PLAN DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA COLOMBIANA DE INGENIERÍA CIVIL CIBJO SAS BIC

ANDREA FRANCO CORTÉS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

PLAN DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA COLOMBIANA DE INGENIERÍA CIVIL CIBJO SAS BIC

ANDREA FRANCO CORTÉS

Proyecto de Grado – Proyecto Aplicado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director
Ing. Sonia Ximena Moreno Molano

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Agosto 08 de 2024.

DEDICATORIA

Dedico este logro a mis hijos y a mis padres que me han apoyado y comprendido en cada paso de mi vida, aun cuando estuve de cuerpo presente, pero de mente ausente, robándoles tiempo valioso y acompañamiento para que yo pudiese superarme y cumplir mis objetivos.

AGRADECIMIENTOS

Agradezco a Dios por la salud, sabiduría y fortaleza que me dio, día a día para seguir adelante y cumplir con todas mis responsabilidades, especialmente con este objetivo. Agradezco a la empresa donde laboro por el apoyo educativo, respaldo y confianza total para poner en práctica el conocimiento adquirido en la organización.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ADWARE: “aplicaciones que, durante su funcionamiento, despliegan publicidad en ventanas emergentes o barras de herramientas.”[1]

ANALISIS DEL RIESGO: “proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.” [2]

ATAQUE: “explotación de una o varias vulnerabilidades, utilizando un método con el din de destruir, exponer, alterar o inhabilitar la información o el sistema de información.”[3]

CIBERATAQUE: “acción producida en el ciberespacio que compromete disponibilidad, integridad, confidencialidad de la información mediante el acceso no autorizado, modificación degradación o destrucción de los sistemas de información, telecomunicaciones o infraestructuras que la soportan.”[4]

CIBERDELITO: “actividad delictiva que emplea el ciberespacio como objetivo, herramienta o medio.”[5]

CODIGO MALICIOSO: “software capaz de realizar un proceso no autorizado sobre un sistema con el propósito de ser perjudicial.”[6]

---

[1] EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. Bogotá, 2019. p. 33.
[2] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de información. Libro I -Método. [Libro Digital] Madrid. (12 de octubre de 2012). p.9.
[3] Ibid., p. 33
[4] Ibid., p. 33
[5] Ibid., p. 33
[6] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de información. Libro I -Método. [Libro Digital] Madrid. (12 de octubre de 2012). p.33.

CONFIDENCIALIDAD: “que la información llegue solamente a las personas autorizadas.”[7]

DISPONIBILIDAD: “disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.”[8]

GESTIÓN DE VULNERABILIDADES**:** “proceso proactivo de seguridad, consiste en identificar vulnerabilidades y reducirlas antes de que sean causa de un incidente de seguridad.”[9]

GUSANO INFORMÁTICO**:** “programa que puede auto aplicarse y enviar copias de sí mismo a un ordenador a otro en una red, realiza tareas indeseables, quizás hasta colapsar el sistema anfitrión.”[10]

INTEGRIDAD: “mantenimiento de las características de completitud, contra la integridad, la información puede ser manipulada, corrupta o incompleta.”[11]

PENTESTING: “Conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas.”[12]

---

[7] Ibid., p. 9.
[8] Ibid., p. 9.
[9] EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. Bogotá, 2019. p. 33.
[10] Ibid., p. 33
[11] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de información. Libro I -Método. [Libro Digital] Madrid. (12 de octubre de 2012). p.9.
[12] INCIBE. Instituto nacional de Ciberseguridad. ¿Qué es el Pentesting?: Auditando la seguridad de tus sistemas.

PUERTA TRASERA: “tipo de software de control remoto que permite ingresar en un sistema operativo, página web o aplicación que usualmente está restringida a un usuario ajeno, evitando métodos de autenticación usuales.”[13]

RAMSOWARE**:** “código malicioso para secuestrar datos, una forma de explotación en el cual el atacante encripta los datos de la víctima y exige un pago por el descifrado. Se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos.”[14]

RIESGO**:** “estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.”[15]

TRATAMIENTO DEL RIESGO: “proceso destinado a modificar el riesgo, hay múltiples formas de tatar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, entre otras.”[16]

TRAZABILIDAD**:** “Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. Es esencial para analizar incidentes.”[17]

SEGURIDAD DE LA INFORMACIÓN**:** “la preservación de la confidencialidad, la integridad y disponibilidad de la información, abarca también la autenticidad, responsabilidad, fiabilidad y no repudio.”[18]

---

[13] EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. Bogotá, 2019. p. 33
[14] Ibid., p. 33.
[15] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de información. Libro I -Método. [Libro Digital] Madrid. (12 de octubre de 2012). p.9.
[16] Ibid., p. 10.
[17] Ibid., p. 9.
[15] EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. Bogotá, 2019. p. 33.

SPAM: “correo no deseado, procedente de un envió automatizado y masivo por parte del emisor.”[19]

SPYWARE: “software malicioso que al instalarse intercepta o toma el control parcial del computador del usuario sin su consentimiento.”[20]

TROYANO**:** “software malicioso que se presenta al usuario como un programa aparentemente legitimo e inofensivo, pero al ejecutarlo le brinda al atacante acceso remoto.”[21]

VIRUS: “segmento de código que puede copiarse para infectar programas, atacando, modificándolos, destruyendo, etc.”[22]

VULNERABILIDAD: “debilidad o falta de control que permitirá o facilitara que una amenaza actuase contra un objetivo o recurso del sistema.”[23]

[19] EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. Bogotá, 2019. p. 34.
[20] Ibid., p. 34
[21] Ibid., p. 34
[22] Ibid., p. 34
[23] Ibid., p. 34

RESUMEN

En el presente proyecto se concibe la problemática actual de vulnerabilidades y brechas de seguridad Informática de la empresa colombiana Cibjo SAS BIC, dedicada a la ingeniería civil con 45 años de experiencia y presencia en el 90 % en el territorio colombiano, experta en todo el ciclo de vida de proyectos de ingeniería civil, participa en la planeación, construcción, operación y mantenimiento de cualquier iniciativa. Certificada con las normas ISO 9001, 14001, 45001. Conformada por 430 colaboradores con la visión de crecimiento para el año 2026, de en un 50%. Mediante una auditoria al área de Tecnología de la organización con una entidad externa, basada en los criterios definidos según las mejores prácticas por cada componente de control (ISO 27001: Sistema Gestión de Seguridad de la Información), los cuales se encuentran orientados a percibir el ambiente de control de T.I. y S.I. en la organización. La evaluación se basó en la aplicación de técnica de entrevistas, y se soportó con análisis documental, sin ejecución de pruebas. Como resultado se obtuvo el diagnostico, mediante la calificación según el Modelo de Madurez de COBIT. Nivel de madurez 1: los procesos son ad-hoc, es decir, no se tiene definido un orden para la ejecución de las tareas.

Tomando como punto de partida el diagnostico actual de la organización, se reconoce la importancia de mejorar la seguridad informática en la organización. Con este proyecto se presenta un Plan de Seguridad Informática para implantar los controles requeridos, adoptando las mejores prácticas, tomando como referente la familia de la norma ISO 27001:2013 y su Anexo A: para gestionar los riesgos y que la organización alcance un nivel aceptable.

Palabras claves: Amenazas, ciberseguridad, Riesgo, Seguridad de la información, Vulnerabilidades.

ABSTRACT

In this project, the current problem of gaps and computer security vulnerabilities is a Colombian civil engineering company Cibjo SAS BIC, with 45 years of experience in civil engineering and presence in 90% in the Colombian territory, an expert in the entire life cycle of projects civil engineering, participates in the planning, construction, operation, and maintenance of any initiative. Certified with the ISO 9001, 14001, 45001 standards. Made up of 430 employees with the vision of growth by el year 2026 the 50%.

Through an audit of the organization's Technology area with an external entity, based on the criteria defined according to the best practices for each control component (ISO 27001: Information Security Management System), which are aimed at perceiving the IT control environment what if. In the organization. The evaluation was based on the application of interview techniques, and was supported by documentary analysis, without the execution of tests. As a result, the diagnosis was obtained through the qualification according to the COBIT Maturity Model.

Keywords: Cybersecurity, Information security, Risk, Threats, Vulnerabilities.

INTRODUCCIÓN

Cibjo SAS BIC, es una empresa, colombiana de ingeniería civil dedicada a prestar servicios en todo el ciclo de vida de proyectos: Planeación, construcción, operación y mantenimiento de cualquier iniciativa. Ha detectado la necesidad e importancia de implantar medidas y controles de seguridad de la información que permitan mejorar el estado actual de la organización. Cabe aclarar que el nombre de la organización y es ficticio para proteger la identidad de esta empresa. Con el fin de asegurar las características fundamentales de la información (Integridad, disponibilidad, confidencialidad). Se propone a la organización un Plan de Seguridad Informática para implantar los controles y mejores prácticas tomando como referente las normas ISO 27001:2013 y su Anexo A.

Por lo tanto, en este documento se presenta como resultado de un proceso de análisis de riesgo de los activos de la organización, los riesgos inaceptables, los controles requeridos, recomendaciones técnicas a evaluar, los proyectos a ejecutar para mitigar dichos riesgos, un análisis de la pérdida anual estimada y el retorno de la inversión para justificar los beneficios de la implementación de este plan.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

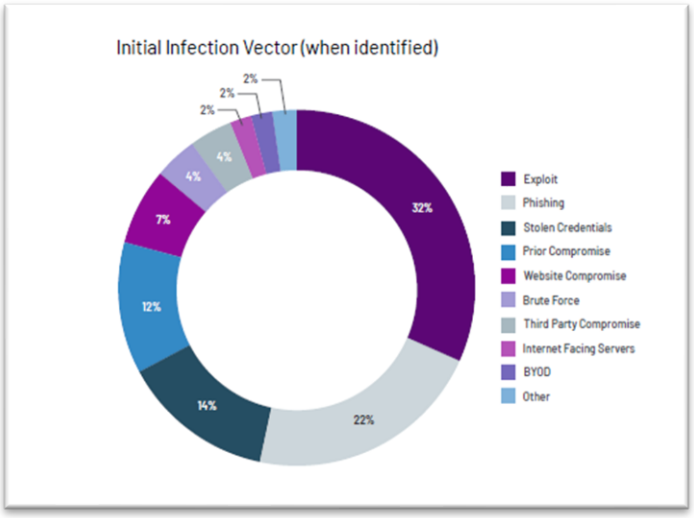
De acuerdo con un estudio realizado por el Equipo de la Policía Nacional y aliados del equipo de investigación, llamado Tendencias Cibercrimen en Colombia 2019 - 2020: El impacto que sufren las empresas colombianas luego de un ciberataque trasciende el coste económico por pérdidas de sus activos financieros y conlleva de manera colateral afectaciones a la productividad, daños reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y data sensible, ese informe presenta las cifras y modalidades de los ciberdelitos en 2019 y las tendencias que enfrentaran las empresas colombianas y los ciudadanos en 2020, publica los datos estadísticos más relevantes de la cibercriminalidad en Colombia y los métodos y técnicas identificadas en 2019. A partir del análisis de 15.948 denuncias y reportes realizados por empresas y ciudadanos al Centro Cibernético Policial Fueron analizadas 447 muestras en el laboratorio de informática forense del centro cibernético policial en donde se identificaron 33 nuevas clases de programas malignos encontrados en los enlaces, adjuntos y páginas infectadas a las que accedieron las víctimas. El delito informático más denunciado en Colombia es el hurto por medios informáticos. En segundo lugar: Violación de datos personales con 8.037 casos, robo de Identidad. El tercer delito más denunciado es el Acceso abusivo a sistema informático con 7.994 casos.[24]

Los datos expuestos anteriormente, nos demuestra con cifras la problemática de los ciberdelitos en Colombia, comprendido entre los años 2019 y 2020, analicemos a hora la tendencia para el año 2023 a nivel mundial; en un reporte especial de Mandiant, firma estadounidense de ciberseguridad y subsidiaria de Google, relata como Rusia participa en operaciones de información para su invasión a Ucrania

[24] EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. Bogotá, 2019. p. 4 – 7.

para interrumpir la infraestructura critica, el uso del espionaje, entre otros posibles ciberdelitos, Mandiant investiga y analiza los últimos ataques y amenazas para responder, mitigarlos y trasmitir esos aprendizajes a sus clientes para mantenerse a la vanguardia de la evolución constante en un panorama de amenazas. El vector de infección inicial que reportan son los exploit (herramienta para los adversarios). El phishing volvió a ser el vector más utilizado para la infección inicial para la obtención de credenciales. Detectaron también una mayor prevalencia en el uso generalizado de malware para el robo de información y compra de credenciales en comparación con años anteriores, probablemente robadas fuera del entorno de la organización y luego se utiliza contra de ella, posiblemente debido a la reutilización de contraseñas, uso de cuentas personales en los dispositivos corporativos. [25] Lo anteriormente expuesto, se puede observar reflejado, en la figura 1. Donde se puede apreciar claramente que el 32% de vectores de infección corresponde a exploit, el 22% phishing y el tercer puesto es para el robo de credenciales.

Figura 1. Tendencia de Vectores de infección de los años 2022 – 2023.



Fuente: MANDIANT. M-Trends 2023. Mandiant Special Report.

[25] MANDIANT. M-Trends 2023. Mandiant Special Report. [en línea]. 2023, p. 23.

De acuerdo con los dos anteriores reportes por expertos en ciberseguridad uno local y otro extranjero, se identifica que los ciberdelincuentes explotan las vulnerabilidades mediante vectores de ataques para el robo de información sensible, donde ya no solo basta con proteger la infraestructura física mediante, dispositivos de seguridad perimetral (seguridad física y lógica) si no se debe contemplar los usuarios finales, hasta posiblemente sus dispositivos personales donde pueden estar manipulando datos corporativos, la nube, entornos híbridos y muchos factores más que hacen del ciberespacio un lugar desconocido infinito y lleno de retos . Las organizaciones hoy en día deben prepararse para prevenir, mitigar y responder ante un ciberataque, con el objetivo de garantizar la seguridad de la información, la continuidad de su negocio y capacidad de recuperación.

1.2 FORMULACIÓN DEL PROBLEMA

Con el crecimiento acelerado de la tecnología y la necesidad de interconexión de los dispositivos, las empresas basan sus actividades en sistemas de información apoyadas en la tecnología. Según Alberto Samuel Yahai, presidente ejecutivo CCIT "El cibercrimen ha experimentado un crecimiento durante los últimos años casi de forma paralela al uso de las nuevas tecnologías y las pérdidas generadas por los ciberataques sitúan a esta problemática como una de las principales economías ilegales en el País." [26] Esto preocupa tanto a las empresas como a los usuarios debido a que son de los ataques con mayor potencial de daño económico e informático que puede producir perdidas en la fiabilidad de sus datos o información. Estas son las consecuencias negativas del desarrollo acelerado de la tecnología y el internet de las cosas.

[26] EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. Bogotá, 2019. p. 4.

En la empresa Cibjo SAS BIC, se ha detectado la dificultad en la gestión de los sistemas de información, al no tener un modelo de seguridad informática implementado, existen brechas de seguridad, vulnerabilidades expuestas que pueden ser explotadas. Surge la siguiente pregunta para dar solución al problema:

¿Cómo mejorar la gestión de la Seguridad Informática en la empresa colombiana de ingeniería civil Cibjo SAS BIC?

2. JUSTIFICACIÓN

Con la ejecución de este proyecto, se beneficia considerablemente toda la organización, permitiéndole identificar los riesgos, establecer directrices, controles, contemplando los principios básicos para la protección adecuada de la información que brinden un nivel de seguridad aceptable. De no tomarse las medidas pertinentes e inmediatas Cibjo SAS BIC, no estará preparada a nivel de infraestructura física ni lógica para responder a un incidente digital o ciberataque que puede ocurrir en cualquier memento. Es el caso de esta organización y de otras empresas colombianas que aún no gestionan apropiadamente su información, y cabe la posibilidad de convertirse en el blanco de un ataque cibernético.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Proponer un Plan de Seguridad Informática para la empresa Cibjo SAS BIC, mediante aplicación de controles y buenas prácticas de seguridad que permita reducir los riesgos y llevarlos a un nivel aceptable.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar la situación actual de la empresa Cibjo SAS BIC para adaptar el nivel de madurez deseado.
- Elaborar inventario de activos y evaluar el riesgo para su tratamiento y minimizar la exposición de este.
- Proponer plan director de Seguridad, mediante controles y proyectos alineados a la organización.
- Sustentar los proyectos propuestos a la Alta Dirección de la organización para aprobación y ejecución.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

En el mundo moderno, donde ha incrementado exponencialmente la interacción e interconectividad con dispositivos tecnológicos, así como el uso de diversas plataformas, redes sociales, entre otros, favoreciendo la productividad y el comercio, especialmente para las empresas. Según Álvarez, en el reglamento 460/2004 de la comunidad europea sobre la creación de la Agencia Europea de la seguridad de las redes y la información: Las redes y sistemas de información se han convertido en un factor esencial del desarrollo económico y social, como ha ocurrido el suministro del agua y la electricidad, por consiguiente, su disponibilidad, es un asunto que preocupa cada vez más a la sociedad, así mismo existe un riesgo al interactuar en la red más grande del mundo conocida como internet, generando potenciales amenazas. Por desgracia paralelamente el crecimiento del uso de la informática y las redes de comunicaciones, se multiplica el número de incidentes de seguridad, cuan mayor es el volumen de información procesado mayor es el riesgo derivado de su perdida. [27] Uribe, también identifica, una dificultad para responder a los incidentes de seguridad; de manera frecuente surgen nuevos tipos de incidentes relacionados con la seguridad informática. Debido a ello se ve la necesidad crear grupos con el objetivo de ayudar a mitigar los incidentes de seguridad informática y que posteriormente se preocuparon por prevenirlos son los CSIRTs. Han sido adoptados por diferentes países en el mundo como una de las opciones más viables para combatir a las organizaciones criminales. Sin embargo, se identificó que no existen muchas publicaciones acerca de cómo crear o establecer servicios en un CSIRT[28]. Por otro lado, Baca, se pregunta ¿Por qué hay personas mal intencionadas que buscan dañar, robar o destruir la información de las empresas o de los usuarios

[27] ÁLVAREZ MARAÑON, Gonzalo. Seguridad Informática para Empresas y particulares. España: 2004. p.31.
[28] URIBE RAYAS, Edgar Felipe. Proceso para la Definición de Servicios Iniciales en un equipo de Respuesta ante Incidencias de Seguridad informática (CSIRT). Zacatecas: 2014. p.2.

de un ordenador? En diversos casos se presume que solo es para demostrar que socialmente son mucho más ingeniosos y creativos que la “gente buena” que esta del otro lado de la mesa. Desde luego hay unos que lo ejecutan por dinero, por ejemplo, robar secretos tecnológicos a otras empresas para venderlos al mejor postor o competencia o extraer números de cuentas o claves bancarias para vaciar cuentas, hacer trasferencias bancarias y miles de acciones maliciosas más.[29]

De acuerdo con Gómez, en su libro de Gestión de incidentes de seguridad informática, existen diferentes tipos de ataques:

- Ataques activos: Producen cambios en la información y en la situación de los recursos del sistema.
- Ataques pasivos: Limitan a registrar el uso de los recursos y/o acceder a la información guardada o trasmitida por el sistema.
- Actividades de reconocimiento de sistemas: Persiguen obtener información previa sobre las organizaciones, redes y sistema informáticos, realizando un escaneo de puertos para determinar servicios que se encuentren activos. Los atacantes utilizarán esta información para tratar de explorar las vulnerabilidades potenciales del sistema.
- Detección de vulnerabilidades e los sistemas: Tratan de detectar y documentar las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como exploits).
- Robo de información mediante la interceptación de mensajes: Tratando de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores, vulnerando de este modo la confidencialidad y la privacidad de los usuarios.
- Modificación del contenido y secuencia de los mensajes transmitidos: Los intrusos tratan de enviar mensajes y documentos que ya habían sido enviado

[29] BACA URBINA. Gabriel. introducción a la seguridad informática. México: Patria, 2016. p. 9.

por el sistema, tras haberlos modificado de forma maliciosa (ejemplo para generar nueva transferencia bancaria) se conocen como ataques de repetición.

- Ataques de suplantación de identidad: La más conocida denominada IP Spoofing (enmascaramiento de la dirección IP), Mediante la cual el atacante consigue modificar la cabecera de los paquetes enviados para similar que proceden de un equipo distinto al que verdaderamente lo ha originado.
- Captura de cuentas de usuario y contraseñas: También es posible suplantar la identidad de los usuarios mediante herramientas que permitan capturar sus contraseñas, como programas de software espía. [30]

Lo anterior es una breve descripción y muestra de ataques, en la actualidad existe una gran cantidad de diferentes técnicas y modalidades de ataques para los cuales los especialistas, administradores de sistemas informáticos deben estar preparados y capacitarse continuamente para batallar ante esta problemática, tal cual lo relata Baca, en su libro, en La introducción a la seguridad informática: Es esencial que los futuros expertos en informática conozcan y se preparen en cómo controlar y mejorar la seguridad informática de una empresa y la propia. Se deben capacitar no sólo los riesgos físicos y lógicos a los que están expuestos todos los sistemas informáticos empresariales y computadoras personales, sino la forma en que puede disminuirse la probabilidad de ocurrencia de tales riesgos. De igual modo existen mecanismos que se han ideado para proteger de riesgos lógicos, las transacciones económicas internacionales, así como las que protecciones comunes toda empresa debe adquirir para resguardar sus datos, como los firewalls y una serie de dispositivos que pueden rastrear y detectar cualquier vulnerabilidad que tenga el sistema informático, con los cuales dicha vulnerabilidad pueda disminuirse, también realizar auditorías informáticas e informática forense.[31]

[30] GÓMEZ VIEITES. Álvaro. Gestión de incidentes de seguridad informática. RA-MA, 2016. p. 26 - 30

[31] BACA URBINA. Gabriel. introducción a la seguridad informática. México: Patria, 2016. p. 9.

Escriba, también nos relata que la mayoría de los expertos coinciden en que no existe ningún sistema totalmente seguro e infalible al 100%, se debe tratar de proteger la información y el sistema que la utiliza para ofrecer un nivel de seguridad razonable. Para que se pueda considerar razonablemente seguro se debe garantizar que se cumplen los principios básicos de la seguridad informática:

- Integridad: Es un principio básico, consiste en garantizar que la información solo pueda ser alterada por las personas autorizadas o usuarios legítimos.
    - Confidencialidad: Garantiza que la información solo es accesible e interpretada por personas o sistemas autorizados.
    - Disponibilidad: Asegurar que la información es accesible en el momento adecuado para los usuarios legítimos.[32]

Por otro lado, Gallardo y equipo de trabajo, en un contexto de riesgos y amenazas, presenta una línea de investigación que propone una estrategia de ciberseguridad no estandarizada a la fecha, basada en el conocimiento de las operaciones de inteligencia de defensa, aplicando una combinación de enfoques estáticos y dinámicos, dejando de lado el viejo concepto de defensa amurallada por uno más innovador donde los espías se infiltran en terreno desconocido o redes externas para extraer información, aprender del contexto, observar y analizar al enemigo, análisis de información, intercambiando otros recursos, compartir el conocimiento, aprendiendo con otros aliados (proveedores externos para cooperación de información y enriquecimiento) y luego poder tomar decisiones defensivas u ofensivas en tiempo real.[33]

De acuerdo con los argumentos anteriormente expuestos, se llega a la conclusión de que toda organización, independientemente de su tamaño, Core de negocio, pública o privada, debería implementar un Sistema de Gestión de Seguridad

[32] Escrivá Gasco. Gema. Seguridad informática p. 22.
[33] GALLARDO URBINI Ignacio Martin, et al. Distributed Cybersecurity Strategy, applying the Intelligence Operations Theory. CISTI (Iberian Conference on Information Systems & Technologies. [online]. (22 - 25 JUNE 2022: Madrid, Spain). p. 1 – 3.

Informática (Proceso organizado) para identificar riesgos, tratarlos adecuadamente, establecer estrategias que vaya a la vanguardia con las últimas tendencias que permitan mitigar el riesgo y que su sistema, sea razonablemente seguro.

