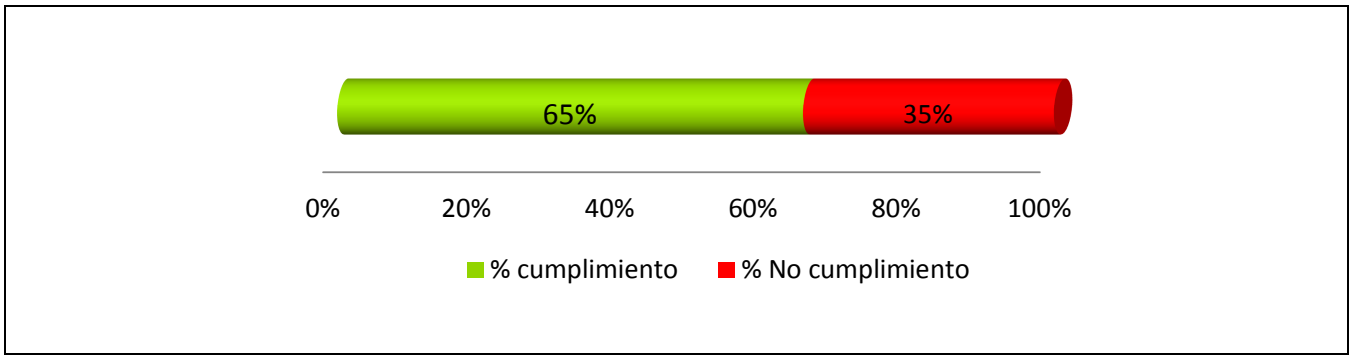
16.1.3 Reporte de debilidades de seguridad de la información	**Hallazgos identificados**
	De acuerdo con la información suministrada no se evidencia la existencia de documentación formal que defina el mecanismo o el procedimiento para que todos los involucrados en los procesos organizacionales reporte las debilidades sobre la seguridad de la información. De acuerdo con la sesión obtenida con el Área de Seguridad, actualmente no hay definido un proceso formal para la gestión de incidentes de seguridad de la información. A pesar de que la mesa de ayuda recibe el tiquete de solicitud de atención no hay canal formalizado sobre la gestión de incidentes de seguridad de la información. No hay definidos tiempos de atención, tiempos de respuesta, no hay definidos niveles de atención, entre otros.
16.1.4 Valoración y decisión de eventos de seguridad de la información	**Hallazgos identificados**
	De acuerdo con la información suministrada no se evidencia la existencia de documentación formal que defina la clasificación de los incidentes de seguridad de acuerdo con la información suscitada, así como el proceso de escalamiento para la atención de los incidentes de acuerdo con el nivel de complejidad, así como la existencia de una bitácora sobre los incidentes de seguridad registrados mensual, trimestral o anualmente.
16.1.5 Respuesta a incidentes de Seguridad de la Información	**Hallazgos identificados**
	De acuerdo con la información suministrada no se evidencia la existencia de documentación formal que defina el procedimiento para dar respuesta a los incidentes de seguridad de la información.
16.1.6 Aprendizaje de incidentes de seguridad de la información	**Hallazgos identificados**
	De acuerdo con la información suministrada no se evidencia la existencia de documentación formal en donde se defina la

	existencia de una base de datos del conocimiento con todos los incidentes registrados, además de la existencia de análisis de los datos sobre los eventos de seguridad más reiterativos con el fin de que todos los usuarios expertos logren dar respuesta eficiente a los incidentes o problemas de seguridad. No existe la definición de una Base de datos de conocimiento de los incidentes de seguridad de la información o un análisis de causa-raíz.
16.1.7 Recopilación de evidencia	**Hallazgos identificados**
	De acuerdo con la información suministrada se evidencia la existencia de documentación formal en donde se define documentar toda la evidencia del incidente de seguridad. Se determina la existencia de un proceso automatizado *(Help desk)* para el registro de incidentes y recopilación de la evidencia.

Nivel de cumplimiento

16.1	Gestión de incidentes de seguridad de la información y mejoras	✗
16.1.1	Responsabilidades y procedimientos	✗
16.1.2	Reporte de eventos de seguridad de la información	✗
16.1.3	Reporte de debilidades de seguridad de la información	✗
16.1.4	Valoración y decisión de eventos de seguridad de la información	✗
16.1.5	Respuesta a incidentes de seguridad de la información	✗
16.1.6	Aprendizaje de incidentes de seguridad de la información	✗
16.1.7	Recopilación de evidencia	√

Porcentaje de cumplimiento



Requisitos ISO 27001:2013 - Cláusula A.17
Definición según el dominio de la norma – Aspectos de Seguridad de la Información para la Gestión de Continuidad del Negocio
La seguridad de la información debe estar implícita en la organización y en su gestión de la continuidad del negocio.
Madurez
Nivel de madurez general

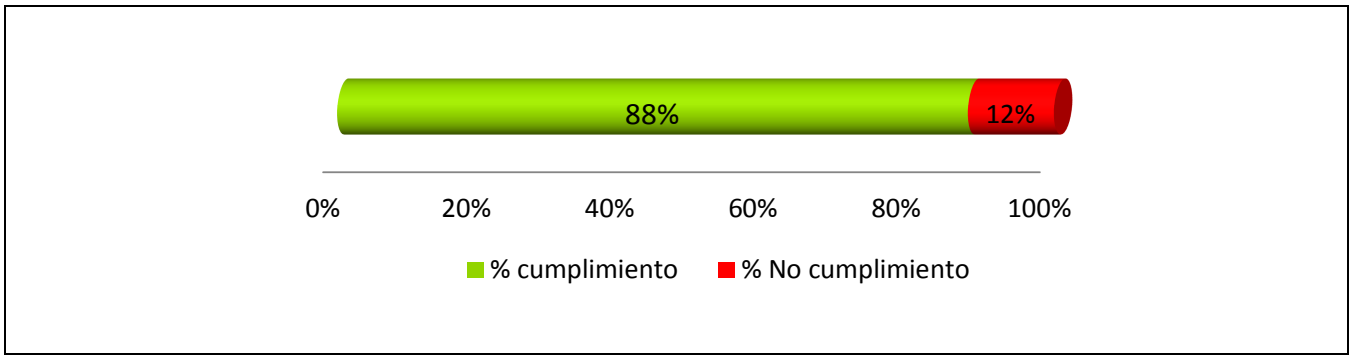
Situación evidenciada	
A17.1Seguridad de la información en la Continuidad	
17.1.1 Planeación la continuidad de la seguridad de la información	**Hallazgos identificados**
	De acuerdo con la información suministrada se evidencia en el documento de política de continuidad la aplicación de lineamientos sobre la continuidad de la seguridad. Además, se evidencia de que se insta a los responsables de la gestión de TI a contar con el BIA y un procedimiento, guía que establece los pasos y recomendaciones necesarias. Se evidencia un plan de recuperación ante desastres, plan de crisis, entre otros. De acuerdo con la sesión obtenida con Continuidad de TI se maneja un manual de continuidad de TI que indica los procedimientos para hacer el plan de continuidad. Dicho plan es distribuido a todas las unidades, para recomendación de que sean implantados. Dicho plan contiene las plantillas para completar el plan de continuidad. De acuerdo con la revisión del plan si se establece como procedimiento la ejecución de análisis de riesgos que contemplen el impacto de negocio. Dentro de los rubros del manual de continuidad si se evidencia el desarrollo de los procedimientos y estrategias de recuperación, así como una sección de recomendaciones de recuperación. Las pruebas de continuidad se realizan periódicamente y se elabora un informe y evaluación de todos los aspectos.
17.1.2 Implementación de Seguridad de la Información en la continuidad	**Hallazgos identificados**
	De acuerdo con la sesión obtenida con la Jefatura del Área de Continuidad de TI la aplicación del plan de continuidad se maneja a nivel país. El área de Continuidad ha realizado las capacitaciones a las demás unidades A nivel de la dirección de TI todas las áreas cuentan un plan de continuidad de TI. Las capacitaciones se efectúan, según el plan de capacitación

	establecido.
17.1.3 Verificación, revisión y evaluación de seguridad de la información en la continuidad	**Hallazgos identificados** De acuerdo con la información corroborada, si existe lineamientos y manejo de planes de continuidad, al menos en lo indicado por los documentos de políticas y normas, se evidencia la correcta aplicación, además se evidencia la existencia de un proceso de verificación, revisión y evaluación en la continuidad de la seguridad en forma periódica. Con base en la sesión obtenida con la Jefatura del de Continuidad de TI las revisiones sobre el cumplimiento con la debida aplicación de los planes de continuidad son efectivas.