4.2 MARCO CONTEXTUAL

De acuerdo con la información corporativa de Cibjo SAS BIC, es una empresa familiar, privada, colombiana de asesoramiento experto en todo el ciclo de vida de proyectos de infraestructura civil, con 45 años de experiencia y presencia en el 90% en el territorio colombiano, participa en la planeación, construcción, operación y mantenimiento de cualquier iniciativa. Certificada con las normas ISO 9001, 14001, 45001. Conformada por varios consorcios del mismo grupo empresarial, actualmente cuenta con 447 colaboradores y la visión para el año 2026 alcanzar los 800 e expandir su negocio internacionalmente, iniciando en Perú, Chile y Norte América. Dentro de sus clientes se encuentran entidades estatales y del sector privado (empresas constructoras, consultoras, bancas, fondos de inversión, operadores viales y puertos). [34]

4.2.1 Servicios que ofrece Cibjo SAS BIC.

A continuación, se listan los servicios ofrecidos por la organización:

- Estructuración de proyectos de ingeniería civil: Evaluación técnica, financiera y jurídica.
- Centro de Investigación e Ingeniería: Se realizan estudios y trabajos de campo.
- Diseños: Se crean soluciones de diseño, innovadoras, versátiles y sostenibles.
- Interventoría de obras civiles.
- Gerencia de Proyectos.

[34] Cibjo SAS BIC. Informe de Gestión BIC. Quienes Somos. p.7.

- Debida Diligencia: Para ingeniería de licitación y compra y venta de proyectos.
- Asesorías Técnicas Especializadas.
- Asesorías Técnica a Financiadores; Inspección y control de los recursos que se invierten para el desarrollo de los proyectos, antes del cierre financiero, durante las etapas de construcción y operación.
- Solución de Controversias y Litigios; Realización de dictámenes y conceptos técnicos para solucionar controversias y litigios, a través de peritajes, amigable componedor, tribunales de arbitramiento, entre otros, enfocados en la identificación de la causa eficiente y aporte en el diseño de estrategia jurídica.[35]

4.2.2 Estrategia corporativa. Cibjo SAS BIC. Define los siguientes cuatro pilares:

- "Asegurar el crecimiento de la organización: Aumentar el tamaño, impacto a la sociedad, a través de la motivación.
- Mantener y adaptar la cultura: Unidos en equipo, suma de fortalezas.
- Garantizar la sostenibilidad: Asegurar permanencia de la organización a través del tiempo.
- Maximizar la rentabilidad."[36]

4.2.3 Gobernanza y estructura organizacional. Cibjo SAS BIC. A través de su Gobierno Corporativo, define directrices organizacionales y construye relaciones de confianza con sus agentes relacionados. Como se puede apreciar en la figura 2. Cibjo SAS BIC, está compuesta por las diferentes direcciones y sus procesos:

[35] Ibid., p. 7.
(*) El nombre de la empresa colombiana Cibjo SAS BIC, es ficticio por confidencialidad de la información.
[36] Cibjo SAS BIC. Informe de Gestión BIC. Direccionamiento Estratégico. p.14.

- Asamblea de accionistas: Máximo órgano conformado por los accionistas de la compañía. Supervisan y velan por adecuado cumplimiento.
- Junta directiva: Amplio mandato para administrar la compañía, atribuciones para ordenar los contratos dentro del objeto social, toma de decisiones para el cumplimiento de los objetivos estratégicos.
- Gerencia: Se provee direccionamiento estratégico y representación legal trabaja con el fin de garantizar el cumplimiento de los objetivos trazados en la organización.
- Comité Directivo: Compuesto por la dirección general y los directores de cada proceso o área, encargados de la administración y gestión de su operación.
- Dirección Administrativa: Elabora modelos integrales de gestión para tomar mejores decisiones con oportunidad y eficiencia económica.
- Dirección Financiera: Planifica, organiza, analiza y genera información para la gestión eficiente de los recursos financieros de la organización.
- Dirección de Gestión Integrada e Innovación: Diseña, implementa y asegúrala mejora continua del Sistema de gestión integrado, desarrolla estrategias para la mejora continua de los procesos, gestión de la seguridad y salud en el trabajo y cuidado del medio ambiente.
- Dirección Comercial: Identifica oportunidades de negocio en los diferentes servicios y sectores.
- Dirección Jurídica: Planeación, ejecución, dirección y control de la gestión legal de la organización incluyendo la gestión de controversias y litigios.
- Dirección de Comunicaciones y Mercadeo: Diseño y ejecución de estrategias orientadas a proteger, gestionar y dirigir las comunicaciones, con el fin de fortalecer la identidad, experiencia corporativa, posición en el mercado, clientes, proveedores y colaboradores.
- Dirección Operativa: Gestiona, evalúa e implementa las acciones tendientes a generar mayor valor agregado a los proyectos desarrollados. Dirección y

control de los servicios prestados para mejorar la calidad, productividad y satisfacción de los clientes.

- Dirección del Centro de investigación e Ingeniería: Realiza estudios y trabajos de campo e integra las diferentes disciplinas de la ingeniería, entrega de resultados para la toma de decisiones.[37]

Figura 2. Estructura Organizacional Cibjo SAS BIC.

Fuente: Cibjo SAS BIC.

4.2.4 Ubicaciones físicas. Cibjo SAS BIC. Cuenta con una oficina propia en Bogotá (oficina administrativa) que soporta 24 puestos de trabajo y tres salas de juntas para un total de 50 personas en esta sede. Debido al COVID-19, en el año 2021 con el regreso paulatino a las oficinas y la necesidad de cumplir con los protocolos de bioseguridad y el aforo permitido, la oficina no soportaba la demanda de usuarios

[37] Cibjo SAS BIC. Informe de Gestión BIC. Gobernanza. p.15.
(*) El nombre de la empresa colombiana Cibjo SAS BIC, es ficticio por confidencialidad de la información.

en Bogotá, la organización opto por trabajar con modalidad alternancia y alquilar espacios de coworking con Wework, (Flexibilidad para el trabajo, contando con espacios e infraestructura tecnológica) Oficinas donde se incluyen políticas y protocolos estrictos para el control de acceso físico y lógico. (Los usuarios deben poseer una tarjeta de la membresía que es requerida desde el acceso principal y para movilizarse en las áreas comunes, para la conectividad a la red wifi se requiere correo de usuario registrado en la comunidad, si es invitado debe conectarse a una red especial, con duración limitada. A todos los usuarios de Bogotá se les asigno portátil corporativo para la movilidad en las oficinas. Los proyectos que se encuentran en ejecución a nivel nacional cuentan con oficina que en su mayoría tiene implementado cableado estructurado, wifi, equipos de escritorio y portátiles según la necesidad de movilizarse el usuario. Cabe resaltar que no se encuentra documentado la topología de la red. A continuación, se lista la ubicación de las oficinas temporales de Cibjo SAS BIC a nivel nacional:

- Transmilenio AV 68 Bogotá).
- Redes Venecia (Bogotá).
- Señalización Norte de Bogotá (Bogotá).
- Altos de Daza (Pasto)
- Troncal Magdalena (San Alberto, Cesar).
- Transversal del Sisga (Guateque).
- Bicentenario (Boyacá).
- Boyacá Red Terciaria (Boyacá).
- Antioquia Red Terciaria. (Antioquia).
- Cartagena – Palestina (Caldas).
- Administración Vial Cauca (Popayán).
- Transversal del Libertador (Popayán).
- Cartago – Calarcá (Calarcá, Quindío).
- Mocoa Fase III (Putumayo)
- San Francisco Fase III (Putumayo).

- L.T. Guaymaral.

En la figura 3. Se observa los diferentes proyectos activos que son administrados a través de las sedes principales en la ciudad de Bogotá. Alrededor de diecinueve proyectos a nivel nacional, unos contratados por entidades del estado a través de licitaciones y otros privados.

Figura 3. Proyectos en ejecución en Cibjo SAS BIC.

Fuente: Cibjo SAS BIC. Informe de Gestión BIC. p.9.

4.2.5 Telecomunicaciones. La oficina administrativa, cuenta con un cuarto de datos que contiene el sistema de control de CCTV, detectores de humo y contraincendios, una UPS de 4 KVA, un rack de telecomunicaciones en el cual aloja tres switches administrables, marca HP, Aruba, el router que provee el internet de 200 megas, Un computador que aloja la aplicación del sistema de control de acceso, carpeta en red como servidor de escáner, una multifuncional laser. En ese mismo cuarto, en un cajón se encuentran almacenados discos externos con información histórica de proyectos finalizados.

La LAN está conformada por red cableada y red wifi con tres Access point marca Ubiquiti. La organización no cuenta con diagramas de la topología de red de esta

sede, ni segmentos de red, ni tampoco una red exclusiva para visitantes. La organización no cuenta con un sistema de telefonía fijo, las comunicaciones se llevan por medio de Teams y telefonía celular (pocas líneas corporativas asignadas) a algunos colaboradores se les asigna un subsidio de telecomunicaciones para que presten su línea personal y otros simplemente, usan su línea y su teléfono personal para comunicaciones relacionadas con su cargo. Los puestos de trabajo no son personalizados, son mesas limpias y despejadas. Cada puesto cuenta con punto de datos cableado y punto de corriente doble.

4.2.6 Marco tecnológico. En los años anteriores al 2015, en los proyectos la información era alojaba en equipos de cómputo con características básicas, empleados como servidor de datos, este concentraba toda la información del proyecto, en red. Al finalizar los proyectos el director entregaba la copia final en un disco externo al área de tecnología. Estos discos de cada proyecto se fueron acumulando hasta recopilar una cantidad aproximada de 60 discos duros externos con un tamaño de información aproximada a 200 teras de información histórica. Cuando esta requiere ser consultada se conecta el disco a un equipo y se da acceso remoto al usuario que la requiere sin ningún control de que pueda modificar o alterar la información. No se cuenta con un inventario de estos discos para identificar en que disco se encuentra la información, que se requiere, para consulta se debe conectar uno a uno hasta ubicarla. Estos discos se encuentran físicamente en la oficina principal de la organización y no cuentan con un respaldo de información.

Cibjo SAS BIC, emplea para la gestión de su información en caliente, la plataforma Office 365 para toda la organización, en ella se gestiona servidor de correo, almacenamiento de información colaborativa (Proceso o Proyectos activos) en SharePoint, información individual de usuario en OneDrive, Teams como herramienta de videollamadas y mensajería instantánea, entre otros. El Proceso de Contabilidad utiliza el aplicativo Siigo, alojado en una nube privada (IaaS) (El

servicio incluye copias de seguridad, antivirus, el proveedor se encuentra certificado con las normas ISO/IEC 27001, CSA STAR, entre otras certificaciones de buenas prácticas para la gestión de seguridad de la información). Instalado en un servidor de escritorios virtuales que soporta 9 usuarios (7 contables y dos de nómina de Talento humano) y administrado por el área de TI de Cibjo. (Se comparte una unidad en red para los usuarios contables para que funcione el aplicativo). No requiere motor de bases de datos por que funciona con archivos indexados. Cabe resaltar que la jefe contable es quien administra la aplicación, crea usuarios y asigna permisos por el conocimiento y dominio del aplicativo, contable.

Talento Humano, para su gestión utiliza dos aplicaciones que se complementan, Siigo nómina y Elemental, también alojados en el servidor de escritorios remotos, administrados por la analista de nómina quien tiene el conocimiento y dominio de las aplicaciones. Los usuarios se conectan por medio de una VPN configurada en los portátiles corporativos.

El área de TI está conformada por tres personas (jefe TIC e Infraestructura, Coordinador TIC y Analista TIC) para administrar los recursos tecnológicos y atender solicitudes y requerimientos de usuarios y de la organización. El jefe TIC tiene una dedicación del 90 % para infraestructura (Locaciones, vehículos, equipos requeridos para la ejecución del proyecto en obras civiles (no relacionados con tecnología, operativos) y el otro 10 % a TIC, para gestionar temas de conectividad, telefonía móvil y solicitudes del proceso de tercer nivel. El coordinador TIC, como su nombre lo indica es encargado de gestionar para que los recursos tecnológicos estén disponibles y funcionen correctamente en toda la organización. El Analista TIC, es responsable de gestionar la mesa de ayuda, solucionar y escalar los casos de un nivel superior y con los diferentes proveedores.

En cuanto a dispositivos y equipos de cómputo, no son propios, la organización con el fin de evitar la depreciación de los activos ha decidido alquilar todos los equipos

de cómputo. El sistema operativo y algunos office están incluidos con el alquiler de la máquina. Debido a la pandemia COVID-19, se remplazaron los equipos de escritorio por portátiles. En el último año se identificó que una buena opción es incluir una licencia de office 365 estándar que incluya el acceso a office 365 y también poder instalar el paquete de office. Por presupuesto limitado en algunos proyectos se comparten equipos de cómputo cuentas de correos y de acceso a plataforma office 365.

La página web es diseñada por un tercero y administrada por el proceso de Comunicaciones, para su gestión también utilizan una suscripción de una herramienta en la web llamada Clientify. La organización cuenta con una herramienta de seguridad llamada Cloud Security Kaspersky, consola centralizada en la web que permite configurar parámetros de seguridad (Firewall, control web, control de dispositivos, vulnerabilidades de aplicaciones, Cloud Discovery, entre otros) para la plataforma office 365 y endpoint. Para el centro de Investigación e Ingeniería adquirió un software, desarrollado a la medida, que será alojado con el mismo proveedor en la nube. (En proceso de entrega). Para concluir, Cibjo SAS BIC, cuenta con muy poca infraestructura tecnológica física, la directriz de la gerencia es: no invertir en equipos físicos para permitir la flexibilidad, movilidad y evitar costos asociados a mantenimientos, adecuaciones, renovación.

5. DISEÑO METODOLÓGICO

Con el fin de dar cumplimiento al objetivo general (Proponer un Plan de Seguridad Informática para la empresa Cibjo SAS BIC) se estableció las siguiente cuatro etapas. Reflejadas gráficamente en la figura 4. Y descriptas a continuación.

5.1 ANÁLISIS Y EVALUACIÓN DEL ESTADO ACTUAL DE LA ORGANIZACIÓN

Basados en el diagnostico que ya posee la organización y conociendo el nivel de madurez actual, se analiza y se contextualiza para conocer el punto de partida de este proyecto.

5.2 ETAPA: ANÁLISIS DEL RIESGO

Incluye los siguientes pasos:

- Identificación de activos y valoración de estos.
- Evaluación del riesgo mediante metodología Magerit V3.
- Análisis de los controles ISO/IEC 27001:2013 a aplicar, de acuerdo con el análisis realizado en el paso anterior.
- Recomendaciones técnicas para el análisis de vulnerabilidades de los sistemas de información con herramientas opensource.

5.3 PLAN DIRECTOR DE SEGURIDAD INFORMÁTICA

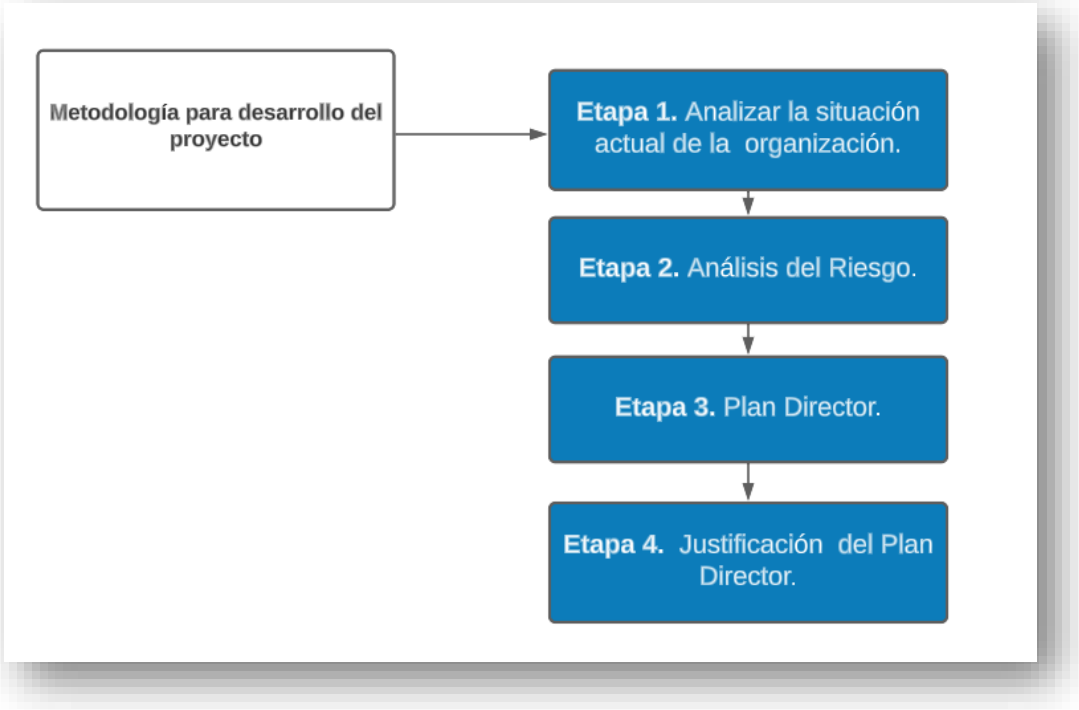
Incluye los siguientes pasos:

- Establecer la Política general de seguridad de la información.
- Priorizar y proponer proyectos de acuerdo con la evaluación y análisis del riesgo.
- Establecimiento de hoja de ruta (Proyectos, presupuesto, tiempo).

5.4 SUSTENTACION DE PROYECTOS E INICIATIVAS

Sustentar los proyectos e iniciativas propuestos a la alta dirección de la organización.

Figura 4. Metodología establecida para el proyecto:



Fuente: El autor.

6. ANALISIS DE ESTADO ACTUAL DE LA ORGANIZACIÓN

La empresa colombiana Cibjo SAS BIC, a pesar de contar con muchos años de experiencia en el mercado y tener definida su estrategia corporativa y organizacional, se detectan brechas de seguridad en la gestión de la información, mediante una auditoria al área de Tecnología, con una entidad externa, conforme a las guías de auditoria alineados con:

- Marco de control para el gobierno de TI, COBIT,
- Norma de seguridad de la información ISO 27001,
- Estándares y mejores prácticas existentes.

La evaluación se realizó basados en los criterios definidos según las mejores prácticas por cada componente de control (ISO 27001: Sistema Gestión de Seguridad de la Información), los cuales se encuentran orientados a percibir el ambiente de control de T.I. y S.I. en la organización. La calificación se aplica según el modelo de madurez de COBIT. De acuerdo con Santacruz en su trabajo de investigación, se puede definir COBIT, como una guía o modelo para realizar auditorías de la gestión y control de los sistemas de información y tecnología, orientado a los departamentos informáticos de una organización, puede ser utilizado por los usuarios y a su vez por los auditores como una lista de verificación minuciosa para los encargados de cada proceso, su utilización de forma adecuada puede generar beneficios operativos, administrativos y económicos en un corto, mediano y largo plazo. Permite identificar y demostrar a la dirección las brechas en la capacidad de mejorar y optimizar los recursos TI para de esta manera concretar los objetivos en los que debe enfocarse la organización y fijar prioridades para la mejora.[38]

[38] SANTACRUZ ESPINOSA, Julio Jhovany, et al. Sistema cobit en los procesos de auditorías de os sistemas informáticos. *Journal of science and research: Revista ciencia e investigación.* 2017, nro. 2, pp. 1- 4.

En la organización, se aplicó la técnica de entrevista al personal del área de TI y contabilidad, se soportó con análisis documental, sin ejecución de pruebas, cubriendo los siguientes componentes y sus hallazgos. En las figuras 6 y 7, se representa el nivel de madurez actual de cada componente auditado, los cuales se describen a continuación:

- Gobierno de Seguridad de la Información (SI): No se cuenta con un Modelo de Seguridad de la Información bajo los lineamientos definidos en el estándar internacional ISO 27001 vigente. El nivel de madurez para este componente de control es del 0% (Inexistente).

- Gobierno de Tecnología de la Información (TI): No se cuenta con una Medición detallada (Indicadores de Gestión) para el área de TI, actualmente se cuenta únicamente con un indicador de soporte a usuarios. No se tiene suficiente visibilidad y empoderamiento de la Gerencia de servicios y recursos TIC's. No se cuenta con un presupuesto independiente para la Gerencia de servicios y recursos TIC's que permita desarrollar las habilidades y recursos técnicos la para la gestión de TI. No se cuenta con una planeación estratégica de TI (PETI) formalmente definida, al momento de nuestra revisión el documento se encontraba en construcción. No se evidencian funciones claramente definidas sobre Seguridad Informática. Las políticas y procedimientos existentes no se encuentran formalizadas. No se cuenta con políticas de capacitación ni con la definición de un cronograma de formación para el personal del área de TI. El nivel de madurez para este componente de control es del 17% (inicial).

- Marco Regulatorio: Derechos de autor, se cuenta con una política sobre la administración de licencias de software y cumplimiento de derechos de Autor; sin embargo, esta no se encuentra aún aprobada ni divulgada. No se cuenta con procedimientos definidos de manera periódica y automatizada

para verificar el software instalado en las estaciones de trabajo. La revisión se hace cada vez que se requiere mantenimiento de un equipo. Tratamiento de datos personales, no se cuenta con un sistema de gestión para el tratamiento de datos personales (SGDP). No se encuentra actualizada la información de registro de bases de datos ante la Superintendencia de Industria y Comercio.

- Gestión de Riesgos: No se cuenta con un Sistema de Administración de Riesgos, bajo los lineamientos definidos en el estándar internacional ISO 31000:2009, u otro con este enfoque.

- Actividades de Control en TI: Acceso a Programas: No se cuenta con un procedimiento formal para la gestión de acceso a los diferentes sistemas de información de la entidad que sea transversal para la gestión tanto de usuarios internos como externos (accesos de consulta a sitios SharePoint). La gestión de acceso al aplicativo Siigo es realizada por el personal del área contable situación que podría generar conflictos debido a la ausencia de segregación de funciones y/o concentración de funciones. Esta situación implica que los controles de la aplicación tales como, apertura y cierre de períodos contables, configuraciones de variables del sistema, registro de comprobantes manuales y automáticos, configuración de cuentas y cierres contables mantienen un nivel de riesgo alto el cual no ha sido valorado ni tratado para garantizar razonablemente la integridad y exactitud de la información financiera. No están definidos procedimientos de revisión periódica de los usuarios autorizados y los permisos asignados en el aplicativo Siigo, donde se contemple otorgar autorizaciones de acceso o depuración de privilegios por parte de un área independiente, al menos cada seis (6) meses. No se cuenta con matrices de roles y perfiles para las diferentes aplicaciones de la compañía. No se identificó la existencia de un procedimiento para la custodia de las claves de usuarios administradores la plataforma tecnológica. No se han definido procedimientos de monitoreo de

actividades de usuarios con privilegios en el servidor de la aplicación contable Siigo, donde el proveedor cuenta con acceso como administrador.

- Continuidad de Operaciones: No se cuenta con un modelo propio de continuidad del negocio, bajo los lineamientos definidos en el estándar internacional ISO 23001 vigente. No se cuenta con un plan de recuperación de tecnología ante desastres (DRP) propio de la compañía. No se cuenta con un plan de contingencia de TI propio y alineado al DRP. No se cuenta con un cronograma de pruebas de restauración del sistema de información Siigo y sus componentes de infraestructura.

- Gestión de Operaciones TI: No se cuenta con un procedimiento formal para la gestión de los diferentes tipos de cambios a los sistemas de información de la entidad. No se cuenta con lineamientos claros para determinar la aprobación, categorización y prioridad de los cambios solicitados. No se cuenta con la definición de una línea base de configuración sobre los parámetros de seguridad para el servidor de Siigo y/o la infraestructura que los soporta o para otros que llegasen a ser requeridos por la entidad.

- Gestión de seguridad en redes y comunicaciones: No se cuenta con documentación, referente al monitoreo de la infraestructura de TI en asocio con los proveedores estratégicos, ni con una herramienta de monitoreo a la infraestructura de TI de manera centralizada.