Nivel de cumplimiento

17.1	Seguridad de la información en la Continuidad	√
17.1.1	Planeación la continuidad de la seguridad de la información	√
17.1.2	Implementación de seguridad de la información en la continuidad	√
17.1.3	Verificación , revisión y evaluación de seguridad de la información en la continuidad	✗

Porcentaje de cumplimiento

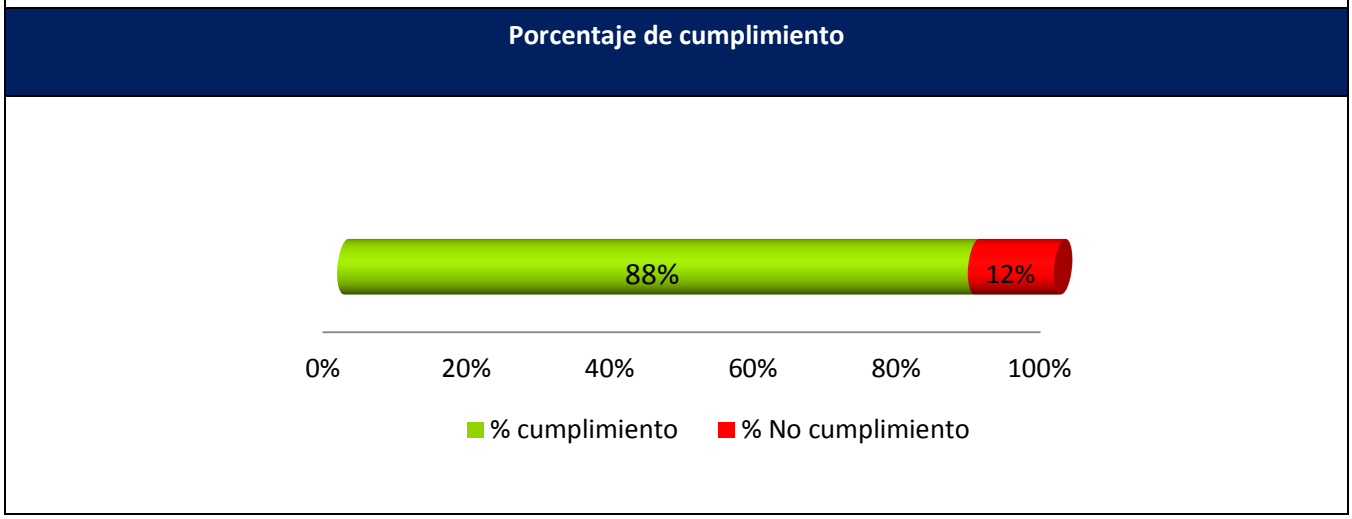


Requisitos ISO 27001:2013 - Cláusula A.18	
Definición según el dominio de la norma – Cumplimiento	
Para evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales en materia de información de seguridad y de los requisitos de seguridad.	
Madurez	
Nivel de madurez general	
	
Situación evidenciada	
A18.1 Cumplimientos de los requisitos legales y contractuales	
18.1.2 Derechos de propiedad intelectual (IPR)	**Hallazgos identificados**
	De acuerdo con la revisión efectuada se evidencia

	documentación que define la aplicación de los derechos de propiedad intelectual para el uso de productos de software, de información, uso de licencias de software adquiridas, transferencia y/o eliminación de software, entre otros. De acuerdo con la información se determinaron las acciones necesarias para el tema de derechos de propiedad intelectual; sin embargo, a la fecha se contemplan solo en los carteles de licitación.
18.1.4 Protección de datos y privacidad de la información personal	**Hallazgos identificados**
	De acuerdo con la revisión efectuada se evidencia documentación formal que define los lineamientos y procedimientos para la protección de datos y privacidad de la información personal. A nivel lógico se exponen debilidades en la seguridad, en algunos casos, por malas prácticas de los usuarios con el manejo de la información.
18.1.5 Regulación de controles criptográficos	**Hallazgos identificados**
	De acuerdo con la información suministrada no hay documentación que evidencie el cumplimiento de este punto. De acuerdo con la sesión obtenida con el Área de Seguridad actualmente no se tiene nada normado, ni existe un proceso de gestión sobre la aplicación y regulación de controles criptográficos. Adicionalmente, la normativa reguladora (Normas técnicas de la CGR) no regula el cifrado de la información no obstante si algunos procesos de seguridad de la información en donde pueden estar envueltos mecanismos de cifrado.
18.2 Revisiones de seguridad de la información	
18.2.1 Revisión independiente de la seguridad de la información	**Hallazgos identificados**
	De acuerdo con la información suministrada hay evidencia de la definición de un proceso de revisión de la

	documentación normativa de la seguridad de la información... Ante ello, debería medirse, una estructura de procesos e indicadores de desempeño sobre esos mismos procesos que realimenten periódicamente el estado de los procesos del área. Actualmente, se hacen revisiones sobre la plataforma, detectando software desactualizado, presencia de malware, entre otros; sin embargo, eso no es suficiente para un área que gestiona la seguridad de la información a nivel de toda la institución. No se encuentran auditorías orientadas a este punto en específico.
18.2.2 Cumplimiento de las políticas y normas de seguridad	**Hallazgos identificados**
	De acuerdo con la información suministrada hay evidencia de la aplicación de dicho proceso del cumplimiento normativo realizado por los responsables de cada área. Así mismo, existe un área de cumplimiento y gobierno que se encargan de este punto.
18.2.3 Comprobación del cumplimiento	**Hallazgos identificados**
	De acuerdo con la información suministrada existe evidencia de documentación que establece las revisiones regulares sobre el cumplimiento de las políticas de seguridad de la de la organización. De acuerdo con la información obtenida y sesión realizada de cómo se ejecutan pruebas a los sistemas de información, los cuales deben ser revisados regularmente por el cumplimiento de las políticas y normas de seguridad de la organización.
Nivel de cumplimiento	
18.1 Cumplimiento de los requisitos legales y contractuales √ **18.1.2** Derechos de propiedad intelectual (IPR) √	

18.1.4	Protección de datos y privacidad de la información personal	√
18.1.5	Regulación de controles criptográficos	X
18.2	Revisiones de seguridad de la información	√
18.2.1	Revisión independiente de la seguridad de la información	√
18.2.2	Cumplimiento de las políticas y normas de seguridad	√
18.2.3	Comprobación del cumplimiento	√



3.4 Identificación de riesgos

A continuación se presenta la identificación de riesgos a los que está sometida la información del BBB, con la finalidad de mitigar, transferir o controlar aquellos riesgos que atenten contra la administración de la seguridad de la información mediante mecanismos definidos y documentados sistemáticamente y se cree un ciclo de mejora continua.

Para la identificación de riesgos a los que está sometida la información del negocio, se han considerado las siguientes fuentes de información:

- Reuniones con diversas áreas de la institución.
- Diagnóstico de seguridad de la información actual.
- Análisis de cumplimiento de la norma ISO/IEC 27001.
- Análisis de fuentes de información observación, documentación y procesos propios institucionales.
- Amenazas.
- Vulnerabilidades

3.4.1 Riesgos identificados

N°	Riesgo	Causa	Nivel de Riego
1	Seguridad de la información.	No se tiene un sistema gestión de la seguridad de la información	Muy Alto
2	Acceso no autorizado a la información contenida en las aplicaciones.	Accesos indetectables por registros de bitácoras incompletos, como en las bases de datos, sistemas operativos, otros.	Alto
		No se realiza supervisión a las bitácoras de los equipos	
		No se realiza supervisión a las bitácoras de los equipos o algunos carecen de ellas.	
		Que no se cuenten con mecanismos eficientes para el control de los usuarios (acceso, operaciones y de privilegios), como gestión de la identidad de los usuarios internos y externos.	
		Usuarios con niveles de privilegios, como usuarios con administradores o con privilegios no propios de su cargo.	

N°	Riesgo	Causa	Nivel de Riego
3	Continuidad de aplicaciones	Falta de afinamiento de la herramienta de evaluación de planes de continuidad y recuperación de desastres.	**Alto**
4	Acceso a la información no autorizada.	Usuarios que ya no tienen necesidad de acceder y / o conocer a la información, como los privilegios para la modificación a los datos.	**Alto**
		Inadecuada segregación de funciones, por lo cual las aplicaciones requieren una revisión de autorizaciones por perfil de usuario.	
5	Divulgación de datos.	Clasificación de información deficiente, ya que no considera la utilización de códigos, sellos, firmas o señales de advertencia según su nivel de seguridad.	**Alto**
		Información revelada a terceros no autorizados durante una emergencia, por lo que es posible que se brinde información a personas no autorizadas durante y luego del evento.	
		Canales de comunicación inseguros, por lo que la información transmitida puede darse a conocer por personas no autorizadas	
		Procesos débiles en la eliminación de la información que está contenida en los medios de almacenamiento móviles, por lo que puede divulgarse cuando este es desechado o reasignado a otro propietario.	
		Ausencia de un custodio de la información, por lo que no hay alguien responsable en aplicar los controles de seguridad.	