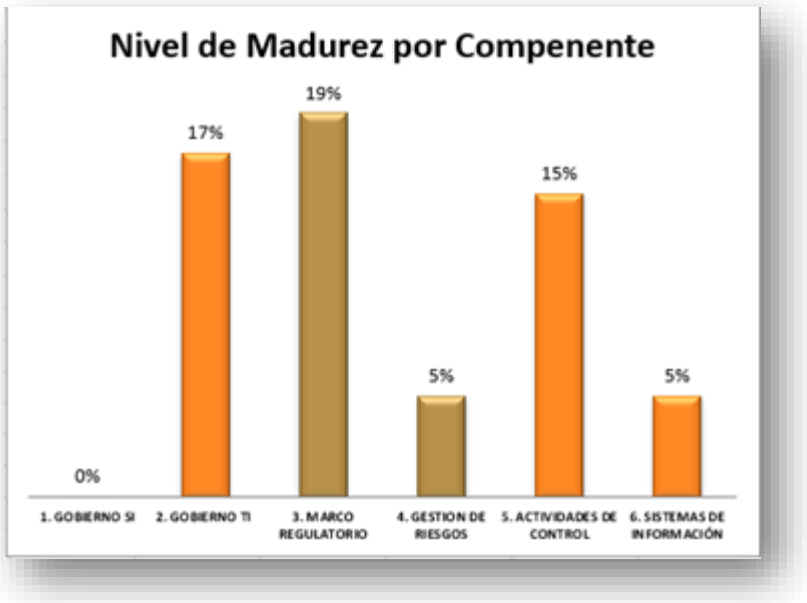
- Gestión de Proyectos: No se evidencian lineamientos y/o políticas documentadas sobre la gestión de proyectos de TI que definan, entre otros, el estándar y criterios para la clasificación de estos.

Figura 5. Porcentaje de madurez por componente de control.

Componente de Control	Madurez
1. GOBIERNO SI	0%
2. GOBIERNO TI	17%
3. MARCO REGULATORIO	19%
4. GESTION DE RIESGOS	5%
5. ACTIVIDADES DE CONTROL	15%
6. SISTEMAS DE INFORMACIÓN	5%

Fuente: Auditsi.

Figura 6. Nivel de madurez por componente auditado.



Fuente: Auditsi

A nivel general, en la figura 7. Se aprecia gráficamente el resultado de esta auditoría, se identificó el estado actual de la Seguridad Informática de la organización: Nivel de madurez 1. Los procesos son ad-hoc y desorganizados.[39] De acuerdo con el reporte anterior de la firma auditora, Cibjo SAS BIC, no tiene definido un orden para la ejecución de las tareas. La organización debe determinar el nivel de madurez que espera alcanzar para lograr la apropiada gestión de control de TI y SI en la organización. (Ver Anexo A).

Figura 7. Nivel de Madurez Cibjo SAS BIC.

Fuente: Auditsi.

6.1 MATRIZ GAP

Se analiza la brecha actual, tomando como punto de partida, el diagnóstico de la auditoria para obtener una visión aproximada del objetivo deseado que permita mejorar la seguridad de la información en la organización Cibjo SAS BIC. Como se puede apreciar en la figura 8. Matriz GAP. Efectivamente existen brechas de seguridad por encima del 60% en cada control auditado, se recomienda inicialmente a la organización, invertir en recurso humano para soportar la demanda, asignación de funciones específicas, contar con un especialista de seguridad informática que

[39] Auditsi. Firma auditora colombiana.
(*) El nombre de la firma auditora es ficticio por confidencialidad de la información.

implemente, dirija, monitoree, un sistema de gestión de seguridad de la información, así mismo contar con un presupuesto exclusivo para este proceso.

Tabla 1. Matriz GAP – Análisis situación actual Cibjo SAS BIC.

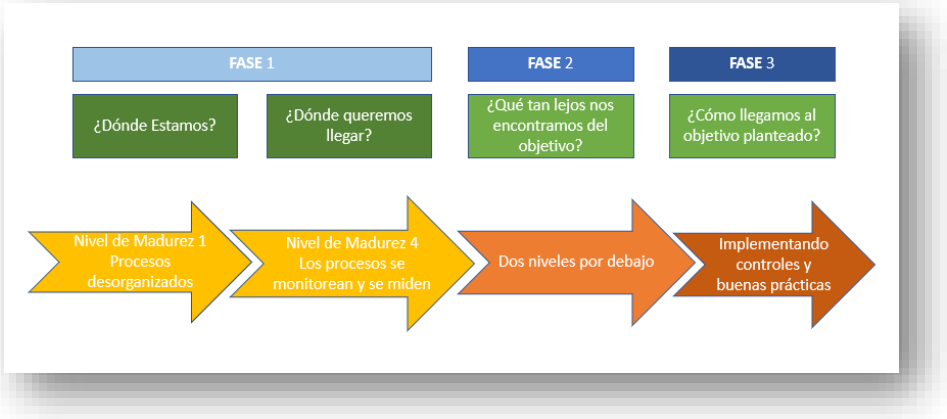
Situación Actual			Expectativas			Soluciones
Control	Resultado Obtenido	Resultado Deseado	¿Existe brecha?	¿De cuánto es la brecha?	¿Por qué existe la brecha?	Soluciones
1. Gobierno SI	0%	80%	Si	80%	La organización no cuenta con un modelo de gestión de seguridad de la información.	Implementación de un modelo de seguridad de la información, bajo lineamientos de estándares internacionales ISO 27001.
2. Gobierno TI	17%	80%	Si	63%	Solo cuenta con un indicador para medir la gestión de TIC. No tiene el suficiente empoderamiento como gerencia de servicios en la organización.	Establecer un plan estratégico que permita trazar unos objetivos medibles y a su vez establecer indicadores de gestión. Establecer políticas y funciones para TICS y seguridad informática independientes la una de la otra. De acuerdo con el plan estratégico, buscar aprobación para la asignación del presupuesto ante la alta gerencia.
3. Marco Regulatorio	19%	80%	Si	61%	No se divulgan las políticas sobre el uso de software, derechos de autor, protección de datos personales.	Establecer los lineamientos, procedimientos para la instalación y revisión del software y derechos de autor. Implementar un sistema de gestión para la protección de datos personales.
4. Gestión de Riesgos	5%	80%	Si	75%–	No cuenta con un sistema de gestión de administración de riesgos.	Implementación de sistema para la gestión de riesgos como por ejemplo Magerit V 3.0.
5. Actividades de Control	15%	80%	Si	65%	No se tienen controles en las diferentes operaciones como: Control de acceso físico y lógico. Monitoreo al comportamiento de los usuarios.	Implementar una matriz de control de acceso que permita identificar los diferentes roles y accesos que posee cada usuario. Revisar periódicamente los diferentes permisos de los usuarios para permitirles el menor privilegio posible. Etiquetado de información y asignación de directivas que permitan identificar el manejo de la información sensible o confidencial.
6. Sistemas de Información.	5%	80%	Si	75%	No se cuenta documentación de los diferentes sistemas de información de la organización.	Implementar un inventario de los sistemas de información con sus características, vigencia, responsable de ese activo. Realizar un reconocimiento, escaneo y pruebas de penetración a los diferentes sistemas de información de la organización para detectar posibles brechas o vulnerabilidades de seguridad.
7. Continuidad de Operaciones	0%	80%	Si	80%	No se tiene un plan de continuidad de negocio ni se realizan copias de seguridad a u información en caliente ni en frio.	Implementar una herramienta que permita hacer copias de seguridad para la plataforma office 365 y para la información histórica.

Situación Actual			Expectativas			Soluciones
Control	Resultado Obtenido	Resultado Deseado	¿Existe brecha?	¿De cuánto es la brecha?	¿Por qué existe la brecha?	Soluciones
8. G. Seguridad Redes y Teleco.	0%	80%	Si		No se tiene documentada la infraestructura física ni lógica.	Se requiere establecer un inventario de activos relevantes y su responsable para identificar los dispositivos activos y software así mismo detectar sus vulnerabilidades. Segmentar las redes de invitados y corporativos. Implementar un firewall. Implementar una herramienta de monitoreo de redes para analizar el tráfico de la red. Implementación de un EDR para detectar intrusiones que genere alertas y permita detener a tiempo cualquier incidencia.
9. Gestión de Proyectos.	0%	80%	Si	80%	No se cuenta con lineamientos ni políticas para la gestión de proyectos de tecnología.	establecer los lineamientos necesarios para la selección de los diferentes proyectos que contemple presupuesto, recurso humano y capacitado, asignación de roles y responsabilidades puntales que permitan sacar a flote los planes estratégicos.
10. Gestión de Operaciones	0%	80%	Si	80%	No se tienen procedimientos para cambios de sistemas de información. No se tienen lineamientos establecidos para la configuración de seguridad de los servidores de servicios críticos.	Información documentada de los procedimientos para configuraciones de los servicios críticos y para cambios de sistemas de información.

Fuente: El autor.

En la figura 8. Se analiza el punto de partida en nivel 1. Donde la gestión de tecnología de la información es un proceso desorganizado y se traza como meta, alcanzar el nivel cuatro, donde los procesos se monitoreen y se midan, queda claro que se encuentra en dos niveles por debajo del objetivo y para llegar allí, se deben concentrar los esfuerzos, estableciendo directrices, siguiendo buenas prácticas y controles para mejorar la gestión, tomando como guía, el nexo A de la norma ISO 27001.

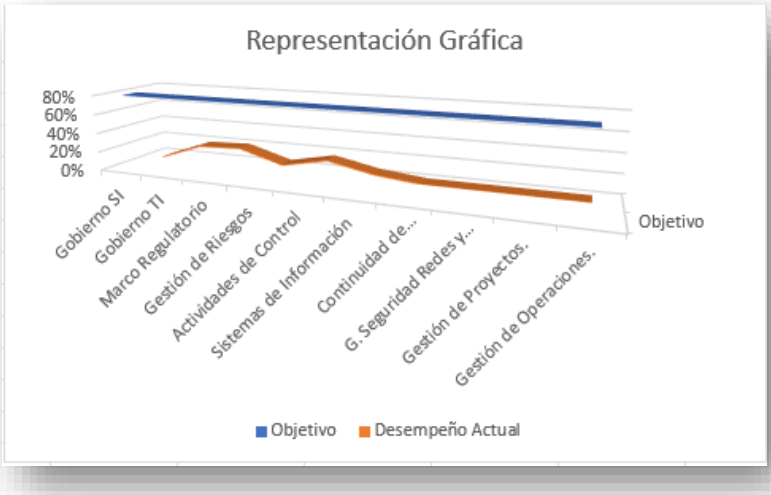
Figura 8. Matriz GAP – Análisis situación actual Cibjo SAS BIC.



Fuente: El autor.

Tomando como referente el nivel actual de la organización, en la figura 9, se puede observar gráficamente, el desempeño y la brecha que lo separa del objetivo, con porcentajes mayores al 60%. Esto indica que el camino es ancho y falta arto por recorrer.

Figura 9. Representación Gráfica el objetivo VS Estado Actual.



Fuente: El autor.

7. ANALISIS DEL RIESGO

El primer paso es identificar los activos que tiene la organización, no se puede controlar lo que no se sabe que se tiene, siendo así, se toma como punto de partida la implementación de un inventario de activos, es necesario descubrir sus vulnerabilidades para una adecuada gestión del riesgo, cada vez son más los delitos informáticos que acecha a las diferentes empresas a nivel mundial, sin dejar de lado, errores humanos, desastres naturales, entre otros que pueden afectar los activos. El objetivo es reducir el riesgo informático al que está expuesto la empresa Cibjo SAS BIC, partiendo de la identificación de activos para priorizar el esfuerzo.

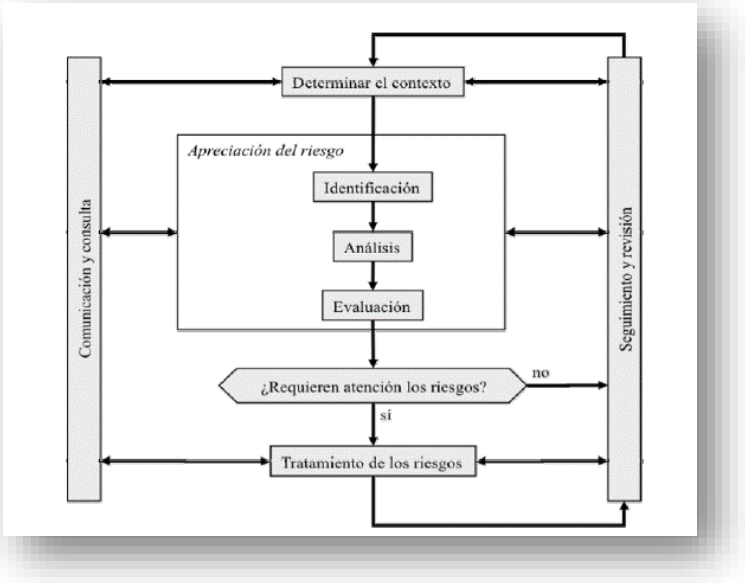
7.1 GESTIÓN DEL RIESGO

De acuerdo con la norma técnica colombiana NTC-ISO 31000, se toma como guía los pasos relacionados a continuación para la gestión del riesgo y representados en la figura 10:

- Determinación del contexto: Se determinan los parámetros y condicionales externos e internos de la organización y sus agentes implicados (Partes interesadas).
- Identificación de los riesgos: Se busca identificar vulnerabilidades de los activos de la organización.
- Análisis de los riesgos: Busca calificar, cualitativa y cuantitativamente, ordenando su importancia que permita centrarnos en lo importante.
- Evaluación de los riesgos: va más allá del análisis técnico y traduce las consecuencias de negocio. Se toman decisiones que riesgos se aceptan y cuáles no.
- Tratamiento de los riesgos: Actividades encaminadas a modificar a la situación del riesgo.

- Comunicación y consulta: Informar a partes interesadas, cuyas necesidades deben ser tenidas en cuenta, proveedores a los cuales se les debe proporcionar instrucciones claras para exigirles cumplimiento y niveles de servicio. Órganos de gobierno para establecer canales de comunicación.
- Seguimiento y revisión: Mejoramiento continuo del sistema y su entorno, evaluar los controles implementados y realizar ajustes.[40]

Figura 10. Proceso de Gestión de Riesgos.



Fuente: ICONTEC. Norma Técnica Colombiana NTC-ISO 31000. Gestión del Riesgo Principios y Directrices. p.18.

7.1.1 Metodología Magerit Versión 3.0. Teniendo en cuenta, la anterior descripción del proceso de gestión de riesgo, se emplea la metodología Magerit Versión 3.0. Para la ejecución. Permite una adecuada gestión en las organizaciones. De acuerdo con el ministerio de hacienda y administraciones publicas: Esta metodología cuenta con un marco de trabajo para que los órganos de gobierno corporativo tomen

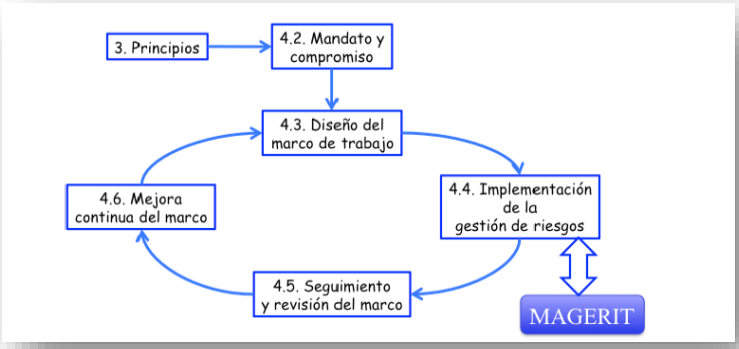
[40] ICONTEC. Norma Técnica Colombiana NTC-ISO 31000. Gestión del Riesgo Principios y Directrices. [Libro Digital] Bogotá. (22 de febrero de 2011). pp.3.

decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Magerit persigue los siguientes objetivos:

- Concientizar a los responsables de las organizaciones de la información de la existencia de riesgos y la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de las tecnologías de la información y comunicaciones.
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación.[41]

En la figura 11. Se observa cómo, la metodología Magerit se encuentra en el proceso de la implementación de la gestión de riesgos, la cual permitirá a la empresa colombiana, Cibjo SAS BIC, identificar sus activos y gestionar sus riesgos.

Figura 11. Marco de trabajo para la gestión de Riesgos – ISO 31000



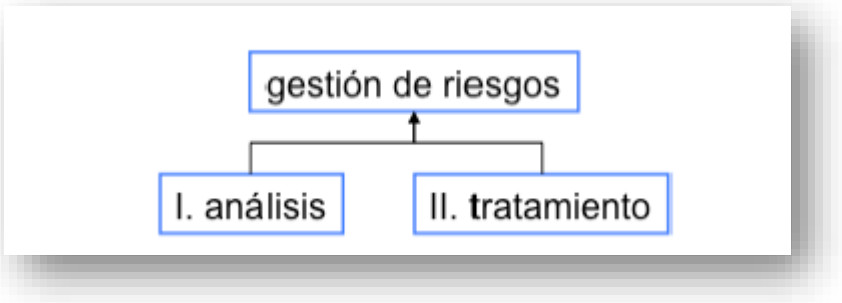
Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. p.7.

[41] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method.

De acuerdo con el Ministerio de hacienda y administraciones públicas, Magerit versión 3.0. Está conformada por las siguientes tareas, las cuales se representan en la figura 12:

- “Análisis de riesgos: Permite determinar que tiene la organización y estimar lo que podría pasar.
- Tratamiento de los riesgos: Permite organizar la defensa concienzuda y prudente y preparar para las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones, el riesgo se reduce a un nivel residual que la dirección asume y se trata el riesgo inaceptable[42]”.

Figura 12. Gestión de Riesgos.



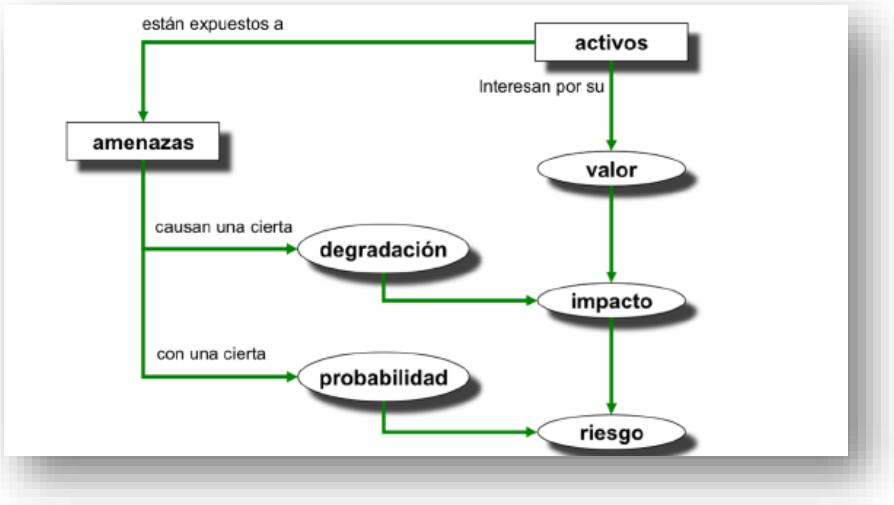
Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. p.17.

7.1.2 Matriz de análisis de riesgos. El análisis del riesgo es una aproximación metódica para determinar el riesgo, evidenciados en la figura 13. Donde se describe gráficamente los pasos mencionados a continuación:

[42] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method.

- Determinando los activos relevantes para la organización, su interrelación y su valor, en el sentido de e perjuicio (Coste) supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos
- Determinar que salvaguardas hay dispuestas y cuan eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.[43]

Figura 13. Elementos del análisis de riesgos potenciales.



Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Version 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. p.20.

[43] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. Pág. 20.

7.1.3 Activos. De acuerdo con el Ministerio de Hacienda y Administraciones Públicas “es un componente o funcionalidad de un sistema de información (En un sistema de información hay dos cosas esenciales: información y servicios que presta) susceptible a ser atacado deliberada o accidentalmente con consecuencias para la organización. Los activos esenciales y servicios dependen de otros activos, lo que genera dependencia estructural o jerárquica, de abajo hacia arriba se propaga el daño en caso de materializarse una amenaza”.[44]En la tabla 2. Se puede observar la clasificación establecida para los tipos de activos de la organización.

Tabla 2. Tipos de Activos.

ACTIVO
DATOS
CRIPTOGRAFICAS
SERVICIOS
SOFTWARE
HARDWARE
COMUNICACIONES
SOPORTE
AUXILIAR
INSTALACIONES
PERSONAL

Fuente: El autor.

7.1.4. Dimensiones. Se reconocen como dimensiones o características básicas: la confidencialidad, integridad, y disponibilidad, en esta metodología se ha añadido la autenticidad y trazabilidad. En la figura 14. Se observa, las dimensiones

[44] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. Pág. 20.

establecidas para su valoración cualitativa: clasificación de los datos, nivel de importancia y si, su estado (físico o electrónico). Estas dos últimas se refieren a:

- Autenticidad: Identificar al usuario, quien accede a los datos para escribir o consultar.
- Trazabilidad: Uso del servicio, del acceso a los datos.

Figura 14. Dimensiones.

Fuente: UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización Seguridad Informática. Administración del Riesgo. [Matriz digital].

7.1.5 Valoración. De acuerdo con el Ministerio de hacienda y administraciones públicas: se puede ver desde la perspectiva de la necesidad de proteger, cuanto más valiosos es un activo mayor nivel de protección requiere en la dimensión de seguridad, el valor suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales). El conjunto de información y servicios esenciales permite caracterizar funcionalmente una organización. Una vez determinadas las dimensiones de seguridad de un activo se procede valorarlo, es la determinación del coste que se supondría recuperarse de una incidencia que destrozara al activo. La valoración puede ser cuantitativa o cualitativa. A continuación, se relacionan algunos factores a considerar:

- Coste de reposición: Adquisición e instalación.
- Coste de mano de obra.

- Pérdida de ingresos.
- Capacidad de operar.
- Sanciones por incumplimiento.
- Daños a otros activos (propios o ajenos).
- Daño a personas.
- Daños medioambientales.[45]

7.1.6 Amenazas. De acuerdo con el Ministerio de hacienda y administraciones públicas: El siguiente paso es determinar las amenazas (causa potencial de un incidente que puede generar daños en un sistema de información o a una organización) que pueden afectar a un activo, como observa en tabla 3. Se relacionan los tipos de amenaza en sus diferentes dimensiones: Origen natural: Como terremotos, inundaciones, entre otros, se debe contemplar ¿qué puede suceder? Interpretando con un ejemplo, con los datos expuestos en la tabla 3, una amenaza natural, como el fuego puede afectar los activos como hardware, locaciones afectando la disponibilidad de estos. A continuación, se describen brevemente otras amenazas.

- Origen industrial: Contaminación, fallos eléctricos, entre otros.
- Defectos de las aplicaciones: problemas nativos por defectos en su diseño o implementación con consecuencias negativas sobre el sistema, se denominan vulnerabilidades técnicas.
- Causadas por personas de forma accidental: Las personas pueden ser causa de problemas no intencionados por error u omisión.
- Causadas por personas de forma deliberada: Personas con acceso al sistema pueden causar problemas intencionados, ataques deliberados, con el ánimo de beneficiarse o de causar daños y perjuicios.[46]

[45] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. Pag. 21.

[46] Ibid., p. 22.