N°	Riesgo	Causa	Nivel de Riego
6	Acceso no autorizado a los medios de almacenamiento, expone los datos sensibles a la divulgación.	Los funcionarios no conocen sobre las políticas de medios de almacenamiento, en el análisis de fuentes de información podría observarse que las áreas no aplican los controles referentes al tratamiento adecuado de los medios de almacenamiento que tienen bajo su custodia.	**Alto**
7	Fallas del sistema no se detectan en momentos oportunos.	Falta de registros de bitácoras, por lo que no puede identificarse la razón de las fallas.	**Alto**
8	Incumplimiento de proveedores.	Falta de supervisión de los requisitos de seguridad en los documentos contractuales, por lo cual hay proveedores sin contrato de confidencialidad y pueden divulgar información.	**Alto**
10	Pérdida de la integridad.	Operación del respaldo de datos de información. Uso de extintores en las áreas sensibles.	**Alto**
11	Interrupción de las operaciones del negocio.	La utilización de los equipos y aplicaciones ha sido descontinuada por el proveedor, por lo cual se dificulta el soporte de los equipos y aplicaciones. Ausencia de esquemas de continuidad de los proveedores de servicios críticos, por lo cual se limitaría la operación normal.	**Alto**

N°	Riesgo	Causa	Nivel de Riego
		Que los tiempos de respuesta por parte de TI ante requerimientos, incidentes o problemas de los usuarios sean inadecuados.	
		Cuarto de comunicaciones de las oficinas sin controles requeridos para su protección	
13	Procesos inadecuados	La documentación es escaza en contenido y forma de acuerdo con la normativa buscada.	**Alto**
		Tiempos de respuesta altos en incidentes.	
		SGSI no conocido por todos	
		Contratación de personal	
		Falta de cumplimiento	
14	Procesos estáticos	Falta de directrices de mejora continua	**Alto**

Capítulo IV

Conclusiones y recomendaciones

4 Introducción

El propósito de este capítulo es que por medio de los planes de acción propuestos basados en las deficiencias encontradas, el BBB pueda mejorar el nivel de madurez de la seguridad de la información con la ayuda de un Plan de Gestión de Seguridad de la Información, para conocer, gestionar y minimizar los posibles riesgos y amenazas que atentan contra la seguridad de la información.

Así mismo se busca disminuir las brechas detectadas en el análisis de las mejores prácticas en materia de Seguridad de la Información, a través de los procesos establecidos en normas y estándares internacionales como ISO/IEC 2700.

4.1 Supuestos

Para implementar cada una de las recomendaciones en el corto plazo deben considerarse los siguientes supuestos:

- El alto compromiso de las partes involucradas y el apoyo de la Gerencia es esencial para garantizar el éxito de cada iniciativa.

- El orden de ejecución de las iniciativas descritas en este documento, puede ser modificado, producto de la existencia de otras actividades con alta prioridad para el BBB, el nivel de apetito al riesgo de la Institución versus la inversión en recursos o alguna otra situación imprevista.

- Las recomendaciones en este documento fueron definidos como iniciativas. Por lo tanto, si el BBB modifica alguna de estas acciones a proyecto, debe considerar el impacto que ocasionará en la asignación de recursos y estimación de tiempo para su desarrollo.

El primer paso para documentar las oportunidades de mejora, fue considerar la matriz de evaluación realizado en el capítulo anterior, analizando los resultados de los siguientes criterios:

- Brechas identificadas que deben subsanarse para asegurar la confidencialidad, integridad y disponibilidad de la información del BBB.
- Plan de tratamiento de los hallazgos identificados cuyos plazos de ejecución fueron definidos que serían en el corto plazo, mediante sesiones con el equipo de trabajo, se determinó que las recomendaciones se debía ejecutar a corto plazo y se debía incluir actividades y tareas que no requirieran más recursos de lo existente ni presupuesto adicional.

4.2 Oportunidades de mejora por objetivo de control

ISO 27001:2013 - Cláusula 4 **Contexto de la organización**
Resumen
Conclusiones y Recomendaciones
Debe definirse un documento formal que defina y establezca el alcance del SGSI y que determine las partes o procesos de la organización que van a ser incluidos, así como los procesos críticos que se quieren proteger y por donde se va a iniciar, además de la definición de las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y las áreas que quedarán excluidas en la implantación del SGSI. Esta cláusula determina la creación del primero de los documentos que constituyen el SGSI, "el alcance del sistema". Así como que determine las partes o procesos de la organización que van a ser incluidos, así como los procesos críticos que se quieren proteger, y por donde se va a iniciar, además de la definición de las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y las áreas que quedarán excluidas en la implantación del SGSI.

El resultado de la prueba no es satisfactorio. Se recomienda definir un proceso formal que establezca los procedimientos para la definición, implantación, mantenimiento y mejora continua del SGSI.

Requisitos ISO 27001:2013 - Cláusula 5 Liderazgo
Resumen
Conclusiones y Recomendaciones
El resultado de la prueba es no satisfactorio. De acuerdo con lo anterior, la organización debe considerar el manejo del área de seguridad como parte de uno proceso de vital importancia para la consecución de los objetivos estratégicos de la organización y en apoyo del bienestar y seguridad de los datos de los asegurados. Es importante para ello contar con el apoyo en los siguiente: 1. La alta dirección se sensibilice con el tema del manejo de seguridad de la información y lo veo como parte de uno de los procesos fundamentales de la organización (Seguridad de TI). 1. Que la alta dirección disponga al área de seguridad de la información la independencia absoluta y descentralizada de la dirección de Tecnologías de Información 2. Responsabilizar al área de seguridad velar por la seguridad de la información organizacional, por lo que la misma responda y proporcione los resultados directamente con la alta dirección. 3. Fomentar y definir los procesos del área de seguridad de manera que se tenga establecidos las actividades del área para con toda la organización. 2. Se recomienda definir una estrategia de acuerdo con los recursos con que cuenta el área de seguridad en la implementación de indicadores de desempeño medibles que permitan obtener resultados sobre evaluaciones para medir el nivel de alcance de los objetivos del SGSI. Se puede obtener como oportunidad de mejora incluir dentro del desarrollo del plan de sensibilización una estrategia de comunicación constante de la política de seguridad informática. Se recomienda que la organización, en este caso, la alta dirección adopte el SGSI como un tema de especial interés y se involucre y colabore con el apoyo al Área de seguridad en la ejecución de un adecuado programa de concienciación, para generar la cultura sobre la administración de la seguridad y a partir de allí el Área

de Seguridad pueda tomar un papel aún más relevante dentro de la organización para dar apoyo y soporte necesario y lograr la correcta aplicabilidad y adopción del SGSI en todas las dependencias de la institución. Debe definirse y aplicarse de manera consecuente mediante el diseño de un proceso formal para el desarrollo de un plan de sensibilización y que establezca entre algunos de sus apartados los canales de comunicación y/o soporte, la frecuencia determinada, los responsables de la ejecución, la definición de indicadores de desempeño para la obtención de resultados y valoración del estado de cumplimiento.

Dentro de algunas situaciones se determinaron algunas oportunidades de mejora que podrían incluirse en la política:

La documentación de la política debe delimitar que es lo que se va proteger, de quién y por qué. Debe explicar que es lo que está permitido y qué no. Debe determinar los límites del comportamiento aceptable y cuál sería la respuesta si estos se incumplen, e identificar los riesgos a los que está sometida la organización. La política debe cumplir al menos con las estipulaciones del conglomerado.

Requisitos ISO 27001:2013 - Cláusula 6 **Planeación**
Resumen
Conclusiones y Recomendaciones
El resultado de la prueba no es satisfactorio. Se recomienda definir un proceso formal para la gestión de riesgos de seguridad de la información que evalúe e identifique los riesgos y determine las oportunidades o medidas correctivas. Se recomienda crear y elaborar el estatuto de aplicabilidad del SGSI. Este documento justifica y define los controles que son aplicables a la norma y la justificación de cuáles no son aplicables, así como definir un proceso formal para la gestión de riesgos de seguridad de la información que involucre la gestión

para el tratamiento de los riesgos.

Requisitos ISO 27001:2013 - Cláusula 7
Soporte
Resumen
Conclusiones y Recomendaciones
El resultado de la prueba no es satisfactorio. De acuerdo con lo anterior es necesario formalizar y definir los procesos del área de seguridad de información y documentarlos formalmente estableciendo las políticas, normas, procedimientos, manuales, guías, formularios que deben cumplirse para el adecuado funcionamiento del área y cumplimiento de los objetivos del SGSI.

Requisitos ISO 27001:2013 - Cláusula 8
Operaciones
Resumen
Conclusiones y Recomendaciones
Se recomienda el diseño de un esquema de gobernabilidad de seguridad de la información formalmente definido, donde puedan gestionarse de una forma más clara todos los procesos del área de seguridad, y a partir de allí generar los procedimientos, manuales, guías, formularios necesarios, una vez comprendido el esquema de procesos. Se deben realizar evaluaciones de riesgos en intervalos debidamente planificados al menos durante dos veces al año, o bien, cuando ocurran cambios significativos al SGSI.

Requisitos ISO 27001:2013 - Cláusula 9 Evaluación de desempeño
Resumen
Conclusiones y Recomendaciones
El resultado de la prueba no es satisfactorio. En éste punto se requiere monitorear y medir los procesos de seguridad y controles. Por lo que es necesario contar con: a) los métodos para monitorizar, medir, analizar y evaluar, cuando sea aplicable, para asegurar unos resultados adecuados. b) definir cuándo deberán ser realizadas las monitorizaciones y mediciones c) quién deberá monitorizar y medir. d) cuando deberán ser analizados y evaluados (rangos de normalidad y anomalía) los resultados de la monitorización y medición f) quién analizará y evaluará estos resultados. Para lo anterior, es necesario definir una serie de indicadores sobre los procesos del área de seguridad, pero para ello es indispensable contar con la definición formal de un modelo de gobierno de seguridad y definir posterior los indicadores de desempeño del SGSI, los cuáles deben caracterizarse por cumplir con el principio SMART. Es indispensable en el proceso de gestión de la seguridad de la información un alto compromiso de la dirección. El proceso de gestión de la seguridad de la información es vital para la consecución de los objetivos del negocio, aspecto que es de interés de los altos jerarcas. Para ello es necesario que al menos se establezca una sesión de los altos jerarcas y los responsables de la gestión del SGSI para valorar los temas y decisiones sobre la adecuada gestión del SGSI. Se podría definir que en forma cuatrimestral se ejecuten sesiones de seguimiento para valorar los temas del SGSI en conjunto con la alta dirección. Al menos deben cubrirse los siguientes puntos y que los mismos queden debidamente documentados.

- Revisión del estado de las acciones tomadas en la reunión anterior en relación al SGSI.

- Cambios internos y externos que afecten la seguridad de la información

- Comentarios sobre el desempeño del SGSI

- No conformidades y acciones correctivas detectadas en el SGSI

- Seguimiento y medición del SGSI

- Resultados de la auditoría interna sobre el SGSI

- Cumplimiento de los objetivos del SGSI.

- Retroalimentación de las partes interesadas.

- Resultados de las evaluaciones de riesgo y planes de tratamiento

- Oportunidades de mejora continua al SGSI

Requisitos ISO 27001:2013 - Cláusula 10
Mejoras
Resumen
Conclusiones y Recomendaciones
El resultado de la prueba no es satisfactorio. Se recomienda definir un plan formal que describa las actividades, responsabilidades, canales de acción, tiempos, entre otros, para el establecimiento de la mejora continua del SGSI.

Requisitos ISO 27001:2013 - Cláusula A.5 Política de seguridad
Resumen
Conclusiones y Recomendaciones
El resultado de la prueba no es satisfactorio. La misma debe ser revisada frecuentemente al menos una vez al año. La política de seguridad de la información debe delimitar que es lo que va a protegerse, de quién y por qué. Debe explicar que es lo que está permitido y qué no. Debe determinar los límites del comportamiento aceptable y cuál sería la respuesta si estos se incumplen, e identificar los riesgos a los que está sometida la organización. La política debe cumplir, al menos, con los siguientes requisitos: a. Ser redactada en una manera accesible para todo el personal de la organización b. Debe ser aprobada por la dirección y publicada por la misma. c. Debe ser de dominio público dentro de la organización. d. Debe definir las responsabilidades teniendo en cuenta que éstas van asociados a la autoridad dentro de la compañía. e. Debe indicar que es lo que se protege en la organización (personal, información, imagen, continuidad, reputación) f. Debe ser personalizada para la organización g. Debe señalar las reglas y normas que va adoptar la organización y las medidas de seguridad que serán necesarias. h. Debe definir lo que es seguridad de la información i. Debe definir un objetivo global de la política de seguridad de la información

j. Debe definir el alcance e importancia de la seguridad como mecanismo de control que permite compartir la información.

k. Declaración formal por parte de la dirección apoyando los objetivos y principios de la seguridad de la información.

l. Debe definir las responsabilidades generales y específicas, en las que se incluirían los roles pero nunca a las personas en concreto.

m. Referencias de documentación que pueda sustentar la política.

Adicionalmente, dentro de los temas la política debe incluir: el control de accesos, clasificación de la información, la seguridad física y ambiental, uso aceptable de activos, política de escritorio limpio y pantalla limpia, transferencia de información, BYOD (dispositivos móviles), teletrabajo, política para la restricción de software y su uso, copias de seguridad, protección contra el malware, gestión de vulnerabilidades técnicas, controles criptográficos, la seguridad en las comunicaciones, confidencialidad y protección de la información, gestión de proveedores

Se recomienda definir un período, al menos, una vez al año para revisión de la política de seguridad, además también se recomienda efectuar actualización cada vez que sucedan grandes incidentes de seguridad, después de auditorías sin éxito y/o frente a cambios que afectan a la estructura de la organización.

Requisitos ISO 27001:2013 - Cláusula A.6 **Organización de seguridad**
Resumen
Conclusiones y Recomendaciones
El resultado de la prueba no es satisfactorio. Existe el riesgo de que algún funcionario que cambie rol o función dentro de la organización y que la jefatura correspondiente no deshabilite los accesos y privilegios que le competen al puesto anterior y que en el actual los mantenga. Para lo anterior se

recomienda revisar el proceso de comunicación que garantice el mantenimiento de los accesos a los servicios de la institución. Se recomienda emitir un procedimiento formal y debidamente aprobado para la des habilitación de accesos y privilegios de todo el personal que: cambie de puesto o rol dentro de la organización, se encuentre incapacitado por un período prolongado, renuncie o despido laboral, personas pensionadas o jubiladas, vacaciones prolongadas. Este procedimiento debe definir el mecanismo y canal a utilizar para la comunicación, así como la frecuencia con la que debe realizarse. Adicionalmente se recomienda definir un control para la revisión frecuente sobre el manejo de los accesos con el fin de garantizar una adecuada segregación de las funciones en los sistemas y aplicaciones institucionales.

Se recomienda establecer convenios formales con documentación que lo respalde con autoridades tales como Micitt, OIJ, bomberos, OIJ, organismos reguladores, colegio profesional de informáticos, entre otros.

Se recomienda establecer convenios formales con documentación que lo respalde con comunidades o grupos de interés, clubes de investigación tecnológica, organizaciones referentes en la gestión de la seguridad, para mejorar el conocimiento sobre las mejores prácticas y estar al día con la información de seguridad más pertinente, recibir información temprana de alertas, avisos y parches relacionados con ataques y vulnerabilidades, acceso a los consejos de seguridad de información especializada, compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades, entre otros.

Dentro de la metodología de gestión de proyectos no se tienen definidos los requisitos a nivel de seguridad de la información en la gestión de proyectos. Los mismos se aplican dependiendo del tipo de proyecto que se encuentre en desarrollo. Por lo tanto se recomienda incorporar dentro de la metodología de gestión de proyectos los requisitos necesarios para abordar el tema de seguridad de la información en la gestión de los proyectos, en todas sus fases.

Se requiere gestionar y abordar el tema de BYOD dentro de la organización para lo que se recomienda lo siguiente:

a- Efectuar un diagnóstico para valorar los riesgos a los que actualmente se expone la institución en el tema de BYOD.

b- Definir una estrategia para la gestión del BYOD en la organización

c- Definir dentro de la política de seguridad los lineamientos con la gestión del BYOD. Dicha política

debe definir al menos

-Tipos de dispositivos móviles a gestionar y permitir

- Requisitos a cumplir por parte del usuario para usar en el móvil información de la organización

- Aceptación del control y monitoreo del móvil por parte de la organización con el dispositivo móvil del usuario

- Aceptación de las pautas institucionales en materia de seguridad para uso del móvil que contiene información organizacional

- Efectos legales producto de un mal uso de la información organizacional

- Otros

Requisitos ISO 27001:2013 - Cláusula A.7 **Gestión de los Capital Humano**
Resumen
Conclusiones y recomendaciones
Es necesario de que la gestión del SGSI tome interés por parte de toda la institución. Para ello, es importante que la alta dirección mantenga una alianza con los gestores del SGSI y apoyo en las labores de concientización del manejo de la seguridad de la información. Para ello es importante que desde cada una de las altas esferas se transfiera la sensibilización con el fin de ir transfiriendo el conocimiento con todos los funcionarios. Para lo anterior es indispensable formalizar un plan de sensibilización/concienciación que establezca la mejor estrategia de comunicación y sensibilización para toda la Institución en el tema de seguridad de la información. Se recomienda definir un proceso formal que establezca el procedimiento y los lineamientos para un proceso disciplinario en los casos de malas prácticas en la gestión de la seguridad de la información donde se garantice entre otros detalles proporcionar una respuesta gradual que tome en consideración

factores tales como la naturaleza y gravedad de la infracción y su impacto en la institución.