Tabla 3. Tipos de amenazas con sus respectivas dimensiones

TIPO AMENAZA	AMENAZA	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	D1	D2	D3	D4	D5
[N] Desastres naturales	[N1] Fuego	HW	MEDIA	AUX	L							DISPONIBILIDAD				
[N] Desastres naturales	[N2] Daños por agua	HW	MEDIA	AUX	L							DISPONIBILIDAD				
[N] Desastres naturales	[N*] Desastres naturales	HW	MEDIA	AUX	L							DISPONIBILIDAD				
[I] De origen industrial	[I1] Fuego	HW	MEDIA	AUX	L							DISPONIBILIDAD				
[I] De origen industrial	[I2] Daños por agua	HW	MEDIA	AUX	L							DISPONIBILIDAD				
[I] De origen industrial	[I*] Desastres industriales	HW	MEDIA	AUX	L							DISPONIBILIDAD				
[I] De origen industrial	[I3] Contaminación mecánica	HW	MEDIA	AUX								DISPONIBILIDAD				
[I] De origen industrial	[I4] Contaminación electromagnética	HW	MEDIA	AUX								DISPONIBILIDAD				
[I] De origen industrial	[I5] Avería de origen físico o lógico	HW	MEDIA	AUX		SW						DISPONIBILIDAD				
[I] De origen industrial	[I6] Corte del suministro eléctrico	HW	MEDIA	AUX								DISPONIBILIDAD				
[I] De origen industrial	[I7] Condiciones inadecuadas de temperatura o humedad	HW	MEDIA	AUX								DISPONIBILIDAD				
[I] De origen industrial	[I8] Fallo de servicios de comunicaciones						COM					DISPONIBILIDAD				
[I] De origen industrial	[I9] Interrupción de otros servicios y suministros esenciales			AUX								DISPONIBILIDAD				
[I] De origen industrial	[I10] Degradación de los soportes de almacenamiento de la información		MEDIA									DISPONIBILIDAD				
[I] De origen industrial	[I11] Emanaciones electromagnéticas	HW	MEDIA	AUX	L								CONFIDENCIALIDAD			
[E] Errores y fallos no intencionados	[E1] Errores de los usuarios		MEDIA			SW		D	KEY	S		DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		
[E] Errores y fallos no intencionados	[E2] Errores del administrador	HW	MEDIA			SW	COM	D	KEY	S		DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		
[E] Errores y fallos no intencionados	[E3] Errores de monitorización (log)							D						INTEGRIDAD	TRAZABILIDAD	
[E] Errores y fallos no intencionados	[E4] Errores de configuración							D						INTEGRIDAD		
[E] Errores y fallos no intencionados	[E7] Deficiencias en la organización										P	DISPONIBILIDAD				
[E] Errores y fallos no intencionados	[E8] Difusión de software dañino					SW						DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		
[E] Errores y fallos no intencionados	[E9] Errores de [re-]encaminamiento					SW	COM			S			CONFIDENCIALIDAD			
[E] Errores y fallos no intencionados	[E10] Errores de secuencia					SW	COM			S				INTEGRIDAD		
[E] Errores y fallos no intencionados	[E14] Escapes de información												CONFIDENCIALIDAD			
[E] Errores y fallos no intencionados	[E15] Alteración accidental de la información		MEDIA		L	SW	COM	D	KEY	S				INTEGRIDAD		
[E] Errores y fallos no intencionados	[E18] Destrucción de información		MEDIA		L	SW	COM	D	KEY	S		DISPONIBILIDAD				
[E] Errores y fallos no intencionados	[E19] Fugas de información		MEDIA		L	SW	COM	D	KEY	S	P		CONFIDENCIALIDAD			
[E] Errores y fallos no intencionados	[E20] Vulnerabilidades de los programas (software)					SW						DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		

TIPO AMENAZA	AMENAZA	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	D1	D2	D3	D4	D5
[E] Errores y fallos no intencionados	[E21] Errores de mantenimiento / actualización de programas (software)					SW						DISPONIBILIDAD		INTEGRIDAD		
[E] Errores y fallos no intencionados	[E23] Errores de mantenimiento / actualización de equipos (hardware)	HW	MEDIA	AUX								DISPONIBILIDAD				
[E] Errores y fallos no intencionados	[E24] Caída del sistema por agotamiento de recursos	HW					COM			S		DISPONIBILIDAD				
[E] Errores y fallos no intencionados	[E25] Pérdida de equipos	HW	MEDIA	AUX								DISPONIBILIDAD	CONFIDENCIALIDAD			
[E] Errores y fallos no intencionados	[E28] Indisponibilidad del personal										P	DISPONIBILIDAD				
[A] Ataques intencionados	[A3] Manipulación de los registros de actividad (log)							D						INTEGRIDAD	TRAZABILIDAD	
[A] Ataques intencionados	[A4] Manipulación de la configuración							D					CONFIDENCIALIDAD	INTEGRIDAD		AUTENTICIDAD
[A] Ataques intencionados	[A5] Suplantación de la identidad del usuario					SW	COM	D	KEY	S			CONFIDENCIALIDAD	INTEGRIDAD		AUTENTICIDAD
[A] Ataques intencionados	[A6] Abuso de privilegios de acceso	HW				SW	COM	D	KEY	S		DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		
[A] Ataques intencionados	[A7] Uso no previsto	HW	MEDIA	AUX	L	SW	COM			S		DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		
[A] Ataques intencionados	[A8] Difusión de software dañino					SW						DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		
[A] Ataques intencionados	[A9] [Re-]encaminamiento de mensajes					SW	COM			S			CONFIDENCIALIDAD			
[A] Ataques intencionados	[A10] Alteración de secuencia					SW	COM			S				INTEGRIDAD		
[A] Ataques intencionados	[A11] Acceso no autorizado	HW	MEDIA	AUX	L	SW	COM	D	KEY	S			CONFIDENCIALIDAD	INTEGRIDAD		
[A] Ataques intencionados	[A12] Análisis de tráfico						COM						CONFIDENCIALIDAD			
[A] Ataques intencionados	[A13] Repudio							D		S				INTEGRIDAD	TRAZABILIDAD	
[A] Ataques intencionados	[A14] Interceptación de información (escucha)						COM						CONFIDENCIALIDAD			
[A] Ataques intencionados	[A15] Modificación deliberada de la información		MEDIA		L	SW	COM	D	KEY	S				INTEGRIDAD		
[A] Ataques intencionados	[A18] Destrucción de información		MEDIA		L	SW		D	KEY	S		DISPONIBILIDAD				
[A] Ataques intencionados	[A19] Divulgación de información		MEDIA		L	SW	COM	D	KEY	S			CONFIDENCIALIDAD			
[A] Ataques intencionados	[A22] Manipulación de programas					SW						DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		
[A] Ataques intencionados	[A23] Manipulación de los equipos	HW	MEDIA	AUX								DISPONIBILIDAD	CONFIDENCIALIDAD			
[A] Ataques intencionados	[A24] Denegación de servicio	HW					COM			S		DISPONIBILIDAD				
[A] Ataques intencionados	[A25] Robo	HW	MEDIA	AUX								DISPONIBILIDAD	CONFIDENCIALIDAD			
[A] Ataques intencionados	[A26] Ataque destructivo	HW	MEDIA	AUX	L							DISPONIBILIDAD				
[A] Ataques intencionados	[A27] Ocupación enemiga				L							DISPONIBILIDAD	CONFIDENCIALIDAD			
[A] Ataques intencionados	[A28] Indisponibilidad del personal										P	DISPONIBILIDAD	CONFIDENCIALIDAD			
[A] Ataques intencionados	[A29] Extorsión										P	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		
[A] Ataques intencionados	[A30] Ingeniería social (picaresca)										P	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD		

Fuente: UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización Seguridad Informática. Administración del Riesgo. [Matriz digital].

7.1.7 Valoración de las amenazas. Según el ministerio de hacienda y administraciones públicas: “una vez determinada la amenaza que puede perjudicar una activo, se debe valorar su influencia en dos sentidos. En la tabla 4. Se observa la dimensión que hace referencia al impacto o degradación y la probabilidad de ocurrencia, así como la calificación de la gestión actual para cada activo, aplicado en la empresa Cibjo SAS BIC:

- Degradación: cuan perjudicado resultaría el activo (mide el daño causado por un incidente en el supuesto que ocurriera).
- Probabilidad: Cuan probable o improbable es que se materialice la amenaza”.[47]

Tabla 4. Valoración de las amenazas

Dimensión		Probabilidad de vulneración		Calificación de Gestión	
B	Bajo	1	Muy raro	1	Control no Existente
M	Medio	2	Poco probable	2	Existe, pero no efectivo
A	Alto	3	Posible	3	Efectivo, pero no documentado
MA	Muy Alto	4	Probable	4	Efectivo y documentado
MB	Muy Bajo	5	Prácticamente seguro		

Fuente: UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización Seguridad Informática. Administración del Riesgo. [Matriz digital].

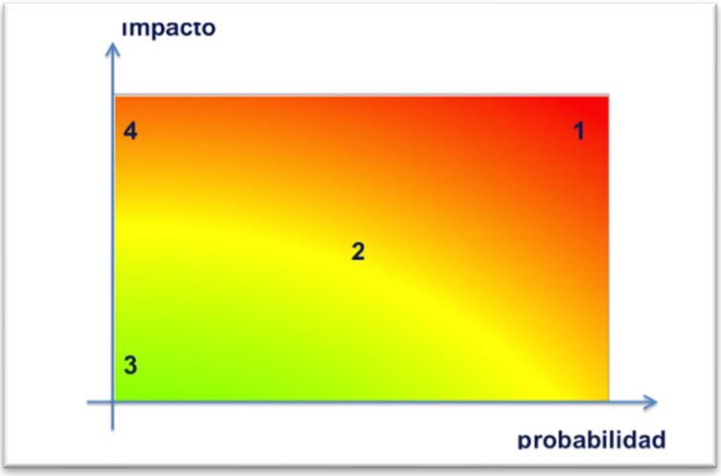
7.1.8 Determinación del riesgo. Según el ministerio de hacienda y administraciones públicas, se denomina riesgo a la medida del daño probable sobre un sistema, el

[47] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. p. 23.

riesgo crece con el impacto y con la probabilidad. En la figura 15. se pueden distinguir las siguientes zonas para tener en cuenta en el tratamiento del riesgo:

- Zona 1: riesgos muy probables y de muy alto impacto.
- Zona 2: franja amarilla, cubre un amplio rango, desde situaciones improbables y de impacto medio hasta situaciones muy probables, pero de bajo o muy bajo impacto.
- Zona 3: riesgos improbables y de bajo impacto.
- Zona 4: riesgos improbables, pero de muy alto impacto.

Figura 15. El riesgo en función del impacto y la probabilidad.



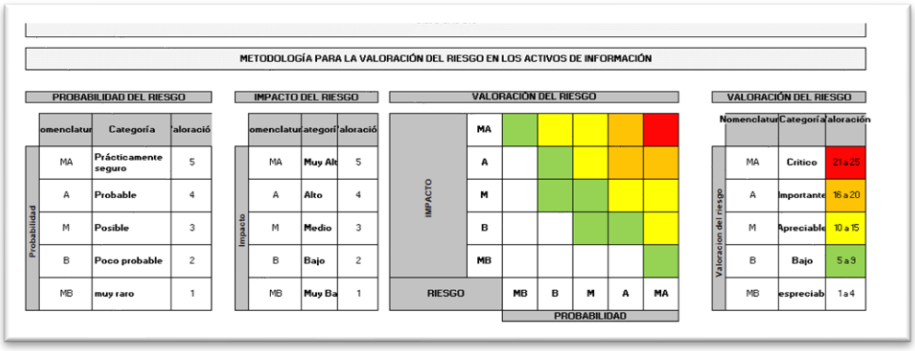
Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. p. 24.

Como se puede apreciar en la figura 16. Se aplica la metodología Magerit versión 3.0. Usando una escala de valores y colores representativos para todas las dimensiones que permite comparar los riesgos a que está expuesto el sistema, condicionadas por diversos factores, como lo menciona, el Ministerio de Hacienda y Administraciones Públicas: La gravedad del impacto, obligaciones de ley, reglamentos sectoriales, imagen pública de cara a la sociedad, relaciones con

proveedores, relaciones con clientes y usuarios, nuevas oportunidades de negocio, entre otras. La anteriores desembocan en una calificación de riesgo:

- critico
- importante
- apreciable
- bajo
- despreciable[48]

Figura 16. Metodología aplicada para la valoración del riesgo de activos.



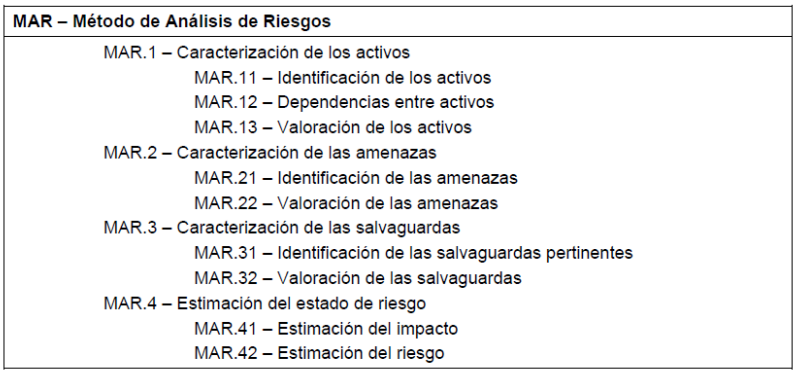
Fuente: UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización Seguridad Informática. Administración del Riesgo. [Matriz digital].

7.1.9 Formalización de actividades. Teniendo cuenta los pasos anteriores, se procede a analizar el riesgo para la empresa colombiana Cibjo SAS BIC, se lleva a cabo por medio de las siguientes tareas, relacionadas en la figura 17. De acuerdo con el Ministerio de Hacienda y Administraciones Públicas, “tienen como objetivo, levantar un modelo del valor del sistema, identificando y valorando los activos relevantes, identificando y valorando sobre estos sus amenazas, evaluar el impacto sobre el sistema, evaluar el riesgo e incluir unas salvaguardas para proteger el

[48] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. p. 22.

sistema y por último informar del riesgo con el fin de tomar decisiones de tratamiento con justificación."[49]

Figura 17. Método de análisis de riesgos.



Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. p. 36.

7.1.10 Información de Inicio. La información se recopila mediante la técnica de entrevistas, con los directores y jefes de cada proceso de la organización. Se puede observar en la tabla 5. Información relevante para dar inicio al proceso de valoración del riesgo, donde se establece el objetivo principal, su alcance, la metodología a aplicar y el riesgo a tratar, entre otra información del contexto de la organización.

[49] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. p. 28.

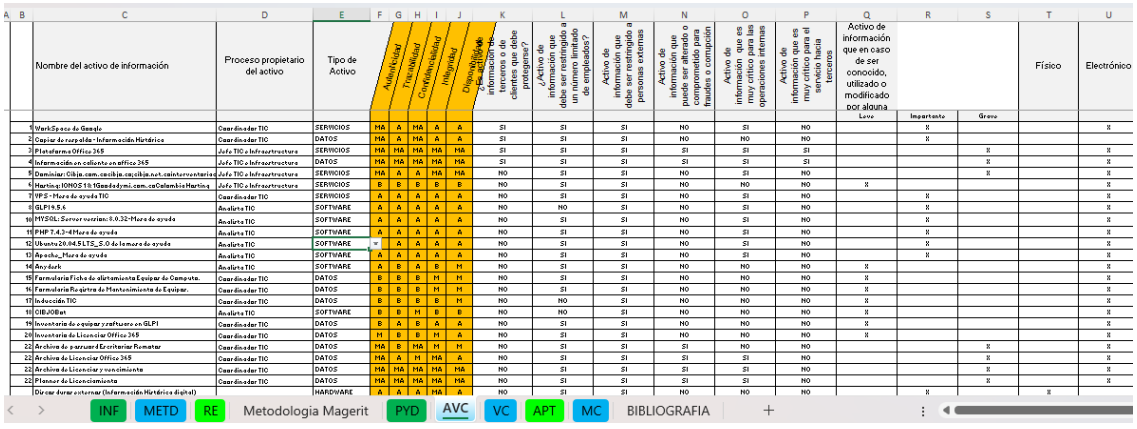
Tabla 5. Información de inicio para la valoración del riesgo

Información de Inicio	
Objetivo	Realizar la identificación, análisis y evaluación de los activos y riesgos de seguridad de la información para proponer controles y recomendaciones que permitan minimizar los riesgos de la organización, hasta un nivel aceptable.
Alcance	Aplica para los activos de la Empresa Cibjo SAS BIC y sus Consorcios.
Nombre de la Empresa:	**CIBJO SAS BIC**
Actividad Comercial	Prestación de servicios de ingeniería Civil. (Consultoría, interventoría, Estudios y diseños, elaboración de proyectos de ingeniería especializada, entre otros).
Contexto Legal	NTC ISO/IEC 27001 - NTC ISO/IEC 27005 - NTC ISO/IEC 31000
Enfoque Metodológico	El enfoque de gestión de riesgos a aplicar está basado en la metodología **MAGERIT V. 3.0**
Tratamiento	Se tratarán los riesgos cuyos niveles sean: 16 a 26 INACEPTABLE(I) Se aceptarán los riesgos cuyo resultado después de la valoración de riesgos sean: **MODERADO** Niveles de aceptación del riesgo (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I)) Una vez aplicados los controles se acepta un riesgo de residual en niveles APRECIABLE o **MPORTANTE** Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))

Fuente: El autor.

7.1.11 Caracterización de los activos. En este paso, como se puede apreciar en la figura 18. Se realiza el inventario de los activos relevantes de la organización, el proceso propietario del activo (Contabilidad, Talento Humano, TIC's, entre otros), caracterizados por tipo (software, datos, hardware, servicios, instalaciones, personal) determinando sus dimensiones de seguridad y valorando su importancia (Que tan importante es su autenticidad, trazabilidad, confidencialidad, integridad, disponibilidad) y su estado (Físico o electrónico). Loa anterior permite obtener una valoración cualitativa d ellos activos relevantes.

Figura 18. Inventario de activos y valoración cualitativa.



Fuente: El autor.

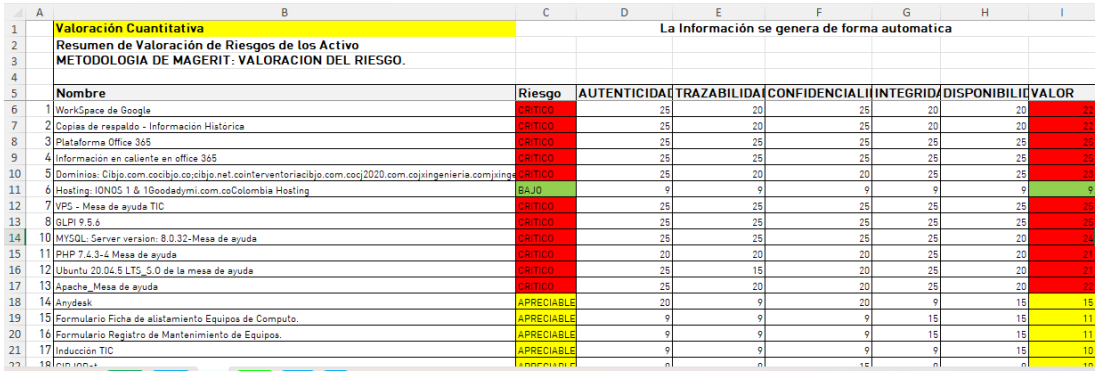
La anterior valoración establece por medio de fórmulas, un puntaje para cada dimensión (definido en la figura 20. Metodología aplicada para la valoración del riesgo de activos), lo que nos permite que identificar el nivel riesgo y obtener la valoración cuantitativa. Como puede observar, en la figura 19, se identifica visualmente, el riesgo (críticos, aceptables, bajo) esto permite centrar nuestra atención y trabajo en esos puntos críticos e inaceptables para tratar.

Algunos de los activos identificados en riesgo critico son:

- Plataforma Microsoft office 365
- Información en caliente alojada en office 365

- Servidor de Escritorios remotos (Aloja contabilidad y Talento Humano)
- Información histórica de proyectos finalizados.
- GLPI (Mesa de ayuda)
- Herramienta de contabilidad (Siigo), entre otros.

Figura 19. Inventario de activos y valoración cuantitativa.



		Valoración Cuantitativa		La Información se genera de forma automatica					
		Resumen de Valoración de Riesgos de los Activo							
		METODOLOGIA DE MAGERIT: VALORACION DEL RIESGO.							
		Nombre	Riesgo	AUTENTICIDAI	TRAZABILIDAI	CONFIDENCIALI	INTEGRIDA	DISPONIBILI	VALOR
6	1	WorkSpace de Google	CRITICO	25	20	25	20	20	22
7	2	Copias de respaldo - Información Histórica	CRITICO	25	20	25	20	20	22
8	3	Plataforma Office 365	CRITICO	25	25	25	25	25	25
9	4	Información en caliente en office 365	CRITICO	25	25	25	25	25	25
10	5	Dominios: Cibjo.com.cocibjo.co;cibjo.net.cointerventoriacibjo.com.cocj2020.com.cojxingenieria.comjxing	CRITICO	25	20	20	25	25	23
11	6	Hosting: IONOS 1 & 1Goodadymi.com.coColombia Hosting	BAJO	9	9	9	9	9	9
12	7	VPS - Mesa de ayuda TIC	CRITICO	25	25	25	25	25	25
13	8	GLPI 9.5.6	CRITICO	25	25	25	25	25	25
14	10	MYSQL: Server version: 8.0.32-Mesa de ayuda	CRITICO	25	25	25	25	20	24
15	11	PHP 7.4.3-4 Mesa de ayuda	CRITICO	20	20	20	25	20	21
16	12	Ubuntu 20.04.5 LTS_5.0 de la mesa de ayuda	CRITICO	25	15	20	25	20	21
17	13	Apache_Mesa de ayuda	CRITICO	25	20	20	25	20	22
18	14	Anydesk	APRECIABLE	20	9	20	9	15	15
19	15	Formulario Ficha de alistamiento Equipos de Computo.	APRECIABLE	9	9	9	15	15	11
20	16	Formulario Registro de Mantenimiento de Equipos.	APRECIABLE	9	9	9	15	15	11
21	17	Inducción TIC	APRECIABLE	9	9	9	9	15	10

Fuente: El autor.

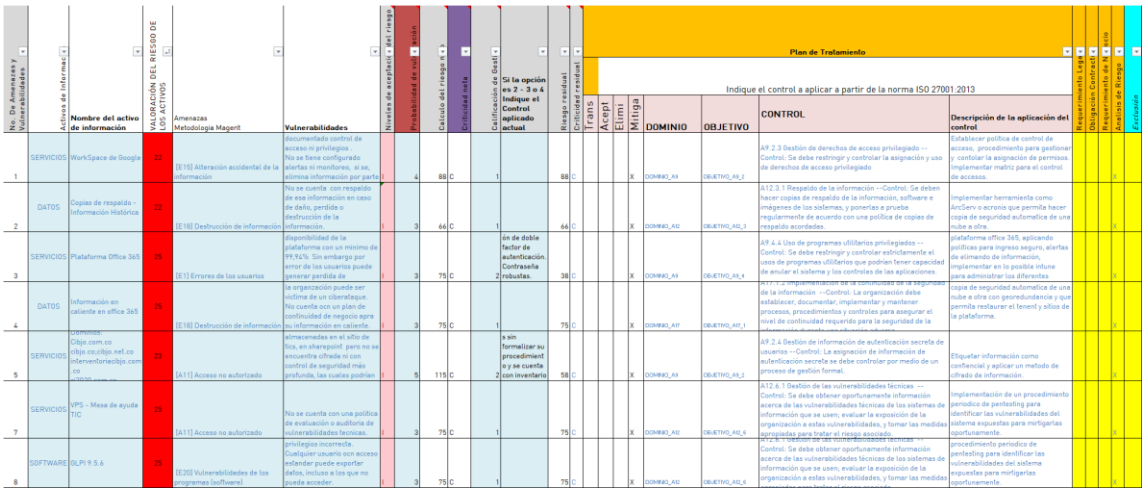
7.1.12 Caracterización de las amenazas. De acuerdo con el Ministerio de hacienda y administraciones públicas, en este paso se "identifican las amenazas relevantes y se valoran, se caracteriza el entorno al que se enfrenta el sistema ¿qué puede pasar? ¿qué consecuencias se derivan? y probabilidad de ocurrencia".[50] En la figura 20, se identifica las amenazas relevantes sobre cada activo, relacionadas con defecto de los productos o servicios, llamados vulnerabilidades que causarían degradación en los activos, a continuación, se relacionan algunas:

- [E18] Destrucción de información: CVE-2023-28288Vulnerabilidad de suplantación de identidad de Microsoft SharePoint Server.
- [E15] Alteración accidental de la información.

[50] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. P. 40.

- [E20] Vulnerabilidades de los programas (software): Vitess es un sistema de agrupación de bases de datos para el escalado horizontal de MySQL. Los usuarios pueden crear, ya sea intencionalmente o sin darse cuenta, un espacio de claves que contenga caracteres `/` de modo que, a partir de ese momento, cualquier persona que intente ver los espacios de claves desde VTAdmin recibirá un error. Intentar listar todos los espacios de teclas usando “vtctldclient GetKeyspaces” también devolverá un error. Todos los demás espacios de claves todavía se pueden administrar mediante la CLI (vtctldclient)
- [E20] Vulnerabilidades de los programas (software): Debido a que los parámetros no se filtran de manera efectiva, el atacante usa la fuente de datos MySQL y los parámetros maliciosos para configurar una nueva fuente de datos para desencadenar una vulnerabilidad de deserialización, lo que finalmente conduce a la ejecución remota de código.