Se requiere definir como parte de los procesos del área de seguridad la gestión del recurso humano, específicamente en la definición formal de un procedimiento para la terminación del empleo o cambio de empleo dentro de la misma institución.

Requisitos ISO 27001:2013 - Cláusula A.8 Gestión de activos
Resumen
Conclusiones y recomendaciones
Como oportunidad de mejora al procedimiento que actualmente se está gestionando se debe dar un mayor alcance al procedimiento descrito adicionando por ejemplo activos de información como las grabaciones, fotografías que son información y deben estar en forma explícita definidas en el documento. Adicionalmente entre otros detalles, si se especifica el nivel de clasificación de la información, no obstante no se detalla el procedimiento sobre cómo se procede a clasificar la información de acuerdo con los requisitos legales, valor de la información, criticidad, sensibilidad, integridad, disponibilidad y confidencialidad. Hay establecido una frecuencia de revisión para determinar cambios en la clasificación de la información de acuerdo con el ciclo de vida de la misma. Se carece del procedimiento para acceder a la información de acuerdo con su nivel de clasificación. Se excluyen activos de información tales como la información contenida en grabaciones, fotografías, conversaciones, reuniones, dispositivos, otros. Es necesario de que este procedimiento defina los responsables para la administración de la documentación y, con esto, la frecuencia de revisión por ejemplo en el caso de políticas o normas institucionales. Se debe formalizar implementar el proceso para la clasificación y etiquetado de la información. Es necesario de que la definición del procedimiento cumpla con lo siguiente: El etiquetado debe reflejar el sistema de clasificación establecido, ya sea en formato físico o electrónico;

Las etiquetas deben ser fácilmente reconocibles en los documentos.

La asignación de responsables de la información de estar documentada.

Para el manejo y acceso con terceros debe ser reconocible la etiqueta del nivel de clasificación, e evidenciar la garantía de confidencialidad y manipulación de la información, por lo que el procedimiento debe aclarar este punto.

El procedimiento debe orientar y definir de cómo se accede a la información, según su clasificación.

La salida de información de los sistemas debe ser clasificada como sensible o crítica, o bien, llevar una etiqueta de clasificación apropiada.

Es indispensable realizar las mejoras descritas en los controles para la clasificación y etiquetado de la información. Además, es necesario definir en dicho procedimiento el manejo de los activos de información con terceros en el intercambio de información, para identificar la clasificación de dicha información e interpretar las etiquetas de clasificación de otras organizaciones. Además, las restricciones de acceso compatibles con los requisitos de protección de los activos; las copias temporales o permanentes a un nivel compatible con la protección de la información original; mantenimiento y actualización de un registro formal de los receptores autorizados de los activos

Se recomienda definir documentación formal que defina o contenga un apartado sobre los procedimientos para la gestión de medios extraíbles (USB, dispositivos móviles, CD, discos duros externos entre otros) y el manejo de información de acuerdo con el esquema de clasificación de la información. Se recomienda instaurar una política para manejar cifrada la información que se transfiere a partir de medios removibles con el fin de limitar el uso no correcto y la fuga de información.

Se exhorta definir un proceso formal que establezca el procedimiento para la eliminación segura de información de los dispositivos de almacenamiento extraíble institucional y personal. Es importante de que el alcance sea definido para todos los tipos de medios extraíbles que hoy existen en la industria.

Es necesario además que se incluya la habilitación de registros para la evaluación de los elementos sensibles.

Se debe definir un proceso formal que establezca los lineamientos para la transferencia de información en medios removibles, el tipo de información que se puede contener en los mismos, la cantidad de tiempo, el procedimiento de eliminación segura, el tipo de información de acuerdo con la clasificación de la

misma, el tipo de dispositivo que es permitido y los dispositivos que son personales. Adicionalmente es importante aplicar el control de cifrado de dispositivos para el transporte de información, para salvaguardar su protección contra el acceso no autorizado.

Requisitos ISO 27001:2013 - Cláusula A.9 Control de acceso
Resumen
Conclusiones y recomendaciones

Se recomienda ajustar proceso para que que defina los lineamientos en el control de acceso físico y lógico. Es importante definir entre algunos aspectos:

- Lineamientos sobre la revocación de los accesos en caso por ejemplo de cese de funciones, pensionados, vacaciones inmediatamente deben eliminarse o deshabilitarse todos los accesos, según corresponda.

-Lineamientos para el mantenimiento o revisión a la gestión de los accesos físicos y lógicos periódicamente.

- Definir la responsabilidad en cada jefatura para la debida comunicación en la des habilitación de accesos en los casos de personal que sale de la institución, vacaciones, incapacidades, pensionados, otros al área de soporte esto de manera inmediata.

Se recomienda definir un proceso formal que norme los lineamientos para el proceso de eliminación de accesos y privilegios en donde al menos se defina el procedimiento para la eliminación de accesos y privilegios tras la terminación de contrato, en los cambios de empleo la eliminación o ajuste de los accesos, incluyendo los accesos físico y lógico.

Adicionalmente el proceso de eliminación o ajuste tiene que efectuarse mediante la eliminación, revocación o sustitución de llaves, tarjetas de identificación.

Definir un proceso formal para la gestión de accesos y privilegios que contemple:

- El uso de identificadores únicos de usuario, la desactivación inmediata de los identificadores o usuarios que dejan la compañía, salen de vacaciones, incapacitados, otros. Asegurarse de que no

haya redundancia de usuarios por medio de la habilitación de revisiones periódicas de los usuarios.

- Definir los lineamientos para la revisión de una adecuada segregación de funciones.

A pesar de que el control de Acceso a la información de los Sistemas y Aplicaciones se gestiona de manera aceptable, no obstante actualmente no se tiene un control para la revisión y el mantenimiento de accesos a la información de los sistemas y aplicaciones por lo que se incumple con la restricción de acceso a la información, puesto que ex-funcionarios podrían estar teniendo acceso a la información. Por lo tanto se recomienda de acuerdo con controles anteriores definir un proceso formal para el mantenimiento y revisión frecuente de accesos a los sistemas y aplicaciones.

Requisitos ISO 27001:2013 - Cláusula A.10
Criptografía
Resumen
Conclusiones y recomendaciones
El resultado de la prueba no es satisfactorio. Se recomienda definir un proceso formal que gestione el uso de controles criptográficos para la protección de la información. Es indispensable que la definición del proceso para el uso de controles criptográfico contenga: - El uso de controles criptográficos, incluyendo los principios generales en que la información se debe proteger. - Sobre la base de una evaluación del riesgo, el nivel de protección requerido debe identificarse teniendo en cuenta el tipo, la fuerza y la calidad del algoritmo de cifrado requerido. - El uso de cifrado para la protección de la información transportada por los dispositivos de medios

móviles o de almacenamiento masivo por medio de las líneas de comunicación.

- El impacto del uso de la información codificada en los controles que se basan en la inspección de contenido (por ejemplo, la detección de malware).

- Robustecer la plataforma tecnológica con equipos especiales con el fin de normar este uso en toda la institución y así lograr canales de comunicación más seguros, accesos remotos, VPN y videoconferencias más seguras.

Requisitos ISO 27001:2013 - Cláusula A.11 Seguridad Física y del Entorno
Resumen
Conclusiones y recomendaciones
Perímetro de seguridad Se debe clasificar si es un funcionario o visitante. El visitante debe registrar su nombre completo, cédula, dependencia a la que visita, nombre del funcionario al que va visitar. (La seguridad física debe constatar con el funcionario indicado, la afirmación de la visita). La responsabilidad sobre la aplicación del control puede delegarse algún funcionario que permanezca en el centro de datos, o bien, al personal que se encuentra monitoreando el centro de datos. - Implementar controles de seguridad para el acceso acompañado de terceros cuando se accede a sitios críticos y no dejarlos solos. Seguridad en oficinas Se recomienda emplear un mecanismo de registro de entrada y salida del personal que se encuentra de visita en la organización. Para ello, es indispensable solicitar a los funcionarios el uso del gafete institucional cada vez que entran y salen de la Institución. Con esto se permite clasificar si es un funcionario o visitante. El visitante debe registrar con el guarda de seguridad su nombre completo,

cédula, dependencia a la que visita, nombre del funcionario al que va a visitar. (La seguridad física debe constatar con el funcionario interno indicado por el visitante, la afirmación de la veracidad de la visita).

Trabajo áreas seguras

El resultado de la prueba no es satisfactorio. Se recomienda definir controles estrictos para las áreas seguras en todas las dependencias. Se recomienda implementar lo siguiente para áreas como los centros de datos:

- Implementar y reubicar cámaras de manera que se sitúen en puntos estratégicos que enfoquen todos los equipos tanto frontal como la parte trasera.

- Utilizar en TODO momento la bitácora de registro manual para todo el personal interno y externo que ingresa al área y que contenga nombre completo, fecha, hora de ingreso, hora de salida, motivo de la visita y firma.

- Implementar controles de seguridad que restrinjan ingresar al área con dispositivos móviles, USBs, CDs, discos duros, laptops, para evitar que se extraiga información y se materialice el riesgo de fuga de información, en este caso, confidencial. Permitir únicamente para casos excepcionales y únicamente a usuarios internos autorizados.

- Implementar controles de seguridad para restringir la toma de fotografías o grabación de vídeos en el área segura bajo ninguna excepción.

- Implementar una bitácora de registro de acceso para acceder a la configuración de los equipos ubicados en el centro de datos en donde se documenten los cambios realizados a nivel lógico o físico.

- Implementar controles de seguridad para el acceso acompañado de terceros cuando se accede a sitios críticos.

Se recomienda definir un procedimiento para el establecimiento de una zona oficial de descarga y carga que permita establecer el acceso a una zona de entrega carga al personal identificado y autorizado. Además la zona de descarga y carga deberán estar diseñados de manera que los suministros pueden ser cargados y descargados sin personal de reparto que acceden a otras partes del edificio, únicamente al perímetro del área diseñada para la carga y descarga. Definir lineamientos para que el material o información entrante sea inspeccionado y examinado en busca de explosivos, productos químicos u otros materiales peligrosos, antes de que se mueva de una zona entrega y de carga.

Además incluir lineamientos para la inspección del material entrante en busca indicios de manipulación en el camino. Si se descubre tal manipulación se debe informar de inmediato al personal de seguridad.

Se recomienda la implementación y acatamiento de inmediato el elaborar planes de acción de manera que a mediano plazo logre estandarizarse las medidas de seguridad física y lógica en los equipos.

Soporte

Se recomienda establecer el diseño de un proceso formal que defina claramente los servicios de soporte y que deben obedecer a lo establecido por la organización en el cumplimiento de mantenimientos preventivos con el fin de asegurar la seguridad de la información y una definición formal de los acuerdos de servicio, así como un plan de eliminar todos los equipos y software obsoleto.

Mantenimiento equipos

Se recomienda definir un proceso formal que establezca los lineamientos para el mantenimiento de los equipos y que sea extensivo y de aplicabilidad obligatoria a todas las áreas de la institución. Es indispensable un cambio estratégico del área de Seguridad Informática, para que esta pueda delegar y pedir cuentas de todos los de servicios técnicos que conforman el núcleo del BBB, para poder estandarizar un modelo de seguridad institucional.

Retiro de activos

Se recomienda definir a nivel organizacional que todos los funcionarios a la hora de entrada y salida de la organización porten su gafete institucional. Cuando se trate de terceros es necesario contar con un registro o bitácora de acceso. Adicionalmente se debe inspeccionar si el tercero porta algún dispositivo tal y como laptop o tablet. En caso de ser afirmativo es necesario realizar el registro del activo por ingresar. En el caso de los funcionarios internos, en caso de que porten alguna laptop o tablet personal deben realizar el mismo procedimiento. Adicionalmente, si es un activo de la organización se recomienda se defina una solicitud de retiro de activo que, al menos, defina fecha salida, fecha de devolución, responsable, marca, número de activo, aprobado por, unidad organizativa, motivo, entre otros.

Seguridad en equipos

Se recomienda definir un proceso formal que norme los lineamientos por ser aplicados en los activos que salen de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de los sitios locales de la organización.

Los equipos y medios de comunicación que salen de las instalaciones no deben quedar sin vigilancia en lugares públicos.

Las instrucciones del fabricante para la protección de equipos se deben observar en todo momento, por ejemplo, protección contra la exposición a los campos electromagnéticos fuertes.

Es necesario establecer los controles para los equipos que salen del establecimiento, tales como sitios de trabajo a domicilio, teletrabajo y temporales deben ser determinados por una evaluación de riesgos y los controles adecuados aplicados según el caso, por ejemplo, armarios con cerradura, la política de escritorio limpio, controles de acceso para los ordenadores y la comunicación segura con la oficina.

Los riesgos, por ejemplo, de daño, robo o espionaje, puede variar considerablemente entre localidades y se debe tomar en cuenta para determinar los controles más adecuados para la protección de la información de la organización

Definir un procedimiento formal para la eliminación segura o reutilización de equipo, medios extraíbles o dispositivos móviles. Es importante verificar la eliminación segura para garantizar que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su eliminación o reutilización

Equipo desatendido

1. Mediante el diseño de un plan de sensibilización, crear conciencia en los usuarios sobre la necesidad de bloquear sus equipos, dispositivos o cualquier tipo de sesión en donde sea de acceso únicamente personal esto cuando dejen el equipo desatendido por más de 1 minuto en áreas comerciales y 5 minutos administrativos.

2. Aplicar a nivel de controlador de dominio el bloqueo automático de las sesiones de los equipos cuando el usuario haya dejado desatendido el equipo por más de 1 minuto en áreas comerciales y 5 minutos administrativos.

Se recomienda definir lo siguiente para escritorio y pantalla limpia:

1. Por medio del diseño de un programa de sensibilización, mostrar las debilidades de la organización y los riesgos de incumplir con este control. Una vez creada la conciencia, mediante el programa de sensibilización disponer a crear una cultura en donde se comprometa toda la organización en cumplir con la campaña de escritorio y pantalla limpia de información.

2. Revisar el cumplimiento de la política de seguridad de la información la adopción de un escritorio limpio de información y pantalla limpia de información.

3. Realizar revisiones periódicas sobre el cumplimiento de los funcionarios con la política de escritorio y pantalla limpia de información.

Requisitos ISO 27001:2013 - Cláusula A.12 Seguridad en las operaciones
Resumen
Conclusiones y recomendaciones
De acuerdo con las buenas prácticas es necesario habilitar las todas las bitácoras de los eventos del controlador de dominio. Puede tomar como referencia el documento CIS Microsoft Windows Server Benchmark_v1.0.0. Se recomienda realizar evaluaciones periódicas para verificar la instalación de programas únicamente autorizados. Realizar un barrido de los equipos y eliminar cualquier privilegio que no tenga una autorización y justificación de la autorización. Actualmente esto es considerado un riesgo alto porque se expone la seguridad institucional ante posibles riesgos de malware.

Requisitos ISO 27001:2013 - Cláusula A.13 Seguridad en las Comunicaciones
Resumen
Conclusiones y recomendaciones
Se debe definir en la política informática los lineamientos para el intercambio o transferencia de información a partir de los canales de comunicación institucionales, para proteger la información transferida sobre cualquier intercepción, copia, modificación, mal enrutamiento o destrucción de la misma y asegurar la confidencialidad de la información de acuerdo con su clasificación y la integridad y disponibilidad. Se recomienda definir dentro de la política el tipo de información que puede compartirse por este canal de comunicación, el alcance sobre el uso que se le da a la herramienta, redes sociales entre otros.

Requisitos ISO 27001:2013 - Cláusula A.14 Adquisición, Desarrollo y Mantenimiento de Sistema
Resumen
Conclusiones y recomendaciones
Se recomienda definir dentro de la metodología de Desarrollo de sistemas, en la fase de pruebas, una etapa para la realización de pruebas de seguridad y que deben competer al área de seguridad informática. El área de seguridad informática debe ser el responsable de la preparación y ejecución de las pruebas a los sistemas de información. Se recomienda definir un control de seguridad donde logren custodiarse los datos de pruebas de los sistemas de información. Se debe proteger la información de identificación personal o información confidencial que se utiliza para propósitos de prueba y todos los detalles y contenidos sensibles deben ser protegidos o incorporar una limpieza de datos exclusivos para pruebas.

Requisitos ISO 27001:2013 - Cláusula A.15 Relaciones con Proveedores
Resumen
Conclusiones y recomendaciones
Se recomienda fortalecer los controles de seguridad con el trato de terceros. Se debe exigir al tercero portar con la identificación personal de su corporación visible en el momento de entrar y salir de la institución. Se debe realizar un control sobre el registro de acceso y salida del personal tercerizado de la institución diariamente. Al término de la contratación solicitar al ente tercerizado la devolución de todo tipo de accesos, información al responsable de la institución. Asegurar el borrado de información segura de los equipos de terceros. Para evitar la fuga de información en el trato de terceros, se recomienda habilitar alguna herramienta o sitio que permita al tercero acceder a la información para visualizarla únicamente y en donde no tenga permitido la copia, almacenamiento, modificación de información confidencial.