Figura 20. Caracterización de amenazas.



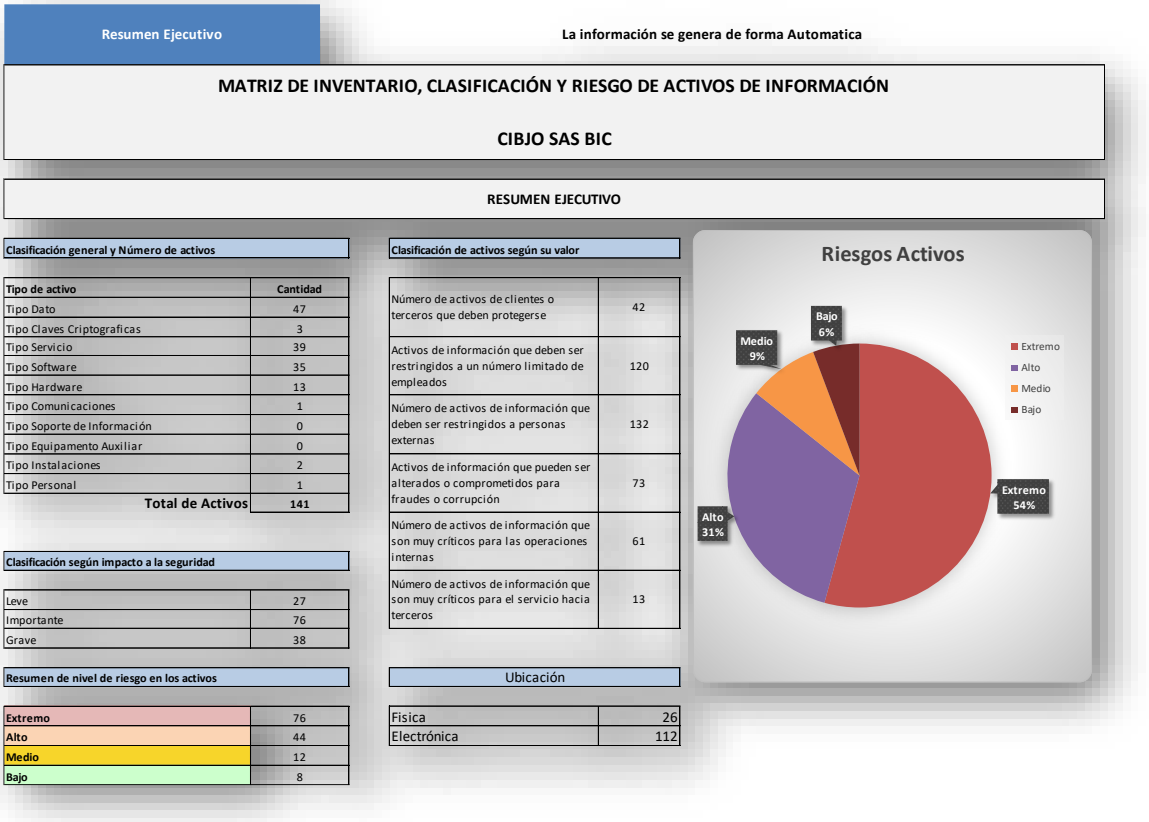
No. De Amenazas y Vulnerabilidades	Activos de Informac	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Nivelas de aceptabi. del riesgo	Probabilidad de ocu	Calculo del riesgo (R =)	Criticidad nula	Confirmación de Gestió	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual	Plan de Tratamiento										
														Trans	Acept	Elimi	Mitiga	DOMINIO	OBJETIVO	Indique el control a aplicar a partir de la norma ISO 27001:2013 CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contract	Requerimiento de N sito	Análisis de Riesgo	Estrategia
1	SERVICIOS	WorkSpace de Google	22	[E15] Alteración accidental de la información	documentado control de acceso ni privilegios . No se tiene configurado alertas ni monitoreo, si se elimina información por parte	1	4	88	C	1		88	C				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado -- Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Establecer política de control de acceso, procedimiento para gestionar y confolar la asignación de permisos. Implementar matriz para el control de accesos.				X	
2	DATOS	Copias de respaldo - Información Histórica	22	[E18] Destrucción de información	No se cuenta con respaldo de esa información en caso de daño, perdida o destrucción de la información.	1	3	66	C	1		66	C				X	DOMINIO_A12	OBJETIVO_A12_3	A12.3.1 Respaldo de la información -- Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Implementar herramienta como ArcServ o acronis que permita hacer copia de seguridad automatica de una nube a otra.				X	
3	SERVICIOS	Plataforma Office 365	25	[E1] Errores de los usuarios	disponibilidad de la plataforma con un mínimo de 99,94%. Sin embargo por error de los usuarios puede generar perdida de	1	3	75	C	2	ón de doble factor de autenticación. Contraseña robustas.	38	C				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.4 Uso de programas utilitarios privilegiados -- Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	plataforma office 365, aplicando políticas para ingreso seguro, alertas de elimando de información, implementar en lo posible intune para administrar los diferentes				X	
4	DATOS	Información en caliente en office 365	25	[E18] Destrucción de información	la organización puede ser victima de un ciberataque. No cuenta con un plan de continuidad de negocio apra su información en caliente.	1	3	75	C	1		75	C				X	DOMINIO_A17	OBJETIVO_A17_1	A17.1.2 Implementación de la continuidad de la seguridad de la información --Control: La organización debe establecer, documentar, implementar y mantener processs, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la	copia de seguridad automatica de una nube a otra con georedundancia y que permita restaurar el tenent y sitios de la plataforma.				X	
5	SERVICIOS	Dominios: Cibjo.com.co cibjo.co;cibjo.net.co intervencioriacibjo.com .co	23	[A11] Acceso no autorizado	almacenadas en el sitio de lics, en sharepoint pero no se encuentra cifrada ni con control de seguridad más profunda, las cuales podrían	1	5	115	C	2	s sin formalizar su procedimient o y se cuenta con inventario	58	C				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.4 Gestión de información de autenticación secreta de usuarios --Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Etiquetar información como confiencial y aplicar un metodo de cifrado de información.				X	
7	SERVICIOS	VPS - Mesa de ayuda TIC	25	[A11] Acceso no autorizado	No se cuenta con una política de evaluación o auditoria de vulnerabilidades tecnicas.	1	3	75	C	1		75	C				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas -- Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Implementación de un procedimiento periodico de penitesting para identificar las vulnerabilidades del sistema expuestas para mirtigarlas oportunamente.				X	
8	SOFTWARE	GLPI 9.5.6	25	[E20] Vulnerabilidades de los programas (software)	privilegios incorrecta. Cualquier usuario ocn acceso estander puede exportar datos, incluso a las que no pueda acceder.	1	3	75	C	1		75	C				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas -- Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas	procedimiento periodico de penitesting para identificar las vulnerabilidades del sistema expuestas para mirtigarlas oportunamente.				X	

Fuente: El autor.

7.2 RESUMEN EJECUTIVO DEL ANÁLISIS DEL RIESGO.

Una vez identificadas las amenazas relevantes, vulnerabilidades de los activos, frecuencia de ocurrencia, su degradación e impacto de concretarse, se obtiene como resultado un mapeo de riesgos, reflejados en la figura 21: se presentan los datos más relevantes: Clasificación general y cantidad de activos. Se identifican 141 activos, la mayoría son de tipo dato (47), le sigue servicios (39) y software (35). En la clasificación según su valor, se resalta entre otros valores: 132 activos deben ser restringidos apersonas externas de la organización, 119 deben ser restringidos a un número de empleados (Confidencialidad), 72 tiene riesgo de ser comprometidos por fraude o corrupción, 59 activos son muy críticos para las operaciones internas de la organización. Se identifica que el 79% de activos de la organización se encuentran en medio electrónico y el restante como físico. Se identifica también que el 54% de activos se encuentra en riesgo extremo y un 31% en riesgo alto, si sumamos esos dos, obtenemos un riesgo de activos del 85% de nivel inaceptable o crítico (nivel definido al inicio del ejercicio) los cuales serán tratados y se les deberá diseñar un salvaguardas, para mayor detalle de la evaluación del riesgo (Ver Anexos B y C)

Figura 21. Análisis del riesgo para Cibjo SAS BIC.



Resumen Ejecutivo

La información se genera de forma Automatica

MATRIZ DE INVENTARIO, CLASIFICACIÓN Y RIESGO DE ACTIVOS DE INFORMACIÓN

CIBJO SAS BIC

RESUMEN EJECUTIVO

Clasificación general y Número de activos

Tipo de activo	Cantidad
Tipo Dato	47
Tipo Claves Criptograficas	3
Tipo Servicio	39
Tipo Software	35
Tipo Hardware	13
Tipo Comunicaciones	1
Tipo Soporte de Información	0
Tipo Equipamento Auxiliar	0
Tipo Instalaciones	2
Tipo Personal	1
Total de Activos	**141**

Clasificación según impacto a la seguridad

Leve	27
Importante	76
Grave	38

Resumen de nivel de riesgo en los activos

Extremo	76
Alto	44
Medio	12
Bajo	8

Clasificación de activos según su valor

Número de activos de clientes o terceros que deben protegerse	42
Activos de información que deben ser restringidos a un número limitado de empleados	120
Número de activos de información que deben ser restringidos a personas externas	132
Activos de información que pueden ser alterados o comprometidos para fraudes o corrupción	73
Número de activos de información que son muy críticos para las operaciones internas	61
Número de activos de información que son muy críticos para el servicio hacia terceros	13

Ubicación

Fisica	26
Electrónica	112

Fuente: El autor.

En la siguiente tabla 6. Se evidencia se observa la valoración cualitativa, obtenida para cada una de las características de la información (confidencialidad, integridad y disponibilidad), se destaca el riesgo extremo para la información alojada en office 365 y en Google Work Space para la información histórica, así mismo datos con información sensible (Credenciales de acceso), entre otros.

Tabla 6. Resumen valoración de los activos.

Resumen de valoración de los activos					
Nombre	Riesgo	Confidencial	Integridad	Disponibilidad	Valor
WorkSpace de Google	ALTO	9	6	6	7
Copias de respaldo - Información Histórica	ALTO	9	6	6	7
Plataforma Office 365	EXTREMO	9	9	9	9
Información en caliente en office 365	EXTREMO	9	9	9	9
Dominios: Cibjo.com.co cibjo.co; cibjo.net.co interventoriacibjo.com.co cj2020.com.co jxingenieria.com jxingenieria.com.co cibjo.com.pe cibjo.pe	EXTREMO	6	9	9	8
VPS - Mesa de ayuda TIC	ALTO	6	6	6	6
GLPI 9.5.6	ALTO	6	6	6	6
MYSQL: Server versión: 8.0.32-Mesa de ayuda	ALTO	6	6	6	6
PHP 7.4.3-4 Mesa de ayuda	ALTO	6	6	6	6
Ubuntu 20.04.5 LTS_S. O de la mesa de ayuda	ALTO	6	6	6	6
Apache_Mesa de ayuda	ALTO	6	6	6	6
Archivo de password Escritorios Remotos	EXTREMO	9	9	9	9
Archivo de Licencias Office 365	EXTREMO	9	9	9	9
Archivo de Licencias y vencimiento	ALTO	5	9	6	7
Planner de Licenciamiento	EXTREMO	9	9	6	8
Discos duros externos (Información Histórica digital)	ALTO	6	9	6	7
Consola de Antivirus	ALTO	6	6	6	6
Equipos de Computo	ALTO	6	5	6	6
Sistema Operativo Windows 10 profesional	ALTO	6	6	6	6
Sistema Operativo Windows 11 profesional	ALTO	6	6	6	6
Servidor Escritorios remotos (Acceso).	EXTREMO	6	9	9	8
Windows server 2019	EXTREMO	9	9	9	9
SIIGO	EXTREMO	6	9	9	8
Elemental	ALTO	9	9	3	7
Contratos de servicios con proveedores	EXTREMO	9	9	6	8
Sistema de Control de Acceso (Biométrico)	EXTREMO	9	9	9	9
Software Control de acceso (Biométrico)	EXTREMO	9	9	6	8
Control de acceso Físico a Oficina Elemento - Tarjetas	EXTREMO	9	9	5	8
Control de acceso Físico a Oficina Elemento - Bases de datos	ALTO	9	9	3	7
Control de acceso Físico a Oficina Wework-Bases de datos.	ALTO	9	5	3	6

Resumen de valoración de los activos

Nombre	Riesgo	Confidencial	Integridad	Disponibilidad	Valor
CCTV_Físico	EXTREMO	9	9	9	9
CCTV_HIKCONECTION	EXTREMO	6	9	9	8
Internet de oficina Principal y proyectos	EXTREMO	6	9	9	8
Access Point Ubiquiti_Tres en Oficina Principal y proyectos (Redes Venecia, Libertador, Señalización norte, Transmilenio AV68, Cartago Calarcá).	ALTO	6	6	6	6
Repetidores wifi de proveedor de internet (AMV Cauca, redes Venecia, TM AV68).	ALTO	6	6	6	6
Impresoras en oficina principal y proyectos.	EXTREMO	9	9	5	8
Vigilancia Electrónica (Redes Venecia, Señalización norte, Calarcá, TM AV68, Sisga, laboratorio).	ALTO	3	6	9	6
Servidor de alojamiento (Biométrico y videoconferencia).	ALTO	6	9	6	7
Servicios Públicos: Agua, luz, teléfono y gas en Oficina Elemento y proyectos.	ALTO	3	9	9	7
Oficinas físicas Proyectos.	ALTO	9	6	5	7
Sigeslab: Software para gestión de laboratorio	ALTO	6	9	6	7
Sigeslab: Alojamiento	EXTREMO	9	9	9	9
Sigeslab: Sistema operativo Windows server estándar 2016	EXTREMO	9	9	9	9
Sigeslab: SQL Server estándar 2016	EXTREMO	9	9	9	9
Página web Transversa del Sisga	EXTREMO	9	9	6	8
Plataformas de Gmail: Cibjo.co y cibjo.com.co	EXTREMO	9	9	6	8
Vehículos	EXTREMO	9	9	6	8
Contratos (Servicios públicos, vehículos, comunicaciones (internet, telefonía móvil y fija)	EXTREMO	9	9	6	8
Formularios control operacional vehículos (4).	EXTREMO	9	9	6	8
Inventario de Topografía y laboratorio	EXTREMO	9	9	5	8
Programas de mantenimiento de (topografía, laboratorio, vehículos, oficinas).	EXTREMO	9	9	5	8
Sitio de Infraestructura de SharePoint	EXTREMO	9	9	9	9
Switchs Administrable HP (Dos).	EXTREMO	9	9	9	9
Base de datos SQL Express de Elemental	ALTO	6	9	3	6
Herramienta CompuTrabajo.	ALTO	6	6	6	6
Plataforma Colegio del Riesgo Sura	ALTO	9	6	6	7
Herramienta mi planilla	EXTREMO	9	9	9	9
Plataforma Sena	ALTO	6	6	5	6
Siigo Nomina	EXTREMO	9	9	9	9
Herramienta Biblioinstrumentos	ALTO	9	9	3	7
Bases de datos BD_GENERAL	EXTREMO	9	9	9	9
Herramienta Data Riesgos	ALTO	9	9	3	7
Sitio SharePoint_Talento Humano	EXTREMO	9	9	9	9
VPN a Servidor de Siigo Nomina.Forticlient 7.0.3	EXTREMO	9	9	9	9

Resumen de valoración de los activos

Nombre	Riesgo	Confidencial	Integridad	Disponibilidad	Valor
Software RFI	EXTREMO	9	9	5	8
Colaboradores	EXTREMO	6	9	9	8
SIIGO Contabilidad	EXTREMO	9	9	9	9
Sitio SharePoint_Información Contable	EXTREMO	9	9	9	9
Sitio SharePoint_Gestión de la información (Correspondencia Recibida)	ALTO	5	9	6	7
Plataforma Bancos (Davivienda, Banco Occidente, Bancolombia)	EXTREMO	9	9	6	8
DIAN	ALTO	6	9	6	7
Hacienda	ALTO	6	9	6	7
People pass	ALTO	6	9	5	7
Superintendencia de Sociedades	ALTO	6	9	5	7
Aportes en Línea	EXTREMO	9	9	6	8
Cámara de Comercio	ALTO	6	9	6	7
Token de Bancos	EXTREMO	9	9	6	8
Herramienta Data riesgos	EXTREMO	9	9	5	8
Clientify Enterprise	EXTREMO	9	9	5	8
Litigando.com	EXTREMO	9	9	5	8
Base de datos de Clientes	EXTREMO	9	9	6	8
Propuestas de negocios	EXTREMO	9	9	6	8
Sitio SharePoint_Información Comercial	EXTREMO	9	9	9	9
Sitio SharePoint_Información Licitaciones	EXTREMO	9	9	9	9
Herramienta mesa de ayuda GLPI_Solicitudes de comunicaciones.	EXTREMO	6	9	9	8
Página web cibjo.co	ALTO	3	9	6	6
Documentos de Sistema de Gestión Integrada	EXTREMO	9	9	6	8
Herramienta Muraby	ALTO	6	9	5	7
Sitio SharePoint_Gestión integrada e Innovación	EXTREMO	6	9	9	8
Sitio SharePoint_Intranet	ALTO	3	9	6	6
Sitio SharePoint_Proyecto Pilo	ALTO	6	9	6	7
Formulario en Survey 123 _Solicitudes de Calidad	ALTO	5	9	5	6
Sitio SharePoint_Compras	EXTREMO	9	6	9	8
Formulario en Survey 123 _Requisiciones de Compras.	EXTREMO	6	9	9	8
Tarjeta de crédito de Compras	EXTREMO	9	9	6	8
Base de datos de Proveedores	EXTREMO	9	9	6	8
Base de datos de Contratistas	EXTREMO	9	9	6	8
Caja menor	EXTREMO	9	9	6	8
Información Histórica en físico	EXTREMO	9	9	6	8

Resumen de valoración de los activos					
Nombre	Riesgo	Confidencial	Integridad	Disponibilidad	Valor
Información Histórica Digital	EXTREMO	9	9	6	8
Alojamiento información Física en Airon Montain	EXTREMO	9	9	6	8
Alojamiento información Física en Oficina (Archivo).	EXTREMO	9	9	6	8
Sitio SharePoint_Información Gestión de la Información.	EXTREMO	9	9	9	9
Sitio SharePoint_Información Jurídica.	EXTREMO	9	9	9	9
Formulario en Survey 123 _Solicitudes a proceso Jurídico	EXTREMO	9	9	6	8
Licencias de ArcGIS	EXTREMO	9	9	6	8
Licencias de Autodesk	EXTREMO	9	9	6	8
Licencia HDM4	EXTREMO	9	9	6	8
Licencia DOCS	EXTREMO	9	9	6	8
Licencia Integromat	EXTREMO	9	9	6	8
Licencia Nero	EXTREMO	9	9	6	8
Global Maper	EXTREMO	9	9	6	8
Circuito de Video en proyecto Sisga	EXTREMO	9	9	9	9
Sitio SharePoint_Información Gerencia General	EXTREMO	9	9	9	9
Sitio SharePoint_Programa Transferencia y Ética Empresarial.	EXTREMO	9	9	9	9
Firma digital Gerencia	ALTO	9	6	5	7
Firma digital director técnico	ALTO	9	6	5	7
Firma digital director Proyecto Sisga.	ALTO	9	6	5	7
Sitio SharePoint_Proyecto	EXTREMO	9	9	9	9
Sitio SharePoint_Comites (Brigadas, Comco, Copasst, Mujer, PESV, Pilo).	EXTREMO	9	9	6	8

Fuente: El autor.

7.3 CARACTERIZACIÓN DE SALVAGUARDAS

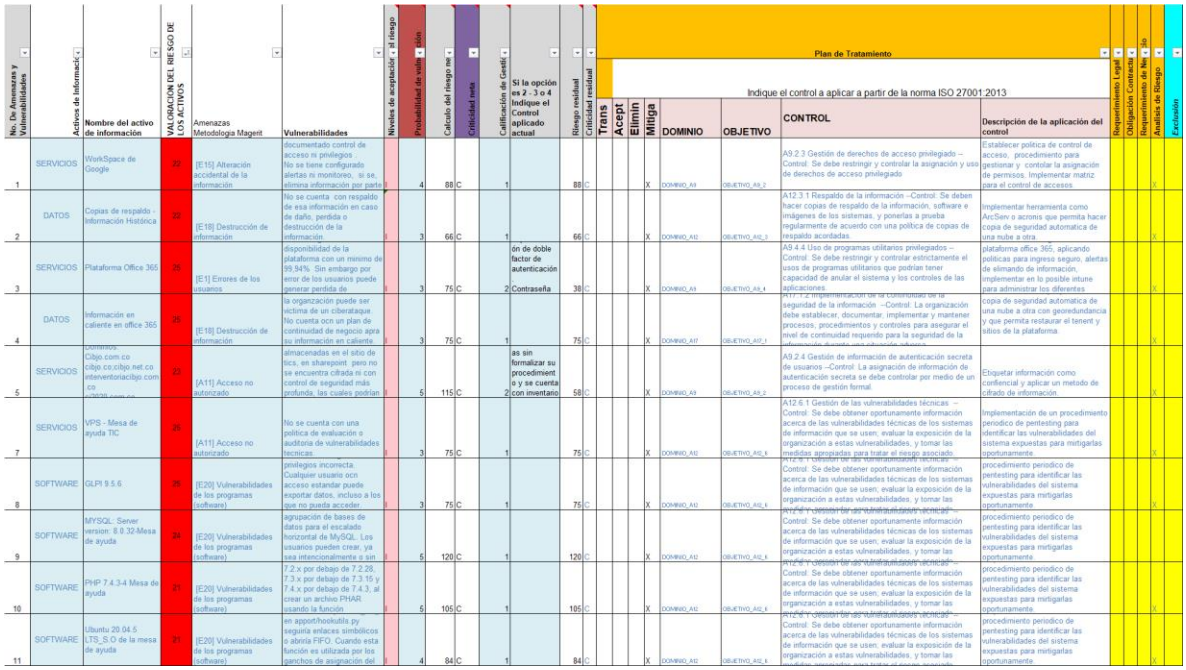
El objetivo de este paso es identificar el salvaguarda conveniente para proteger el sistema mediante la declaración de aplicabilidad. De acuerdo con Safecom, en su guía para comenzar una evaluación de riesgos de ciberseguridad, “un salvaguardas es un proceso que no está destinado a realizarse solo una vez por el contrario debe ser una determinación continua de las medidas de una organización y

perfeccionarse a medida que nuevas tecnologías y métodos estén disponibles”.[51] Partiendo del análisis del peor escenario que pudiese ocurrir en términos de ciberseguridad en una organización, Jay y Kemp en su libro Cybersecurity, expresa lo siguiente: Los estragos que un ataque podría causar afectando la infraestructura de una organización con vulnerabilidades, puede ocasionar pérdida o robo de datos, violaciones de seguridad, filtración de información sensible, requiere tiempo y trabajo intensivo para tratar de sobreponerse ante un ciberataque. El desafío para los administradores de los sistemas de grandes y pequeñas empresas es mantenerse a la vanguardia de tecnología que continuamente se transforma en nuevas amenazas, al mismo tiempo no pueden solo preocuparse por el ataque o amenaza más reciente, deben tener una visión del panorama general para determinar que se necesita para estar siempre operando en un entorno seguro, como responder sin exceder sus presupuestos.[52]

Una vez identificados los riesgos inaceptables o críticos de los activos de la organización con sus respectivas amenazas y vulnerabilidades, como se observa en la figura 22. Se plantea el tratamiento para mitigar el riesgo detectado, apoyados en los objetivos de control de “la norma ISO 27002: La norma contiene 114 controles agrupados en 14 capítulos, cada uno subdividido en áreas de seguridad, y a su vez, cada uno con sus objetivos de control” [53], los cuales se aplicarían, de acuerdo con la necesidad de proteger el activo. Para ello, continuamos trabajando con la matriz de gestión del riesgo.