Requisitos ISO 27001:2013 - Cláusula A.16 Gestión de incidentes
Resumen
Conclusiones y recomendaciones
Al no existir un procedimiento formal para el majeo de los incidentes de seguridad se acogen a el manejo de incidentes normales recibiendo el mismo tratamiento que estos en temas de sla y slo. Se debe incluir el proceso de análisis causa raíz en los incidentes y documentarlos, utilizar una base de conocimiento para el uso de cualquier involucrado en caso de presentarse de nuevo el incidente. Se recomienda definir un proceso formal para los incidentes del SGSI pueden utilizar los mismo definidos para el

manejo de incidentes normales.

Requisitos ISO 27001:2013 - Cláusula A.17 Aspectos de Seguridad de la Información para la Gestión de Continuidad del Negocio
Resumen
Conclusiones y recomendaciones
Se recomienda la revisión del instrumento de evaluación utilizado para las aplicaciones, con el fin de optimizar los pesos y elementos en el descrito para obtener un resultado fidedigno de la continuidad.

Requisitos ISO 27001:2013 - Cláusula A.18 Cumplimiento
Resumen
Conclusiones y recomendaciones
Se recomienda definir un proceso formal que defina los lineamientos para los Derechos de Propiedad Intelectual en donde se asegure el cumplimiento legal, regulatorio y contractual de los requerimientos de Derechos de Propiedad Intelectual, uso de productos de software. Es necesario, además, definir los lineamientos para el cumplimiento de los derechos de propiedad intelectual que define el uso legal de software y productos de información. Entre otros lineamientos necesarios se recomienda definir: Los lineamientos para los contratos con los distribuidores de software para identificar la legalidad y el complimiento de los derechos de autor.

La definición de los controles y registros de activos que logren identificar los activos con requisitos de protección de derechos de propiedad intelectual.

Definición de lineamientos para el resguardo apropiado de las condiciones de las licencias adquiridas.

Definición de lineamientos para la transferencia y eliminación de software.

Definición de lineamientos para los derechos de diseño, marcas registradas, patentes y licencias de código fuente.

Se recomienda aplicar controles más robustos para la protección de datos y privacidad de la información personal. En este punto es recomendable de acuerdo con el procedimiento de clasificación y etiquetado de la información, que información es de carácter personal y la cual debe ser custodiada con todas las medidas de seguridad por la organización.

Se recomienda definir controles para protección de la información personal, en la no divulgación ni la exposición de datos personales sin consentimiento del usuario. Se debe reforzar la cultura de seguridad de los usuarios por medio de la definición de un plan de sensibilización, además de realizar pruebas de vulnerabilidades que determinen si se está violando la privacidad de la información de los usuarios.

Se recomienda definir un proceso formal que gestione el uso de controles criptográficos para la protección de la información. Una vez definido dicho proceso se debe por medio de la normativa interna definir los lineamientos necesarios sobre las regulaciones para la gestión de los controles criptográficos.

Se debe efectuar el proceso de revisión y monitoreo sobre el desempeño de la seguridad de información que al menos se efectúe entre 1 y 2 veces al año, incorporando los lineamientos de la norma.

4.3 Plan de tratamiento de los riesgos

Se presentan a continuación los planes de tratamiento de cada riesgo identificado producto del análisis del nivel de **alineación** con la norma, para lograr mitigar la brecha de cumplimiento.

N°.	Riesgo	Causa	Acciones de mitigación
1	Confidencialidad comprometida.	1	Establecer un sistema de gestión de la seguridad de la información con todos los controles aplicables del ISO 27000, un custodio, responsable, alineación con el ISO 9000 y las necesidades institucionales.
2		1	Realizar una auditoría o evaluación a todos los sistemas para identificar las bitácoras que se tienen habilitadas. Seguidamente, deben analizarse la viabilidad de habilitar las bitácoras, según los resultados del análisis.

	Acceso no autorizado a la información contenida en las aplicaciones.	2	Configurar las alertas correctamente. Activar la bitácora AUDIT TRAIL, DBA_OBJ_AUDIT_OPTS, DBA_PRIV_AUDIT_OPTS y DBA_STMT_AUDIT_OPTS para identificar oportunamente los eventos exitosos y fallidos en el dominio Revisar mensualmente los logs.
		3	Establecer una directriz o lineamiento donde se establezcan las pautas relacionadas con los controles a implementar una vez que se presenta la finalización o cambio de puestos de los funcionarios, tales como: - Borrado/respaldo de la información de los activos que utilizaban. - Notificar a encargados de AD inmediatamente comunicación formal para remover los derechos de acceso o privilegios - Incorporar como norma el establecimiento de bitácoras activas para los sistemas.
		4	Incorporar la evaluación de mecanismos para el control de los usuarios en las auditorías y actividades de control de seguridad de información.
		5	Se deben deshabilitar los usuarios con permisos superiores como ya que ellos podrían acceder a la información no concerniente a su cargo. Así mismo, para el resto de la plataforma debe realizarse evaluaciones periódicas de la configuración de los equipos. Roles en el AD y aplicaciones debe ser revisada con una frecuencia menor y de cumplimiento obligatorio la notificación de traslado o renuncia del funcionario.

3	Disponibilidad y recuperación.	1	Definir una herramienta que informa de manera real la continuidad de las aplicaciones en los simulacros definidos para tal fin y aspectos como participación ser solo cumplimiento y no tener peso en la evaluación.
4	Acceso a la información no autorizada.	1	Revisión de los niveles de acceso y privilegios asignados en todos los sistemas y aplicaciones de la institución.
		2	Evaluar los roles que están asignados a una sola persona para generar los certificados y eliminar los que no son necesarios. Además, debe evaluarse con el área dueña del producto los roles asignados a los usuarios en todas las aplicaciones.
5	Divulgación de datos.	1	Definir una metodología de clasificación de información que considere la que se encuentra en formato físico o digital, esta metodología debe considerar los siguientes criterios:- Controles de acceso- Tratamiento a la información según su clasificación. - Etiquetado de la información.- Transporte de la información según su clasificación.- Desecho de la información.- Controles de resguardo de la información.
		2	Establecer una metodología de comunicación que permita evitar divulgaciones no autorizadas en caso de emergencia.
		3	Utilizar canales de comunicación de acuerdo con la directriz de clasificación de información y política de crisis.
		4	Realizar un borrado físico sobre los medios de almacenamiento que no van a utilizarse o desechados por obsolescencia.

		5	Incorporar la evaluación de custodios en las auditorías y actividades de control de seguridad de información.
6	Acceso no autorizado a los medios de almacenamiento, expone los datos sensibles a la divulgación.	1	Definir una metodología de clasificación de información que considere la que se encuentra en formato físico o digital, esta metodología debe considerar los siguientes criterios:- Controles de acceso- Tratamiento a la información según su clasificación. - Etiquetado de la información.- Transporte de la información según su clasificación.- Desecho de la información.- Controles de resguardo de la información. Criptografía para almacenamiento de datos. Ajustar la política de accesos a nivel de seguridad lógica y física.
7	Fallas del sistema no se detectan en momentos oportunos.	1	Realizar una auditoría/evaluación a todos los sistemas para identificar qué bitácoras tienen habilitadas y cuáles no. Habilitar las bitácoras según los resultados del análisis.
8	Incumplimiento de proveedores.	1	Incorporar las responsabilidad de seguridad de información en la evaluación de terceras partes Realizar revisiones mensuales sobre el cumplimiento de terceras partes en seguridad de información.
10	Pérdida de la integridad.	1	Realizar pruebas de integridad de datos a las bases de datos.

		2	Capacitar al personal donde se encuentran los extintores para su eventual uso en caso de un siniestro, no solo a un encargado sino a toda la oficina.
11	Interrupción de las operaciones del negocio.	1	Identificar las herramientas que no poseen soporte por parte del proveedor y evaluar sustituirlas o por herramientas más nuevas.
		2	Incorporar como requisitos a los proveedores de servicios críticos esquemas de continuidad de operaciones y ajustarlos en los sla.
		3	Indicar a TI las prioridades de los requerimientos para la atención oportuna, alineados los procesos críticos de la institución con los acuerdos de servicio establecidos y documentados. Establecer sla más acordes las necesidades del negocio y evaluar si TI puede cumplir con la demanda solicitada.
		4	Hacer que los controles de seguridad sean cumplidos aun cuando solo es una visita o un visitante frecuente a los centros de datos para salvaguardar los equipos de intrusos o mala manipulación.
		1	Establecer procedimientos de documentación de procesos con los lineamientos respectivos institucionales y de buenas prácticas alineados con los contenidos necesarios para su ejecución. Hacer una revisión continua de la documentación y retiro de la vigente. Junto con el catálogo de servicios se debe documentar cada procedimiento y dar la capacitación necesaria para su acatamiento.

13	Procesos inadecuados.	2	Establecer los procedimientos de solicitud de servicios bajo un parámetro de prestación de servicios de buenas prácticas, en los procesos de mesa de ayuda, incidentes, cambios, problemas, base de conocimiento y control de cambios. Con sla acorde a la institución y no solo a la capacidad del servicio.
		3	Implantar planes de comunicación efectiva de los procedimientos a los funcionarios y funcionarias de la importancia de la seguridad de la información así como el acatamiento de buenas prácticas.
		4	Creación de un contrato con estipulaciones de seguridad según recomendación de buenas prácticas y aceptación del funcionario o funcionaria.
		5	Creación de políticas de cumplimiento de acatamiento regulatorio como propiedad intelectual, protección, privacidad de datos entre otras.
14	Procesos estáticos.	1	Incluir en cada procedimiento y política donde aplique el control, monitoreo, seguimiento y mejora continua.

4.4 Conclusiones

Con la conclusión de este estudio se alcanzó el objetivo general señalado el cual consistía en evaluar el Sistema Gestión de Seguridad de la Información de acuerdo con la norma ISO 27000:2013 y la normativa aplicable de la institución, para emitir un criterio a la gestión sobre el nivel de madurez y riesgos alcanzado.

A continuación se exponen las principales conclusiones resultado del análisis ejecutado por este trabajo:

- Actualmente, no existe un sistema de gestión de la seguridad de la información que esté alineado al estándar internacional ISO27001:2013, donde se lleve un control adecuado de toda la institución en materia de seguridad de la información, por lo cual el nivel de madurez del BBB en relación al cumplimiento de las cláusulas definidas en el estándar ISO 27001 se considera una madurez inicial.
- Las áreas operativas de la institución no conocen sobre las responsabilidades que tienen de la seguridad de la información, por lo cual debe reforzarse en capacitación y divulgación.
- El área de Seguridad de TI no debe ser la única encargada de la divulgación de los temas de seguridad, sino trabajar en conjunto con las otras áreas y apoyado por la Gerencia para crear un plan integral acorde a las necesidades.
- Cada área realiza un esfuerzo en la gestión adecuada de sus fuentes de información, por lo cual la forma en que se debe tratar para asegurar la confidencialidad, integridad y disponibilidad es establecida según lo estipule cada área, esto por la ausencia de lineamientos claros en la forma de gestionar la información, según su clasificación.
- No se tienen métricas definidas para los controles del BBB para evaluar su cumplimiento para asegurar la seguridad de la información.
- El control de accesos tanto lógico y físico deben ser ajustados porque podría provocar pérdida de la integridad y confidencialidad de la información, por una acción deliberada o accidental en la operación del personal.
- Los incidentes de seguridad de la información actualmente no son gestionados (identificar, escalar, atender y dar seguimiento) adecuadamente en la institución, esto, por la ausencia de un proceso definido y comunicado.
- No se tienen integrados todos los procesos de documentación con el ISO 9000 y su alienación de la documentación de procesos, calidad de los datos, seguimiento y control, así como la mejora continua.

- La planificación de la seguridad de la información debe contener los interesados de áreas circunscritas a la seguridad y volverse un asunto institucional prioritario, no delegarse a solo un área.
- El área de Seguridad, con el apoyo de la Gerencia, ha realizado esfuerzos para el cumplimiento de lo indicado en el acuerdo Sugef 1409 sin embargo se debe tomar en consideración las recomendaciones anteriormente planteadas para lograr la ejecución óptima del proceso, haciendo énfasis en las debilidades identificadas en el capítulo 3 de este trabajo.

Referencias

- IT Governance Institute®. Objetivos de Control para la Información y la Tecnología Relacionada. Cobit 5®, 2013.
- IT Governance Institute®. Cobit Control Practices. Segunda edición, 2013.
- IT Governance Institute®. IT Assurance Guide Using Cobit, 2013.
- Contraloría General de la República. Normas técnicas para la gestión y el control de las Tecnologías de Información. (N-2-2007-CO-DFOE)
- International Organization for Standardization. ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security management. EE.UU. 65
- International Organization for Standardization. (2005) ISO/IEC 27001:2013. Information technology-Security techniques-Information security management systems–Requirements. EE.UU.
- International Organization for Standardization. (2005) ISO/IEC 27002:2013. Information technology-Security techniques-Information security management systems–Requirements. EE.UU.
- IT Governance Institute, ITGI. (Cobit 5, 2013). Control Objective for Information and Related Technologies. EE.UU. CGR. (N-2-2009- CO-2009). Normas de Control Interno para el Sector Público.
- Superintendencia General de Entidades Financieras. Acuerdo Sugef 1409. San José, Costa Rica, 2009.
- Cámara de Bancos Instituciones Financieras de Costa Rica y la Academia Bancaria. Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo Sugef 1409, 2012.
- COHEN, C.; GRAFFE, D & FARACHE, J,: “Auditoría de Sistema”. UNA. Caracas, 1989
- DAVIS, G & OLSON, M.; “Sistemas de Información Gerencial”. Editorial Mc Graw Hill. México, 1987.

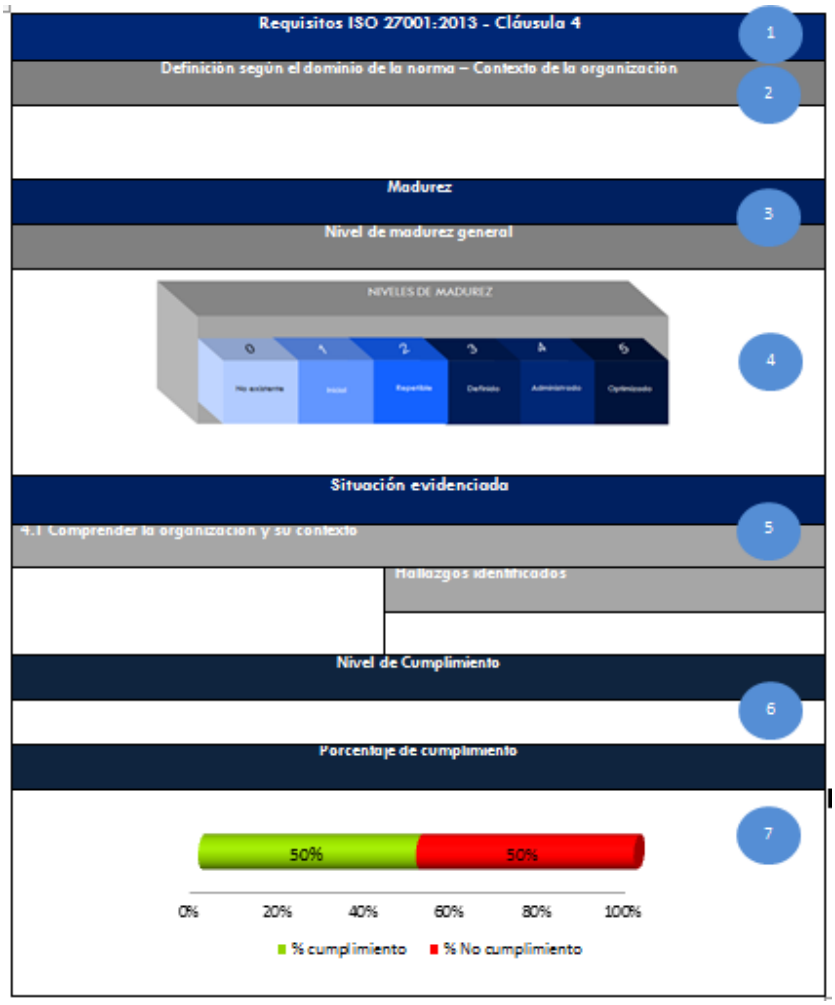
Anexo 1

Matriz ISO 27000 para la evaluación de la Norma en la Institución

Matriz ISO 27000 - BBB.xlsx

Anexo 2

Para la consolidación de los resultados producto de la aplicación de la Matriz de ISO 27000 en Capítulo 3.



Índice	Definición
1	Nombre de la cláusula de la norma.
2	Descripción de la cláusula de la norma
3	Nivel de madurez
4	Representación gráfica del nivel de madurez obtenido según Cobit, en la

	aplicación de la matriz de ISO 27000 a la institución. De autoría propia.
5	Situación evidenciada, se describe el ítem a evaluar de la cláusula junto con los hallazgos en cada una.
6	Se define una matriz de sí/no para cada ítem de la cláusula evaluada.
7	Porcentaje de cumplimiento, se define el porcentaje con base en los pesos de cumplimiento.