[51] SAFECOM. Guide to Getting Started with a Cybersecurity Risk Assessment. [online]. pp. 5.
[52] JAY GONZALEZ Joaquín, KEMP L. Roger. Cybersecurity: Current Writings on Threats and Protection.
[53] ISO27001. Norma ISO 27001.

Figura 22. Plan de Tratamiento del Riesgo.



No. De Amenazas y Vulnerabilidades	Activos de Informació	Nombre del activo de Información	VALORACION DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación al riesgo	Probabilidad de ocurrencia	Calculo del riesgo neto	Criticidad neta	Calificación de Gestió	Si la opción es 2 - 3 o 4 indique el Control aplicado actual	Riesgo residual	Criticidad residual	Plan de Tratamiento							Requerimiento Legal	Obligación Contract	Requerimiento de Negocio	Análisis de Riesgo	Excepción
														Trans	Acept	Elimin	Mitiga	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					
														Indique el control a aplicar a partir de la norma ISO 27001:2013												
1	SERVICIOS	WorkSpace de Google	22	[E15] Alteración accidental de la información	documentado control de acceso ni privilegios ... No se tiene configurado alertas ni monitoreo, si se elimina información por parte	5	4	88	C	1		88	C				X	DOMINIO_A9	OBJETIVO_A9.2	A9.2.3 Gestión de derechos de acceso privilegiado -- Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Establecer política de control de acceso., procedimiento para gestionar y contolar la asignación de permisos. Implementar matriz para el control de accesos.					
2	DATOS	Copias de respaldo Información Histórica	22	[E18] Destrucción de información	No se cuenta con respaldo de esa información en caso de daño, perdida o destrucción de la información	5	3	66	C	1		66	C				X	DOMINIO_A12	OBJETIVO_A12.3	A12.3.1 Respaldo de la información --Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Implementar herramienta como ArcServ o acronis que permita hacer copia de seguridad automatica de una nube a otra.				X	
3	SERVICIOS	Plataforma Office 365	25	[E1] Errores de los usuarios	disponibilidad de la plataforma con un mínimo de 99.94%. Sin embargo por error de los usuarios puede generar perdida de	5	3	75	C	2	ón de doble factor de autenticación , Contraseña	38	C				X	DOMINIO_A9	OBJETIVO_A9.4	A9.4.4 Uso de programas utilitarios privilegiados -- Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	plataforma office 365, aplicando políticas para ingreso seguro, alertas de elimando de información, implementar en lo posible intune para administrar los diferentes				X	
4	DATOS	Información en caliente en office 365	25	[E18] Destrucción de información	la organización puede ser victima de un ciberataque. No cuenta ocn un plan de continuidad de negocio apra su información en caliente	5	3	75	C	1		75	C				X	DOMINIO_A17	OBJETIVO_A17.1	A17.1.2 Implementación de la continuidad de la seguridad de la información --Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	copia de seguridad automatica de una nube a otra con georedundancia y que permita restaurar el tenent y sitios de la plataforma.				X	
5	SERVICIOS	Dominios Cibjo.com.co cibjo.co;cibjo.net.co interventoriacibjo.com .co	23	[A11] Acceso no autorizado	almacenadas en el sitio de sics, en sharepoint, pero no se encuentra cifrada ni con control de seguridad más profunda, las cuales podrían	5	5	115	C	2	as sin formalizar su procedimient o y se cuenta con inventario	58	C				X	DOMINIO_A9	OBJETIVO_A9.2	A9.2.4 Gestión de información de autenticación secreta de usuarios --Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Etiquetar información como confiencial y aplicar un metodo de cifrado de información.				X	
7	SERVICIOS	VPS - Mesa de ayuda TIC	25	[A11] Acceso no autorizado	No se cuenta con una política de evaluación o auditoria de vulnerabilidades técnicas	5	3	75	C	1		75	C				X	DOMINIO_A12	OBJETIVO_A12.6	A12.6.1 Gestión de las vulnerabilidades técnicas -- Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Implementación de un procedimiento periodico de pentesting para identificar las vulnerabilidades del sistema expuestas para mitigarlas oportunamente.				X	
8	SOFTWARE	GLPI 9.5.6	25	[E20] Vulnerabilidades de los programas (software)	privilegios incorrecta. Cualquier usuario ocn acceso estandar puede exportar datos, incluso a los que no pueda acceder.	5	3	75	C	1		75	C				X	DOMINIO_A12	OBJETIVO_A12.6	A12.6.1 Gestión de las vulnerabilidades técnicas -- Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las	procedimiento periodico de pentesting para identificar las vulnerabilidades del sistema expuestas para mitigarlas oportunamente.				X	
9	SOFTWARE	MYSQL: Server version: 8.0.32-Mesa de ayuda	24	[E20] Vulnerabilidades de los programas (software)	agrupación de bases de datos para el escalado horizontal de MySQL. Los usuarios pueden crear, ya sea intencionalmente o sin	5	5	120	C	1		120	C				X	DOMINIO_A12	OBJETIVO_A12.6	A12.6.1 Gestión de las vulnerabilidades técnicas -- Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las	procedimiento periodico de pentesting para identificar las vulnerabilidades del sistema expuestas para mitigarlas oportunamente.				X	
10	SOFTWARE	PHP 7.4.3-4 Mesa de ayuda	21	[E20] Vulnerabilidades de los programas (software)	7.2.x por debajo de 7.2.28, 7.3.x por debajo de 7.3.15 y 7.4.x por debajo de 7.4.3, al crear un archivo PHAR usando la función	5	5	105	C	1		105	C				X	DOMINIO_A12	OBJETIVO_A12.6	A12.6.1 Gestión de las vulnerabilidades técnicas -- Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las	procedimiento periodico de pentesting para identificar las vulnerabilidades del sistema expuestas para mitigarlas oportunamente.				X	
11	SOFTWARE	Ubuntu 20.04.5 LTS_S.O de la mesa de ayuda	21	[E20] Vulnerabilidades de los programas (software)	en apport/hookutils.py seguiría enlaces simbólicos o abriría FIFO. Cuando esta función es utilizada por los ganchos de asignación del	5	4	84	C	1		84	C				X	DOMINIO_A12	OBJETIVO_A12.6	A12.6.1 Gestión de las vulnerabilidades técnicas -- Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las	procedimiento periodico de pentesting para identificar las vulnerabilidades del sistema expuestas para mitigarlas oportunamente.				X	

Fuente: Elaboración propia.

A continuación, en la tabla 7, se evidencian los controles con más frecuencia detectados para implementar:

- Seguridad en operaciones: De acuerdo con ISMS, este objetivo trata de: “operaciones, procedimientos y responsabilidades de la información: Los procedimientos operativos deben documentarse, esto garantiza el funcionamiento coherente y eficaz de los sistemas para el personal nuevo o los recursos cambiantes, también son fundamentales para la recuperación de desastres, continuidad de negocio. Es importante que los documentos se mantengan en un estado correcto y actualizados por tanto deben estar sujetos a procedimientos formales de gestión de cambios y revisión periódica”.[54]

[54] ISMS.ONLINE. ISO 27001 Annex A.12.1 Operational procedures and responsabilities.

- Control de acceso: De acuerdo con Irwin en la publicación de su blog: el objetivo de este anexo es garantizar que solo los colaboradores puedan ver la información relevante con su trabajo o cargo. Dividido en cuatro secciones: requisitos comerciales de control de acceso, gestión de acceso de los usuarios, responsabilidades del usuario.
- Organización de seguridad de la información: corresponde a la asignación de responsabilidades para tareas específicas, dividido en dos sesiones. A.6.1. garantiza que la organización establezca un marco que pueda implementar y mantener adecuadamente prácticas de seguridad de la información. Y el anexo A.6.2. Aborda los dispositivos móviles y trabajo remoto, diseñado para seguir las practicas adecuadas.
- Seguridad de los recursos humanos: El objetivo de este anexo es garantizar que los colaboradores y contratistas comprendan sus responsabilidades, dividido en tres secciones: responsabilidades individuales antes del empleo, durante y cuando ya no esté en la organización o por cambio de cargo. [55]

[55] IRWIN L. ISO 21001 Annex A controls explained.

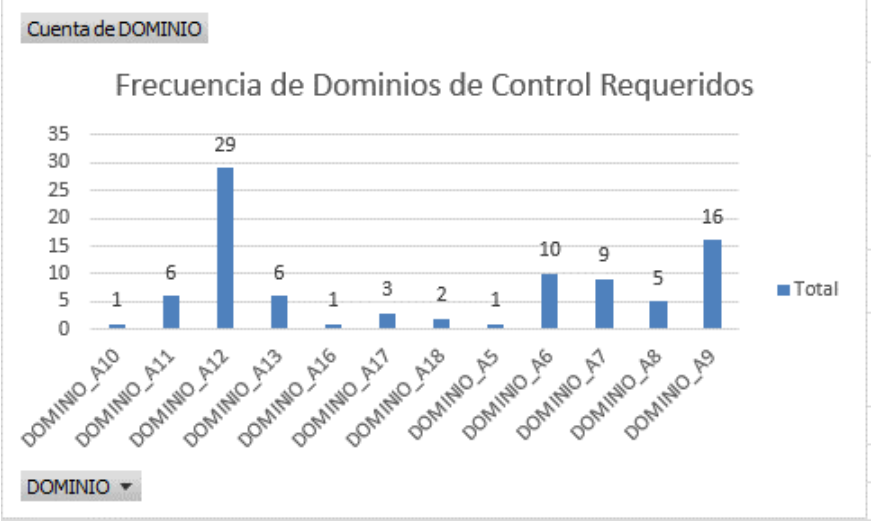
Tabla 7. Dominios de control requeridos de manera prioritaria.

Etiquetas de fila	Cuenta de Dominio	Nombre
DOMINIO_A10	1	
DOMINIO_A11	6	
DOMINIO_A12	**29**	**Seguridad de las operaciones**
DOMINIO_A13	6	
DOMINIO_A16	1	
DOMINIO_A17	3	
DOMINIO_A18	2	
DOMINIO_A5	1	
DOMINIO_A6	**10**	**Organización de Seguridad de la Información**
DOMINIO_A7	**9**	**Seguridad de los Recursos Humanos**
DOMINIO_A8	5	
DOMINIO_A9	**16**	**Control de Acceso**

Fuente: El autor.

En la figura 23. Obtenemos la estadística donde se observa que predomina el domino de control A12 Seguridad de las operaciones: trata de asegurar la operación de las instalaciones de procesamiento de la información como lo es información documentada de los procesos, gestión de cambios, gestión de capacidad, separación de ambientes para desarrollo y pruebas de operación. El siguiente dominio de control con más frecuencia es A9 Control de acceso: orientados a controlar y monitorizar los accesos a los medios de información. El domino A6 Organización de seguridad de la información, ocupa el top 3 en este reporte, establece un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. Por último, la seguridad de los recursos humanos, los errores humanos son el mayor riesgo para la seguridad de la información, abordan contratación, durante y finalización del empleo[56].

Figura 23. Estadística de Dominios de control requeridos.



Fuente: El autor.

[56] ISO270001. Norma ISO 27001. ISO27002.

En la tabla 8. Se observa los otros controles de dominio, hacen referencia a la necesidad de realizar la gestión de vulnerabilidades técnicas para detectar brechas de seguridad, desconocidas. Así mismo la separación de deberes, no es recomendable, ser juez y parte en la administración de aplicaciones de la organización, se requiere un procedimiento de ingreso seguro para las diferentes aplicaciones, servicios o herramientas de la organización y respaldo de información. Si, se aplica control a los dominios anteriormente mencionados, se estaría mitigando el riesgo de aproximadamente el 72% de los riesgos detectados como críticos.

Tabla 8. Descripción de los controles de dominio a aplicar a Cibjo SAS BIC

Controles de dominio	(Varios elementos)
A12.1.1 Procedimientos de operación documentados --Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	1
A12.2.1 Controles contra códigos maliciosos --Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	3
A12.3.1 Respaldo de la información --Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	9
A12.4.1 Registro de eventos --Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	2
A12.6.1 Gestión de las vulnerabilidades técnicas --Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	13
A12.7.1 Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos	1
A6.1.2 Separación de deberes --Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	7
A6.1.5 Seguridad de la información en la gestión de proyectos. --Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	3
A7.1.2 Términos y condiciones del empleo --Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	5
A7.2.1 Responsabilidades de la dirección --Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	3
A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. --Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	1

Controles de dominio	(Varios elementos)
A9.1.2 Acceso a redes y a servicios en red --Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	1
A9.2.1 Registro y cancelación del registro de usuarios --Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	1
A9.2.2 Suministro de acceso de usuarios --Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	1
A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	2
A9.2.4 Gestión de información de autenticación secreta de usuarios --Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	1
A9.4.2 Procedimiento de ingreso seguro --Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	7
A9.4.3 Sistema de gestión de contraseñas --Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	2
A9.4.4 Uso de programas utilitarios privilegiados --Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	1
Total, general	**64**

Fuente: El autor.

8 RECOMENCACION PARA EL ANALISIS DE VULNERABILIDADES TÉCNICAS

Dando continuidad al punto anterior, se detecta la necesidad de gestionar las vulnerabilidades técnicas, según Bin Azad, en su publicación, Introduction to security. Definig vulnerability “son problemas específicamente integrados en la tecnología, el software tiene errores que puede generar fuga de información o elevación de privilegios, implementaciones incorrectas pueden crear vulnerabilidades que pueden explotarse.”[57] Consiste en la ejecución de diferentes herramientas y metodología para identificar brechas de seguridad en una infraestructura objetivo.

8.1 METODOLOGÍA

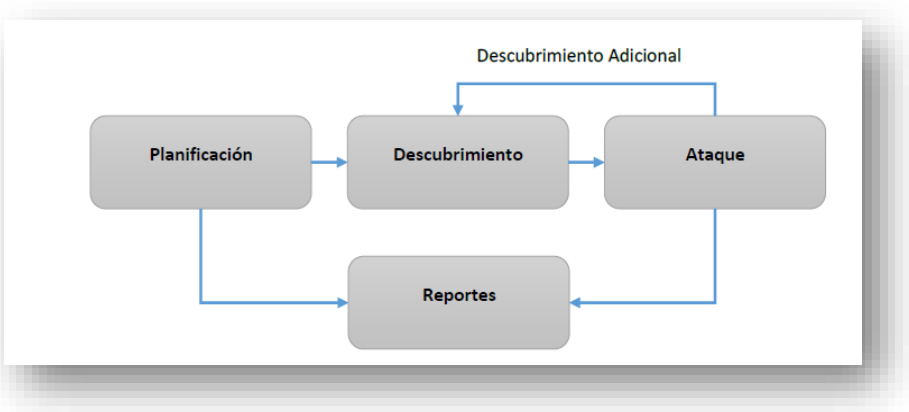
Tomando como referencia la NIST SP 800-11: Guía Técnica para pruebas y evaluación de seguridad de la información del Instituto Nacional de Estándares y Tecnología del gobierno de los EE. UU, en donde se describen las pautas de la manera correcta para realizar una evaluación de seguridad de la información. Pueden usarse tres métodos para la evaluación, en la figura 24, se representa gráficamente las siguientes fases:

- Pruebas: Poner a prueba uno o varios objetos de evolución bajo condiciones específicas para comparar el comportamiento real y el esperado.
- Examen: En este proceso se ejecuta la comprobación, inspección, revisión, observar, en el que se analiza uno o varios objetos para evaluación en el que se permita facilitar su comprensión, aclaración y obtención de evidencias.
- Entrevista: En este proceso se basa en las discusiones e intercambios con grupos de personas con el objetivo de facilitar la comprensión, identificación localización de las evidencias asociadas a los objetos.

[57] BIN AZAD, Tariq. Introdution to security. Definig vulnerability. ScienceDirect.

La NIST SP 800-115 propone un “proceso de evaluación de seguridad de la información, compuesto por al menos tres fases: Planeación, ejecución y post-ejecución.”[58]

Figura 24. Fases de una prueba de intrusión.



Fuente: NIST SP-800-115

Se presenta la siguiente propuesta de ejercicio de Análisis de vulnerabilidades técnicas para la empresa colombiana Cibjo SAS BIC, siendo muy importante, como plan de gestión. Una vez se obtenga aprobación por parte de la gerencia, se complementaría con el diagnostico que ya se tiene, con ello la organización obtendría un análisis más completo, identificando el estado en cuanto a vulnerabilidades detectadas desde la parte técnica de sus activos de infraestructura tecnológica.

8.2 PLANIFICACIÓN

En este proceso determina qué sistemas serán evaluados, enfoque, logística, consideraciones legales y políticas. Establece un plan de gestión en el que se

[58] NIST. Technical Guide to Information Security Testing and Assessment. p. 13.

incluya metas, objetivo general y objetivos específicos, alcance, requerimientos, roles y responsabilidades de los equipos, limitaciones, factores de éxito, condicionantes, recursos, planificación de tareas y entregables. En él se debe recopilar toda la información obtenida acerca de los activos que serán evaluados.
"Las evaluaciones de seguridad tienen objetivos específicos, niveles aceptables de riesgo y recursos disponibles. Se requiere recursos como tiempo, personal, hardware y software, la disponibilidad de recursos suele ser un factor limitante en el tipo y la frecuencia de las evaluaciones de seguridad. Evaluar los tipos de pruebas y exámenes de seguridad que ejecutará la organización".[59] Teniendo en cuenta lo anterior, se implementa la siguiente Política de Evaluación de Seguridad, una vez aprobada, se debe socializar con las partes interesadas y terceros involucrados.

8.3 OBJETIVO GENERAL

Realizar evaluaciones de seguridad de la infraestructura tecnológica y sus componentes (redes, servicios, dispositivos, entre otros). Utilizando metodologías y herramientas para la detección y explotación de vulnerabilidades.

8.4 POLÍTICA DE EVALUACIÓN DE SEGURIDAD PARA LA EVALUACIÓN DE VULNERABILIDADES TÉCNICAS

La organización contará con un proceso para identificar, **evaluar**, documentar, gestionar y mitigar los riesgos de Seguridad de la Información; dicho proceso se hará por lo menos **una vez al año o cuando ocurra algún evento especial**, en donde se identificarán riesgos y se evaluará su probabilidad. La alta Dirección y el responsable de Seguridad de la Información deberán alinearse con la gestión de Riesgos de Seguridad de la Información, para identificar el nivel de tolerancia y la

[59] NIST. Technical Guide to Information Security Testing and Assessment. p. 12.

capacidad máxima de aceptación del riesgo, considerando el efecto de la naturaleza de sus operaciones y líneas de negocio. [60]

8.4 ALCANCE.

El ejercicio de evaluación de seguridad que se recomienda realizar es de tipo caja negra, basado en que el evaluador o pentester, no dispone conocimiento previo acerca de la infraestructura que será probada, similar a un ataque real. Las pruebas de vulnerabilidad se realizarán a dos servidores, un aplicativo web y tres plataformas de servicios web, como se puede observar en la tabla 9. Servidor Contable y Talento Humano, alojado en nube privada contratada con un tercero y su aplicativo publicado: Nominal.

- Servidor Labsig: Alojado en una nube publica y su aplicativo Labsig
- Página web CIBJO.
- Sitio de tenant office 365: Office 365: Sitio colaborativo y repositorio de información en caliente.
- Página de WorkSpace de Google: Repositorio de información histórica.

Tabla 9. Objetivos para realizar la evaluación de vulnerabilidades.

Nombre de Servidor o Servicio	Dirección IP	Sistema Operativo	Servicios
Servidor Contable y Talento Humano **(DAYF2020)**	225.250.220.2	Windows server 2019	Escritorios Virtuales para conexión de Contabilidad y Talento Humano Siigo: Software contable Nominal: Software para la gestión de Talento Humano SQL Express: Bases de datos. Año de Implementación: 2020 Procesos que soporta: De apoyo transversales a la organización.
Servidor Labsig **(Labo2022)**	230.240.210.3	Windows 2019	Labsig: Software de gestión de laboratorio. SQL Estándar 2019

[60] CIBJO. Política de Seguridad de la Información y Ciberseguridad. Versión 1. [digital]. 2023. 12 p.

Nombre de Servidor o Servicio	Dirección IP	Sistema Operativo	Servicios
www.cibjo.co	236.228.215.4		Año de Implementación: 2022 Procesos que soporta: Misional. Página web CIBJO.
Portal.office.com/CIBJO	234.225.228.5	N/A	Año de Implementación: 2019. Procesos que soporta: De apoyo transversales a la organización. Sitio Colaborativo: Información en caliente en Share Point. One drive: Información de usuarios. Correo Electrónico Herramienta de mensajería y video llamadas: Teams Herramientas de Automatización de flujos. Formularios y Planner Repositorio información Histórica.
Cibjo.net.co	228.220.222.6	N/A	Cuenta de correo para administrar la plataforma. Procesos que soporta: Misionales y de apoyo. Año de Implementación: 2015

Fuente: El autor.

La anterior selección pertenece a los aplicativo publicados en la web y categorizados con información confidencial y critica de la organización. Para las pruebas realizadas, “se estudian los recursos utilizados en el almacenamiento, transporte, procesamiento de la información, lo anterior implica verificación de puertos, configuración de servicios, validación de permisos críticos, verificación de antivirus, actualizaciones de parches de sistema operativos y de aplicativos” [61]

Los tipos de pruebas a realizar son:

- Identificación de credenciales débiles.
- Fallas de Inyección: SQL.
- Exposición de datos sensibles.

[61] ALCALDIA MAYOR DE BOGOTA D.C. Guardianes de la Información. Penetración Testing.

- Entidades externas XML que se puedan utilizar para divulgar archivos internos, ejecución remota de código y ataques de denegación de servicio.
- Secuencias de comandos entre sitios (XSS): Ocurren cuando una aplicación incluye datos que no son de confianza en una nueva página web, sin validación adecuada. También puede ocurrir cuando una web existente la página se actualiza con datos proporcionados por el usuario usando un navegador API que puede crear HTML o JavaScript. Ciberdelincuentes aproveche las secuencias de comandos entre sitios para ejecutar secuencias de comandos en el sistema objetivo.
- Control de acceso roto: Acceso del atacante a cuentas de usuario con accesos incorrectamente restringidos.
- Deficiente configuración de seguridad: Configuración predeterminadas, inseguras o incompletas.
- Uso de componentes con vulnerabilidades conocidas.
- Servicios web.
- Pruebas de Ajax.
- Registro y monitoreo insuficientes: El registro y la supervisión insuficientes pueden permitir ciberdelincuentes para atacar los sistemas, incluso pueden manipular, extraer o destruir datos. [62]

8.5 HERRAMIENTAS REQUERIDAS PARA LA EVALUACIÓN DE VULNERABILIDADES TÉCNICAS.

Se solicita a la alta dirección autorización para la ejecución de las siguientes herramientas al equipo especializado, contratado para la evaluación de vulnerabilidades:

- Virtual Box: De acuerdo con la página oficial de VirtualBox “es una herramienta de virtualización para uso empresarial y doméstico, solución

[62] PERFORCE. Secure Coding Standards Best Practices. A guide to security in software development

empresarial disponible gratuitamente como software de código abierto bajo términos de licencia publica general GNU. Se ejecuta en Windows. linux, macOS, solaris y admite gran cantidad de sistemas operativos invitados."[63]

- Kali Linux: De acuerdo con la página oficial de Kali "es una distribución de código abierto, basada en debían orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa."[64]

8.7 HERRAMIENTAS PARA EL RECONOCIMIENTO

- Httrack: Palacios lo registra en su trabajo de grado "Es una aplicación que permite copias sitios web en Internet, permite la descarga de los directorios, imágenes u otros archivos desde el servidor web. Httrack organiza la estructura de enlaces relativa del sitio original. Al abrir una página del sitio web en el navegador se podrá navegar por el sitio de enlace en enlace, como si estuviera en línea".[65]
- Whois: De acuerdo con la página oficial "es un directorio público para identificar propietario de un dominio, buscar direcciones IP, ubicación, información del servidor web, permite localizar información de contacto administrativa y técnica del propietario de cualquier nombre de dominio," [66]
- Búsqueda en la web, redes sociales, búsqueda de metadatos que puedan arrojar información valiosa de la organización.

8.8 HERRAMIENTAS PARA ESCANEO DE PUERTOS Y VULNERABILIDADES

[63] VIRTUALBOX. Welcome to VirtualBox.org
[64] KALI. The most advanced penetration testing distribution.
[65] PALACIOS GALARDO, Margaret Lesly. Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la empresa DEVHUAYRA SAC Huancayo. Pág. 37.
[66] WHOIS. Welcome to Who.is.

- Nmap: De acuerdo con la página oficial “es un Software gratuito de código abierto para exploración de red y auditoria de seguridad, también es útil para inventario de red, gestión de cronogramas de actualización de servicios y monitoreo en tiempo real del host o del servicio.”[67]
- Owas Zap: De acuerdo con kali “es una herramienta de prueba de penetración para encontrar vulnerabilidades en aplicaciones web.” [68]
  De código abierto, identifica fallos de seguridad, asigna un nivel de riesgo y recomienda mecanismos de explotación y solución.
- Nessus: De acuerdo con la página oficial “es una herramienta con versiones tanto de código abierto como de pago, escanea vulnerabilidades de sistemas operativos, escanea puertos, detección de servicios, identifica vulnerabilidades.”[69]

8.9 HERRAMIENTAS PARA EXPLOTACIÓN DE VULNERABILIDADES

- Metasploit: Según Catoira, en su publicación, en la revista de seguridad de la universidad Nacional Autónoma de México “Metaesploit Framework Community (marco de trabajo o conjunto de prácticas) de código abierto, es una herramienta que permite ejecutar y desarrollar exploit contra sistemas objetivos, actualmente integrado con Kali Linux.”[70] Proporciona información de escaneo de vulnerabilidades, pruebas de penetración o Pentesting, entre otros.

---

[67]

[68] KALI. Zaproxy. Tool documentation.

[69] TENABLE. Tenable Nessus.

[70] CATOIRA, Fernando. Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit framework. Revista seguridad. Cultura de prevención para TI. Revista bimestral. (2013: México) nro. 19

- Hydra: De acuerdo con Kali “es una herramienta para explotar por fuerza bruta contraseñas de diferentes protocolos como: http, https, ftp, proxy, MySQL, entre otros.”[71]
- Inyección de SQL: De acuerdo con Kaspersky, se trata de “Insertar código en un sitio web para quebrantar medidas de seguridad e intentar acceder a los datos confidenciales y protegidos.”[72]En las siguientes tablas 10, 11 y 12, se puede observar, de forma resumida las herramientas propuestas anteriormente para las diferentes fases:

Tabla 10. Herramientas para el reconocimiento.

Técnicas	Herramienta de software
Obtención de la estructura de un sitio web mediante la clonación.	Httrack
Reconocimiento del dominio	Whois
Reconocimiento del sitio web	NetCraft

Fuente: PALACIOS GALLARDO, Margaret Lesly.

Tabla 11. Herramientas para el Escaneo.

Técnica	Herramienta de software
Barrido de puertos	Httrack
Obtención de información de Banner de los puertos y posibles vulnerabilidades	NMAP Scripting
Escaneo de Vulnerabilidades plataformas web	Owas Zap

Fuente: PALACIOS GALLARDO, Margaret Lesly.

Tabla 12. Herramientas para Explotación de Vulnerabilidades.

Técnica	Herramienta de software
Explotación de vulnerabilidades encontradas en las fases previas	Metasploit

[71] KALI. Hydra.
[72] KASPERSKY. ¿Qué es la inyección de SQL? Definición y explicación.

Inyección SQL	Comandos SQL
Explotación de contraseñas	Hydra

Fuente: PALACIOS GALLARDO, Margaret Lesly.

8.10 CONFIDENCIALIDAD DE LOS DATOS

Se debe firmar un acuerdo de confidencialidad y no divulgación de la información entre las partes, previamente al ejercicio. El manejo de datos e información recopilada deberá ser almacenada en el sitio de SharePoint de la organización, Cibjo SAS BIC (Proceso TICS – en la biblioteca de documentos: Seguridad). Las Personas autorizadas para conocer y analizar esta información son:

- Equipo de Tic: jefe de TIC e Infraestructura, Coordinador TIC, Analista TIC
- Dirección Administrativa: directora Administrativa.

8.11 MANEJO DE INCIDENTES.

Debido a que se realizará un ejercicio de intrusión de caja negra a los servicios publicados en la web y críticos de la organización, previamente se realizará copia de seguridad de los diferentes servicios para evitar posibles alteraciones y se comunicará con anticipación a los diferentes procesos con el fin de contar con disponibilidad y no afectar actividades relevantes en ejecución. Aun así, se puede presentar alteraciones que conlleven a restablecer un servicio que se vea afectado. **Sin embargo, como todo proceso existen unos riesgos no contemplados o desconocidos, los cuales la organización acepta ese apetito de riesgo.**

8.12 ACTIVIDADES PROHIBIDAS.

Se prohíbe la alteración de resultados, así como la divulgación de información confidencial fuera y dentro de la organización a personal que no esté autorizado para su conocimiento. Se prohíbe manipulación mal intencionada de los servicios

detectados como vulnerables, cabe resaltar que la evaluación a realizar es para detectarlas e identificar hasta donde podría llegar un ciberdelincuente,

8.13 UBICACIONES FÍSICAS DONDE SE ORIGINAN LAS EVALUACIONES

Debido a que el personal de evaluación es externo y resaltando el objetivo, se requiere hacer pruebas desde las redes externas de la organización, las ubicaciones físicas, deben ser informadas por el personal contratado, los equipos de cómputo empleados, así como las personas que conforman el equipo de trabajo.

8.14 AUTORIZACIÓN PARA EVALUACIÓN VULNERABILIDADES TÉCNICAS EN CIBJO SAS BIC

Cibjo SAS BIC, entendiendo la importancia de realizar evaluaciones de reconocimiento e intrusión a los diferentes servicios críticos de la organización para detección y mitigación de vulnerabilidades. Una vez enterados del procedimiento a seguir y los posibles riesgos. Por parte de **empresa evaluadora**, en acompañamiento del proceso de TIC de la organización, con el compromiso de fortalecer la seguridad de la información y la ciberseguridad de la organización nos comprometemos a mantener absoluta confidencialidad de la información obtenida mediante las pruebas ejecutadas y actuar con cautela y precaución para no afectar la ejecución del negocio durante este proceso.

Firman en Bogotá D.C., a los () días del mes de () de 2023

_____	_____
Empresa Auditora.	
Representante equipo Auditor Técnico	Gerente General Cibjo SAS BIC
C.C. No.	C.C. No**.**

9 PLAN DIRECTOR DE SEGURIDAD

De acuerdo con Dawson y compañía en su artículo, el rol de director de seguridad de la información (CISO) en las organizaciones es esencial, es el líder con función administrativa, pero desplegando esfuerzos en la gestión de la implementación y desarrollo de controles de seguridad, identificado con plena responsabilidad de la seguridad de la información dentro de la organización. Una de sus herramientas más importantes es el plan de seguridad que abarca todas las facetas de seguridad ya sea técnica, física y lógica. Proporciona su dirección en términos de disponibilidad, integridad, confidencialidad, no repudio y autenticación. Los tres objetivos más importantes del CISO son:

- Garantizar la continuidad del negocio y la recuperación ante desastres.
- Hacer cumplir la política de seguridad.
- Alinear la estrategia de seguridad con los objetivos comerciales.

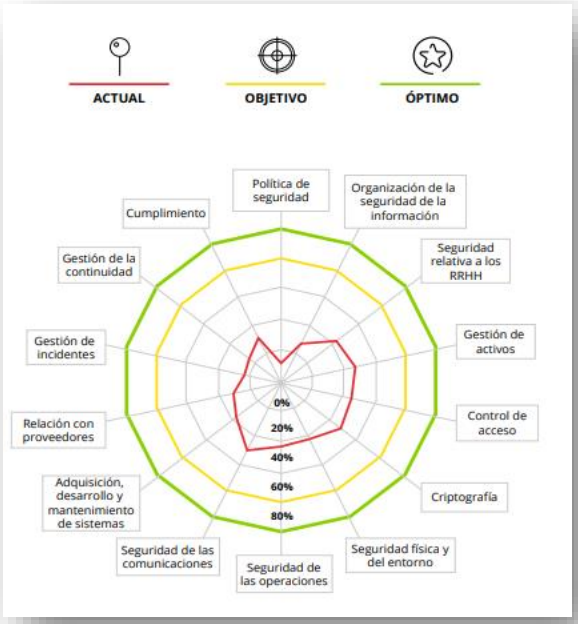
El CISO debe involucrar a los colegas para obtener apoyo a los objetivos, debe conseguir presupuesto para la seguridad de la información, formación y tecnologías. El cual refleje un retorno positivo de las inversiones en seguridad. También debe motivar y liderar equipos y aportar una cultura consciente de las seguridad dentro de la organización, el CISO prueba y evalúa constantemente efectividad de las políticas, procedimientos, prácticas de seguridad de la empresa.[73]

El Instituto Nacional de Ciberseguridad de España, resalta “la importancia de tener una planificación de las actividades a realizar, que cuente con un compromiso de la dirección contemplando: prioridades, responsables y recursos que se van a emplear para mejorar el nivel de seguridad de la organización. Se puede apreciar en la figura

[73] DAWSON, M. et al. Examining the Role of the Chief Information Security Officer (Ciso) & Security Plan.

25, los ámbitos para mejorar en aspectos normativos y regulatorios, tomando como referente la norma ISO/IEC 27002."[74] También refleja el cumplimiento de los dominios de control, La línea roja representa el grado de cumplimiento actual, la línea amarilla objetivo de cumplimiento a mediano plazo, la línea verde representa el nivel de cumplimiento optimo a largo plazo.

Figura 25. Aspectos normativos y regulatorios – ISO 27002:2017.



Fuente: INCIBE. Instituto nacional de Ciberseguridad. Plan director Seguridad. p.14.

9.1 OBJETIVO GENERAL

Proponer proyectos técnicos como organizativos, desde el punto de partida del análisis del riesgo, alineados con la estrategia del negocio para prevenir incidentes de seguridad y preparar a la organización para reaccionar ante ellos.

[74] INCIBE. Instituto nacional de Ciberseguridad. Plan director Seguridad

9.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

De acuerdo con la necesidad de establecer lineamientos que rijan a la organización en tema de Seguridad de la Información, se establece la siguiente política:

Cibjo SAS BIC y sus consorcios reconocen la importancia de proteger adecuadamente la información de amenazas que vulneren la continuidad del negocio, alineado con las estrategias para alcanzar los objetivos y necesidades de la organización y promoviendo una cultura de cumplimiento y buen uso. Basado en esto, establece el desarrollo de actividades de control para la protección de los activos de información, gestión de riesgos de seguridad de la información, conductas y aplicabilidad, definidos en esta política y que deben ser adoptados por los agentes implicados, que en el ejercicio de sus funciones utilicen información y servicios tecnológicos, a su vez es responsabilidad de estos agentes, reportar los incidentes de los que pudiera tener conocimiento, a través de los canales de comunicación establecidos. De acuerdo con lo anterior, se determinan las siguientes premisas:

- Minimizar el riesgo de las funciones más importantes de la organización.
- Cumplir los principios de seguridad de la información.
- Mantener la confianza de sus clientes, socios y colaboradores.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los agentes implicados de la organización.

Para visualizar con mayor detalle las políticas específicas (Ver Anexo D).

9.3 DECLARACIÓN DE APLICABILIDAD (SOA)

Según el Instituto Nacional de Ciberseguridad de España “la declaración de aplicabilidad es un documento que recoge los controles o medidas de seguridad que se deberán aplicar, también incluye descripción o de madurez o nivel actual de cada dominio de control.”[75] A continuación se establece el SoA que se debe implementar en la empresa Cibjo SAS BIC para fortalecer la seguridad de la información, le permitirá llevar a cabo la trazabilidad de los controles. En la figura 26. Se observa, la cantidad de controles, las iniciales del código del estado con su respectivo significado y la contribución u estado actual en la organización.

Tabla 13. Representación de códigos de Declaración de Aplicabilidad SoA

Cantidad	Códigos	Significado	Contribución %
26	**D**	El control se documentó e implementó	**23%**
43	**MD**	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	**38%**
8	**RD**	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	**7%**
34	**PNP**	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	**30%**
3	**NA (No Aplicable)**	El control no es aplicable para la empresa ni para el negocio	**3%**
114			

Fuente: El autor.

[75] INCIBE. Instituto nacional de Ciberseguridad. ¿Sabes cómo mejorar la ciberseguridad de tu organización? Implanta un Plan director de Seguridad.

En la tabla 14. Declaración de aplicabilidad SoA para Cibjo SAS BIC. En la columna de controles se listan los 14 dominios, con sus respectivos 35 objetivos de control para los cuales se revisa uno a uno los 114 controles de la norma ISO/IEC 27002:2013 (En esa revisión se indica el estado actual, si aplica o no el control, depende del contexto del negocio de la organización). Se registra su estado u observaciones y las recomendaciones.

Tabla 14. Declaración de aplicabilidad SoA para Cibjo SAS BIC

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
5.	**POLITICAS DE SEGURIDAD.**			
5.1	**Directrices de la Dirección en seguridad de la información.**			
5.1.1	Conjunto de políticas para la seguridad de la información.	D	Se cuenta con política de seguridad de la información y ciberseguridad, general y específicas.	Se debe fortalecer, complementando conjunto de las políticas de seguridad de la información de acuerdo con las necesidades identificadas en el análisis de riesgos, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
5.1.2	Revisión de las políticas para la seguridad de la información.	D	Recientemente se estableció la política general y específicas, de acuerdo con lo allí establecido se revisará y actualizará una vez al año o cuando se requiera.	se debe revisar de forma periódica las políticas de seguridad de la información para mantenerlas actualizadas, o si ocurren cambios significativos, asegurar su conveniencia, adecuación y eficacia continua.
6.	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.**			
6.1	**Organización interna.**			
6.1.1	Asignación de responsabilidades para la seguridad de la información.	MD	Actualmente se identifican los diferentes activos de los procesos, pero se detecta que varios roles comparten las mismas responsabilidades, se debe asociar un único responsable y documentarlo en las funciones de cada uno de los roles.	se debe mantener una organización de seguridad, donde los roles y responsabilidades estén definidas y asignadas a los participantes en el modelo de seguridad establecido por la organización.
6.1.2	Segregación de tareas.	PNP	En la actualidad, se detecta que se requiere capacitar a el administrador de tecnología en Siigo, Sigeslab, Clientify y otras herramientas para denegar full administración a los dueños de los procesos.	los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional de la información de la Entidad, o el uso indebido de los activos de la organización.
6.1.3	Contacto con las autoridades.	PNP	La organización no cuenta con un proceso, ni mecanismo definido para la comunicación externa.	Se deben mantener los contactos apropiados con las autoridades pertinentes, que pueden apoyar a solucionar conflictos en cuanto a la seguridad de la información de la Entidad. Auditorías externas permiten en caso de ser necesario velar por el cumplimiento de la seguridad de la información, de ser así se podrá contar con estos contactos.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
6.1.4	Contacto con grupos de interés especial.	PNP	La organización cuenta con la asesoría de su partner de Microsoft, quienes se encuentran certificados en normas de seguridad de la información y buenas prácticas.	Para la entidad siempre debe ser conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Se recomienda Contactar con otros grupos que fortalezcan el conocimiento y apoyo.
6.1.5	Seguridad de la información en la gestión de proyectos.	MD	En algunas oportunidades, por disponibilidad de recursos algunos proyectos son un poco limitados, sin embargo, cuentan con una persona especializada en seguridad para asesorarlos en las mejores prácticas y se trabaja con base a la experiencia en la ejecución de proyectos.	Durante la planeación y ejecución de los proyectos de la Entidad, además de las áreas interesadas, debe participar el área de Seguridad de la Información como generador de recomendaciones en la evaluación de los riesgos inherentes con dichos proyectos.
6.2	**Dispositivos para movilidad y teletrabajo.**			
6.2.1	Política de uso de dispositivos para movilidad.	MD	Los colaboradores que por su cargo lo requiera, se les asigna portátiles y teléfonos corporativos para la ejecución de sus funciones desde cualquiera de las sucursales, sin embargo, se requiere en especial para los teléfonos, implementar políticas y aplicar controles.	el uso de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Entidad, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la Gerencia de Seguridad de la Información y podrá llevarse a cabo sólo en dispositivos provistos por la organización para tal fin.
6.2.2	Teletrabajo.	D	Actualmente el trabajo desde casa es un beneficio para la mayor parte de colaboradores en la ubicación en Bogotá.	se debe aplicar más controles para proteger la información a la que se tiene acceso, que es procesada o almacenada desde los dispositivos en los que se realiza teletrabajo.
7.	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**			
7.1	**Antes de la contratación.**			
7.1.1	Investigación de antecedentes.	D	En la actualidad el área encargada de este control es recursos humanos y se lleva a cabalidad.	los nuevos empleados que ingresen a la entidad deben pasar por un proceso de investigación de antecedentes, con el fin de mitigar los riesgos en el uso de la información.
7.1.2	Términos y condiciones de contratación.	D	En la actualidad el área encargada de este control es recursos humanos y se lleva a cabalidad.	los contratos de los empleados deben incluir cláusulas que especifiquen las responsabilidades y los cuidados que deben tener con la información de la Entidad.
7.2	**Durante la contratación.**			
7.2.1	Responsabilidades de gestión.	MD	Aunque los empleados conocen sus deberes, es importante reforzar a través de capacitación estos temas de forma continua.	La organización debe proveer los mecanismos necesarios para asegurar que sus empleados cumplan con sus responsabilidades en Seguridad de la Información desde su ingreso hasta su retiro. (Monitoreo continuo y auditorias).
7.2.2	Concienciación, educación y capacitación en seguridad de la información	MD	Aunque los empleados conocen sus deberes, es importante reforzar a través de capacitación estos temas de forma continua.	Semestralmente se realizan capacitaciones de sensibilización y cultura en seguridad de la información para los empleados y terceros, capacitándolos constantemente en actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
7.2.3	Proceso disciplinario.	D	Actualmente el incumplimiento de políticas o falta grave es sujeta a un proceso disciplinario e incluso a la terminación de contrato si es necesario.	las Políticas de Seguridad de la Información con sus respectivas normas, estándares, procedimientos y demás documentos que se generen, son de obligatorio cumplimiento.
7.3	**Cese o cambio de puesto de trabajo.**			

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
7.3.1	Cese o cambio de puesto de trabajo.	MD	Actualmente el incumplimiento de políticas o falta grave es sujeta a un proceso disciplinario e incluso a la terminación de contrato si es necesario. Para este particular se capacita al personal antes de ocupar una nueva posición dentro de la compañía.	Se debe informar a los empleados o contratistas, las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato, los cuales deben cumplir. Se informa los nuevos accesos, se valida la capacitación inicial en el manejo de las herramientas que requiere.
8.	**GESTIÓN DE ACTIVOS.**			
8.1	**Responsabilidad sobre los activos.**			
8.1.1	Inventario de activos.	MD	Durante el proceso de mejora se realizó inventario y su respectivo control. Hace falta documentar y proceder con la clasificación de la información para aplicar los controles respectivos.	La organización debe mantener un inventario de recursos o activos de información. Los dueños de la información deben clasificar la información basados en su valor, sensibilidad, riesgo de pérdida o compromiso y/o requerimientos legales de retención.
8.1.2	Propiedad de los activos.	MD	Actualmente el proceso de TIC lleva el inventario y su respectivo control.	El área responsable del proceso debe realizar el debido control y mantenimiento al inventario de activos de tecnología e información, para establecer responsabilidad sobre la tenencia de estos y la información sobre estos, incluido el control al licenciamiento de software. Se detecta que en los diferentes procesos existen varios responsables del mismo activo, se recomienda establecer un solo responsable y socializarlo en los equipos de trabajo.
8.1.3	Uso aceptable de los activos.	MD	Con la asignación de los activos, se realiza acta de entrega para el buen uso y responsabilidad por parte del colaborador. Así como la inducción a la herramienta de Office 365 para el buen uso de la plataforma y las mejores prácticas.	Fortalecer el uso aceptable de activos, especialmente para la información, éstos deben ser clasificados por el dueño de la información, mediante el estándar de clasificación establecido.
8.1.4	Devolución de activos.	MD	En la actualidad para el retiro de personal, talento humano notifica su retiro, se procede a denegar accesos y recibir elementos asignados, validando con el inventario. Una vez se valida que la información se encuentra en la nube, se procede a formatear el equipo para ser devuelto al proveedor.	Se recomienda automatizar el proceso para que sea más ágil.
8.2	**Clasificación de la información.**			
8.2.1	Directrices de clasificación.	PNP	Se requiere clasificar la información según su función.	Los dueños de la información deben clasificar los niveles de sensibilidad de esta, de acuerdo con criterios que permitan velar por la seguridad de la información, estos se encuentran en detalle en las políticas de seguridad.
8.2.2	Etiquetado y manipulado de la información.	PNP	En la actualidad este control no se lleva a cabo.	Los dueños de la información deben etiquetar y manipular los niveles de sensibilidad de esta, de acuerdo con criterios que permitan velar por la seguridad de la información, estos se encuentran en detalle en las políticas de seguridad.
8.2.3	Manipulación de activos.	RD	En la actualidad este control no se lleva a cabo.	Cada jefe de proceso debe realizar el proceso de clasificación de información, inventariando la información utilizada por su proceso.
8.3	**Manejo de los soportes de almacenamiento.**			

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
8.3.1	Gestión de soportes extraíbles.	MD	Actualmente se cuenta con control para los equipos corporativos, sin embargo, ciertas maquinas requieren excepción por la función.	Se requiere fortalecer, cuando se permite la conexión a la red de la Entidad de equipos portátiles, notebooks, computadores, dispositivos móviles o cualquier otro dispositivo que se considere removible, de uso personal de los funcionarios, sin la debida autorización del jefe inmediato y de la Gerencia de Seguridad de la Información.
8.3.2	Eliminación de soportes.	RD	En la actualidad se realiza copia de seguridad a proceso contable y talento humano de forma automática y cuando se requiere en algunas ocasiones manual, para office 365 depende de los ANS de Microsoft para office 365 y WorkSpace los cuales no se encuentran documentados.	Se debe implementar un plan de continuidad y/o respaldo de información. Permanentemente se debe efectuar copia de respaldo de toda la información considerada confidencial o sensible y que se encuentre contenida en los herramientas en nube. En especial se debe asegurar el respaldo de información cuando termine el vínculo laboral del funcionario o contractual del proveedor responsable de su generación, edición y manejo, así como cuando se vaya a dar de baja un activo tecnológico (por pérdida, daño, devolución, enajenación o donación, entre otros).
8.3.3	Soportes físicos en tránsito.	D	En la actualidad se encuentra vigente este control garantizado por el proceso de Gestión de la Información, para cada uno de los movimientos que se presente fuera de la compañía. Sin embargo, se debe revisar a detalle el etiquetado de la información.	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro. Se etiquetarán las cajas con el nivel confidencialidad de la información que contienen.
9.	**CONTROL DE ACCESOS.**			
9.1	**Requisitos de negocio para el control de accesos.**			
9.1.1	Política de control de accesos.	MD	En la actualidad está política se encuentra documentada, se recomienda reforzar de forma periódica cada uno de los empleados de la compañía.	el uso de la información de la Entidad debe ser controlado para prevenir accesos no autorizados. Los privilegios sobre la información deben ser otorgados y mantenidos de acuerdo con las necesidades de la operación, limitando el acceso sólo a lo que es requerido.
9.1.2	Control de acceso a las redes y servicios asociados.	RD	Se requiere implementar matriz acceso a usuarios con su respectiva documentación de acuerdo con el Rol de usuario y las aplicaciones permitidas.	El acceso a la red de la organización debe ser otorgado solo a usuarios autorizados, previa definición, verificación y control de los perfiles y roles para el acceso en los diferentes sistemas de información, en coordinación con el área de Recursos Humanos, la Gerencia Administrativa y la Gerencia de IT.
9.2	**Gestión de acceso de usuario.**			
9.2.1	Gestión de altas/bajas en el registro de usuarios.	MD	Este control se realiza en la actualidad con las políticas existentes, pero hace falta documentar el proceso.	Se debe establecer por la organización, los procedimientos para cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	MD	Se debe documentar el correcto acceso a cada una de las aplicaciones y mecanismos de control que permiten garantizar seguridad en el tratamiento de información.	se deben establecer mecanismos de control de acceso físico y lógico para los usuarios, con el fin de asegurar que los activos de información se mantengan protegidos de una manera consistente con su valor para el negocio y con los riesgos de pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	MD	Dependiendo del cargo del personal se brindan acceso a algunas aplicaciones que son restringidas, sin embargo, si se llega a presentar alguna novedad con el empleado, este debe comprometer y aceptar su responsabilidad por medio de un acta de indemnidad donde acata tosa su responsabilidad.	La organización se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. El personal seleccionado por la organización podrá utilizar tecnología de uso restringido como la de monitoreo de red, datos operacionales y eventos en seguridad de la información.
9.2.4	Manejo de claves de acceso	D	Se cuenta con política para el manejo de contraseñas y autenticación a las diferentes herramientas de la organización.	los usuarios de la Organización serán requeridos para que se autentiquen ellos mismos, previa obtención del acceso a la información.
9.2.5	Revisión de los derechos de acceso de los usuarios.	MD	Se realiza este proceso, pero no se encuentra documentados.	En el uso de la información de la organización se debe presumir privacidad, por lo que cuando ésta sea utilizada se deben crear registros de la actividad realizada, que pueden ser revisados periódicamente o en una investigación, con el objetivo de detectar abusos y amenazas.
9.2.6	Retirada o adaptación de los derechos de acceso	D	Se realiza este proceso, pero no se encuentra documentados y requiere control para que se mantenga y permita hacer seguimiento de las políticas instauradas.	Todos los usuarios que acceden la información de la Entidad deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal, la cual puede ser modificada cuando se presente un cambio de funciones del empleado o se retire definitivamente de la organización.
9.3	**Responsabilidades del usuario.**			
9.3.1	Uso de información confidencial para la autenticación.	RD	Dependiendo del cargo del personal se brindan acceso a algunas aplicaciones que son restringidas, se requiere establecer un control que permita la segregación de deberes y clasificación de información.	cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de la Entidad. Por lo tanto, la identidad de cada usuario que acceda los recursos informáticos debe ser establecida y autenticada de una manera única y no puede ser compartida.
9.4	**Control de acceso a sistemas y aplicaciones.**			
9.4.1	Restricción del acceso a la información.	RD	Dependiendo del cargo del personal se brindan acceso a algunas aplicaciones que son restringidas, se requiere establecer un control que permita la segregación de deberes y clasificación de información.	el acceso a la información de la Entidad y a las funciones de los sistemas de las aplicaciones, será restringido de acuerdo con la política de control de acceso, ya que se debe asegurar que los usuarios de la información únicamente tengan acceso a lo que les concierne.
9.4.2	Procedimientos seguros de inicio de sesión.	D	Semestralmente y en la inducción del colaborador, el proceso TIC capacita en seguridad de la información y buenas prácticas.	Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos de manera segura.
9.4.3	Gestión de contraseñas de usuario.	D	La política se encuentra establecida con los lineamientos para tener en cuenta en la definición de contraseñas.	• Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc. • Tener mínimo ocho caracteres alfanuméricos. • Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
9.4.4	Uso de herramientas de administración de sistemas.	MD	Este control se encuentra implementado en el área de IT y está funcionando acorde a la normatividad solicitada por la compañía. Sin embargo, requiere monitoreo continuo y documentar.	el área de Tecnología de la Entidad velará porque los recursos de la plataforma tecnológica y los servicios de red sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichas plataformas y servicios.
9.4.5	Control de acceso al código fuente de los programas.	PNP	Este control no se encuentra implementado.	el área de Tecnología de la Entidad, como responsable de la administración de los sistemas de información, aplicativos y sus códigos fuente, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.
10.	**CIFRADO.**			
10.1	**Controles criptográficos.**			
10.1.1	Política de uso de los controles criptográficos.	PNP	Este control no se encuentra implementado.	La organización velará porque la información, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio, con el propósito de proteger su confidencialidad e integridad.
10.1.2	Gestión de claves.	PNP	Este control no se encuentra implementado.	La organización debe proteger los tipos de claves de modificación o destrucción; las claves secretas y las privadas además requieren protección contra su distribución no autorizada.
11.	**SEGURIDAD FÍSICA Y AMBIENTAL.**			
11.1	**Áreas seguras.**			
11.1.1	Perímetro de seguridad física.	D	Actualmente cada una de las áreas cuenta con el espacio propicio para su desarrollo, teniendo en cuenta controles que permiten su correcto funcionamiento. Aplicable para el laboratorio de Bogotá.	la seguridad física de la Entidad debe basarse en perímetros y áreas seguras, las cuales serán protegidas por medio de controles circundantes apropiados.
11.1.2	Controles físicos de entrada.	MD	Aplica para las oficinas en Bogotá, fortalecer extendiéndose a los proyectos a nivel nacional.	Todas las entradas a las áreas físicas del negocio deben tener un nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas.
11.1.3	Seguridad de oficinas, despachos y recursos.	MD	Actualmente cada una de las áreas cuenta con acceso a cada uno de sus funcionarios previamente identificados, permitiendo tener un control efectivo en los accesos del personal.	Los ingresos y egresos de personal a las instalaciones de la Entidad deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
11.1.4	Protección contra las amenazas externas y ambientales.	MD	Actualmente se cumple con la normatividad necesaria para cumplir con la seguridad de los recursos físicos, pero requiere optimización y monitoreo para garantizar que se cumpla en la oficina Elemento. (Para os proyectos se debe implementar un espacio especial para los dispositivos activos de telecomunicaciones).	la organización debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos, en especial la plataforma tecnológica ubicada en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
11.1.5	El trabajo en áreas seguras.	D	Actualmente cada una de las áreas cuenta con el espacio propicio para su desarrollo, teniendo en cuenta controles que permiten su correcto funcionamiento, brindando seguridad a los equipos de trabajo. Aplica en especial para laboratorio en Bogotá.	la Entidad proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así
11.1.6	Áreas de acceso público, carga y descarga.	NA (No Applicable)	No aplica	No aplica
11.2	**Seguridad de los equipos.**			
11.2.1	Emplazamiento y protección de equipos.	MD	Actualmente se cumple con la normatividad necesaria para cumplir con la seguridad de los recursos físicos, en caso de que se presente alguna novedad por temas ambientales, sin embargo, se ve en algunas ocasiones exceso de confianza y no cumplimiento de normativas, por lo cual es necesario reforzar a través de capacitación.	Los recursos informáticos de la Entidad deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades.
11.2.2	Instalaciones de suministro.	D	Actualmente este control se encuentra implementado a través de planes de mantenimiento periódico que permite alertar en caso de emergencia y adicional dar un soporte preventivo para evitar futuros daños. Requiere fortalecimiento para que se cumpla puntualmente.	La organización debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.
11.2.3	Seguridad del cableado.	D	Actualmente este control se encuentra implementado para las ubicaciones en Bogotá, se recomienda fortalecer en los proyectos a nivel nacional.	el área de Tecnología de la Entidad debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
11.2.4	Mantenimiento de los equipos.	MD	Actualmente este control se encuentra implementado a través de planes de mantenimiento periódico que permite alertar en caso de emergencia y adicional dar un soporte preventivo para evitar futuros daños	Los medios y equipos donde se almacena procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento; para ello se debe realizar los mantenimientos preventivos periódicamente cada seis meses y correctivos cuando se requieran.
11.2.5	Salida de activos fuera de las dependencias de la empresa.	MD	Actualmente se realizan registros de las salidas y entradas de los diferentes equipos que se mueven entre sedes, sin embargo, requiere ser documentado en qué casos aplica.	la Entidad debe velar porque la entrada y salida de información, software, estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos corporativos de las instalaciones, cuente con la autorización documentada y aprobada previamente por el responsable de los recursos físicos o en su defecto el área responsable del activo.
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	D	El proceso de TIC, a través de control de registros el movimiento externo de equipos y activos de la compañía, en algunos casos utiliza trasportadoras privadas para evitar inconvenientes en los traslados. Sin embargo, se requiere fortalecer la forma de asegurar los equipos por robo en el desplazamiento de los teletrabajadores.	El proceso responsable de los recursos físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera del instituto posean pólizas de seguro que cubran los diferentes riesgos que puedan presentar.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	PNP	La organización en general no cuenta con dispositivos de almacenamiento externo, sin embargo, en los proyectos antiguos si los tenia, se debe implementar control para los casos que se presenten.	el área de Tecnología debe efectuar la reutilización o retirada segura de los dispositivos de almacenamiento que tienen información de la Entidad, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.
11.2.8	Equipo informático de usuario desatendido.	MD	Para estaciones de trabajo conectadas en acceso remoto, teletrabajo se cuenta con controles de acceso que permiten garantizar el correcto uso de las aplicaciones dentro y fuera de la compañía.	Se recomienda controlar la conexión desde dispositivos no permitidos. El proceso TIC, debe velar porque los equipos informáticos de los usuarios que no trabajan dentro de las instalaciones de la Entidad tengan sus medios de almacenamiento cifrados, los softwares para protección de la información, que eviten que la información se accedida por personas no autorizadas.
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	D	Este control se encuentra implementado en el área de IT y está funcionando acorde a la normatividad solicitada por la compañía.	Se recomienda fortalecer, se identifica que muchos usuarios no acatan las recomendaciones y buenas prácticas. Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores
12.	**SEGURIDAD EN LA OPERATIVA.**			
12.1	**Responsabilidades y procedimientos de operación.**			
12.1.1	Documentación de procedimientos de operación.	D	El proceso de tecnología en la actualidad se encuentra en proceso de gestión del cambio aplicado controles y procedimientos que permitan mejorar la seguridad de la información (En construcción).	La organización debe efectuar, a través de sus funcionarios responsables de los procesos, la actualización de la documentación y los procedimientos relacionados con la operación y administración de la plataforma tecnológica.
12.1.2	Gestión de cambios.	D	Se lleva a cabo este control, se requiere fortalecer con actualización frecuente.	Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios del proceso TIC y sistemas de Información de la Entidad.
12.1.3	Gestión de capacidades.	MD	El control se realiza, pero debe ser documentado.	El proceso de TIC, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica
12.1.4	Separación de entornos de desarrollo, prueba y producción.	MD	De acuerdo con la necesidad, se implementan ambientes de prueba. No se encuentra documentado.	el área de Tecnología debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción
12.2	**Protección contra código malicioso.**			
12.2.1	Controles contra el código malicioso.	MD	Se cuenta con controles en la plataforma office 365 y herramienta en nube de Kaspersky, también se capacita a usuario final, concientización. Sin embargo, es necesario reforzar a través de capacitaciones para evitar incidentes de seguridad.	La organización proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso
12.3	**Copias de seguridad.**			

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
12.3.1	Copias de seguridad de la información.	RD	Las copias de seguridad se realizan por el proceso TIC, cuando se requiere de forma manual, se tiene implementado para software de Talento Humano y Contabilidad. Sin embargo se requiere establecer control para las herramientas en la nube. .	La organización certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades
12.4	**Registro de actividad y supervisión.**			
12.4.1	Registro y gestión de eventos de actividad.	PNP	No se tiene implementado este control	La organización realizará monitoreo permanente del uso que dan los funcionarios y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información.
12.4.2	Protección de los registros de información.	PNP	Actualmente el proceso TIC se queda corto en recurso humano para realizar seguimiento y monitoreo a las diferentes herramientas de seguridad con las que cuenta la organización (Seguridad de office 365 y Kaspersky).	el proceso TIC debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de la Entidad.
12.4.3	Registros de actividad del administrador y operador del sistema.	PNP	Actualmente el proceso TIC se queda corto en recurso humano para realizar seguimiento y monitoreo a las diferentes herramientas de seguridad con las que cuenta la organización (Seguridad de office 365 y Kaspersky).	el proceso de Control Interno debe revisar periódicamente los registros de auditoría de los administradores y operadores de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo
12.4.4	Sincronización de relojes.	PNP	No se tiene implementado este control	El proceso TIC debe proveer un sistema que sincronice los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la Entidad o de un dominio de seguridad.
12.5	**Control del software en explotación.**			
12.5.1	Instalación del software en sistemas en producción.	MD	Este control se realiza, pero no se encuentra documentado y no se tiene definido los responsables.	a través del proceso TIC, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado
12.6	**Gestión de la vulnerabilidad técnica.**			
12.6.1	Gestión de las vulnerabilidades técnicas.	PNP	Este control se encuentra en proceso, propuesta para aceptación por parte de la gerencia.	A través del proceso de TIC, se revisa periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades
12.6.2	Restricciones en la instalación de software.	D	Es importante que el área de IT tenga en cuenta los perfiles y roles de cada uno de los usuarios para la instalación de aplicaciones.	La instalación de software en los computadores suministrados por la Entidad es una función exclusiva del proceso TIC
12.7	**Consideraciones de las auditorías de los sistemas de información.**			

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
12.7.1	Controles de auditoría de los sistemas de información.	D	Se realizan auditorias para la validación de cumplimiento el proceso.	El proceso de Auditoría debe realizar monitoreo periódicamente para evaluar la conformidad con las políticas de la organización, para evaluar el nivel de implementación de los sistemas de información, para evaluar el estado de mantenimiento y la capacidad de mejoramiento de los sistemas de información
13.	**SEGURIDAD EN LAS TELECOMUNICACIONES.**			
13.1	**Gestión de la seguridad en las redes.**			
13.1.1	Controles de red.	PNP	No se tiene implementado este control	La organización establecerá, a través del área de Tecnología, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas y minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos
13.1.2	Mecanismos de seguridad asociados a servicios en red.	MD	Se cuenta con niveles de servicio para los clientes internos de la organización en mesa de ayuda, así como acuerdos con proveedores estratégicos. Falta documentarlos.	Se debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
13.1.3	Segregación de redes.	PNP	No se tiene implementado este control	el proceso TIC debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Entidad
13.2	**Intercambio de información con partes externas.**			
13.2.1	Políticas y procedimientos de intercambio de información.	MD	Toda información que se envíe a dominios diferentes de la compañía debe ser enviada por correo seguro y cifrada para evitar fugas de información. Se fortalece con campañas de concientización, política de seguridad. En proceso de aplicación de controles.	la Entidad asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades u otro destino externo y establecerá los procedimientos y controles necesarios para el intercambio de información
13.2.2	Acuerdos de intercambio.	MD	Toda información que se envíe a dominios diferentes de la compañía debe ser enviada por correo seguro y cifrada para evitar fugas de información. Se fortalece con campañas de concientización, política de seguridad. En proceso de aplicación de controles.	El proceso jurídico, en acompañamiento con el proceso TIC, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la Entidad y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos
13.2.3	Mensajería electrónica.	D	Toda información que se envíe a dominios diferentes de la compañía debe ser enviada por correo seguro y para evitar fugas de información. Se fortalece con campañas de concientización, política de seguridad. En proceso de aplicación de controles.	la Entidad, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio
13.2.4	Acuerdos de confidencialidad y secreto.	MD	están establecidos controles entre partes terceras y de la compañía con el fin de que la información no se vea vulnerada en ninguno de principios. Se recomienda fortalecer con todos los proveedores y terceros.	El proceso jurídico, en acompañamiento con el proceso TIC, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la Entidad y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
14.	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**			
14.1	**Requisitos de seguridad de los sistemas de información.**			
14.1.1	Análisis y especificación de los requisitos de seguridad.	MD	De acuerdo con las necesidades de la compañía se especifican requisitos de seguridad en funcionamiento a la seguridad de la información.	los requerimientos de seguridad de la información deben ser identificados previos al diseño de los sistemas de tecnología de la información.
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	MD	Se requiere fortalecer y documentar los requisitos previos Para lograr el acceso a los diferentes medios de la empresa.	El proceso TIC debe asegurar que los sistemas de información o aplicativos informáticos que pasan a través de redes públicas incluyen controles de seguridad y cumplen con las políticas de seguridad de la información, con el fin de proteger la información de la Entidad de posibles ataques.
14.1.3	Protección de las transacciones por redes telemáticas.	MD	Para pagos del proceso financiero y compras se les recomienda las mejores prácticas desde su equipo corporativo. No documentado.	los desarrolladores de las aplicaciones deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.
14.2	**Seguridad en los procesos de desarrollo y soporte.**			
14.2.1	Política de desarrollo seguro de software.	PNP	Aunque no se hacen desarrollos, si se automatizan procesos con herramientas en línea que son publicados a los cuales se requiere aplicar control para garantizar la seguridad de la información.	Se debe velar porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado
14.2.2	Procedimientos de control de cambios en los sistemas.	PNP	No se tiene implementado este control	el proceso TIC, debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Entidad.
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	PNP	No se tiene implementado este control	el proceso TIC, debe realizar pruebas de todos los sistemas, cuando se presente un cambio de sistema operativo en los equipos de cómputo de la Entidad, con el fin de revisar los posibles impactos en las operaciones o en la seguridad de la información de la organización.
14.2.4	Restricciones a los cambios en los paquetes de software.	PNP	No se tiene implementado este control	la realización de un cambio tecnológico en un paquete de software entregado por un tercero, que no considere los requerimientos de seguridad de la Información hace que la Entidad esté expuesta a riesgos.
14.2.5	Uso de principios de ingeniería en protección de sistemas.	PNP	No se tiene implementado este control	Se deberían establecer mecanismos de control en la labor de implementación en el sistema de información, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.
14.2.6	Seguridad en entornos de desarrollo.	NA (No Aplicable)	La organización no hace desarrollo.	la Entidad establecerá y protegerá adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
14.2.7	Externalización del desarrollo de software.	PNP	No se tiene implementado este control. Se firman acuerdos de confidencialidad cuando se terceriza un desarrollo.	el proceso TIC debe establecer el procedimiento y los controles de acceso a los ambientes de desarrollo de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	NA (No Aplicable)	Al no desarrollar aplicaciones, no aplica, sin embargo, al tercerizar si se realizan pruebas de funcionalidad, pero muy básicas, enfocadas a lo operativo.	los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, pasando desde el diseño hasta la puesta en marcha.
14.2.9	Pruebas de aceptación.	PNP	Luego de realizadas cada una de las pruebas y se verifica el correcto funcionamiento de la automatización.	el área proceso TIC, debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
14.3	**Datos de prueba.**			
14.3.1	Protección de los datos utilizados en pruebas.	PNP	La información utilizada en los ambientes de prueba es eliminada para evitar filtración de información	La organización protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.
15.	**RELACIONES CON SUMINISTRADORES.**			
15.1	**Seguridad de la información en las relaciones con suministradores.**			
15.1.1	Política de seguridad de la información para suministradores.	MD	Se le s informa a los proveedores y terceros, el fortalecimiento de seguridad de la información y buenas prácticas en las que está trabajando la organización hace falta fortalecer divulgando la política a los agentes implicados.	la Entidad establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	MD	Proveedores de herramientas para el alojamiento de la información, cuentan con su respectiva política de seguridad para la información. Sin embargo, los proveedores de alquiler de equipos de cómputo aún carecen de ella. Por lo cual se debe informar la de la organización y se acojan a ella.	El proceso TIC, el área Legal y el área de Seguridad de la Información deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	MD	Se realizan acuerdos de confidencialidad de acuerdo con los servicios contratados.	El proceso TIC, jurídico, deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes.
15.2	**Gestión de la prestación del servicio por suministradores.**			
15.2.1	Supervisión y revisión de los servicios prestados por terceros.	MD	Periódicamente se realiza monitoreo a los servicios prestados por terceros.	El proceso TIC, debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.
15.2.2	Gestión de cambios en los servicios prestados por terceros.	PNP	No se tiene implementado este control	los supervisores de contratos con terceros, con el apoyo del proceso TIC, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.
16.	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**			
16.1	**Gestión de incidentes de seguridad de la información y mejoras.**			

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
16.1.1	Responsabilidades y procedimientos.	MD	Se encuentran definidos a en la política de seguridad de la información y en canal para registrarlos.	la Entidad promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.
16.1.2	Notificación de los eventos de seguridad de la información.	D	El personal es capacitado para este tipo de situaciones, sin embargo, es importante reforzar en el personal la importancia de reportar los incidentes que puedan afectar la seguridad de la información para tomar acciones.	los propietarios de los activos de información deben informar lo antes posible al área de Seguridad de la Información, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.
16.1.3	Notificación de puntos débiles de la seguridad.	MD	El personal es capacitado para este tipo de situaciones, sin embargo, es importante reforzar en el personal la importancia de reportar los incidentes que puedan afectar la seguridad de la información.	En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo al proceso TIC y oficial de cumplimiento, de la Información para que se registre y se le dé el trámite necesario.
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	PNP	No se cuenta con comité de seguridad de la información, sin embargo, el proceso TIC, analiza los eventos o incidentes que se presentan para tomar medidas inmediatas.	el Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
16.1.5	Respuesta a los incidentes de seguridad.	PNP	Se cuenta con personal calificado, pero no es exclusivo para temas de seguridad. Debido a la demanda de otras actividades, la dedicación en ese tema es limitado.	El proceso TIC, debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su ocurrencia.
16.1.6	Aprendizaje de los incidentes de seguridad de la información.	RD	Los incidentes de seguridad de la información son informados en las diferentes áreas con el fin de alertar a los colaboradores y evitar incidentes mayores.	El proceso TIC, debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.
16.1.7	Recopilación de evidencias.	RD	En cada uno de los casos se recopilan las evidencias necesarias para garantizar la seguridad de la información y se lleva una trazabilidad completa de cada uno de los casos.	Es importante evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares, reuniendo las evidencias necesarias y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente.
17.	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**			
17.1	**Continuidad de la seguridad de la información.**			
17.1.1	Planificación de la continuidad de la seguridad de la información.	PNP	No se tiene implementado este control. Se encuentra en proceso.	se debe desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de la Entidad, sin disminuir los niveles de seguridad establecidos.
17.1.2	Implantación de la continuidad de la seguridad de la información.	PNP	No se tiene implementado este control. Se encuentra en proceso.	Es necesario proporcionar los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en el instituto y que afecten la continuidad de su operación.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	PNP	No se tiene implementado este control. Se encuentra en proceso.	Se debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.
17.2	**Redundancias.**			
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	PNP	No se tiene implementado este control. Se encuentra en proceso.	Se debe propender por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables.
18.	**CUMPLIMIENTO.**			
18.1	**Cumplimiento de los requisitos legales y contractuales.**			
18.1.1	Identificación de la legislación aplicable.	MD	La organización siempre busca estar alineada con las normatividad vigente, haciendo referencia a su marco de trabajo y entorno de negocio.	el área de tecnología debe identificar y velar porque el software instalado en los recursos de la plataforma tecnología cumpla con los requerimientos legales y de licenciamiento aplicables.
18.1.2	Derechos de propiedad intelectual (DPI).	D	En las actas de entrega de los equipos y en la inducción se informa a los colaboradores, también se refuerza en las campañas de concientización.	para todo el personal de la entidad es importante tener presente que deben cumplir con las leyes de derechos de autor y acuerdo de licenciamiento de software.
18.1.3	Protección de los registros de la organización.	PNP	Actualmente el proceso TIC, está en constante monitoreo de las aplicaciones como seguimiento a posibles incidente de seguridad de información. Sin embargo, es importante trabajar en capacitaciones al personal que permitan reducir aún más el riesgo.	El proceso jurídico y TIC deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Entidad, que están relacionados con los registros de la organización, para protegerlos contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados.
18.1.4	Protección de datos y privacidad de la información personal.	MD	Política definida, en proceso de implementación Sistema de Gestión para la protección de datos personales.	En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la Entidad a través del área de Seguridad de la Información, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.
18.1.5	Regulación de los controles criptográficos.	PNP	No se tiene implementado este control.	El proceso TIC debe implantar los controles criptográficos necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.
18.2	**Revisiones de la seguridad de la información.**			
18.2.1	Revisión independiente de la seguridad de la información.	PNP	Apenas se está organizando la gestión de seguridad de la información. Aplicar control.	La Entidad debe realizar revisiones periódicamente, para validar si se deben realizar actualizaciones a las políticas de seguridad. Los controles que se establezcan deben ser los que corresponden a la norma de seguridad internacional ISO 27001 y otras fuentes como COBIT, ITIL, BASILEA II, entre otros.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES				
ISO 27002 Controles	**Descripción**	**Status**	**Estado u Observaciones**	**Recomendaciones**
18.2.2	Cumplimiento de las políticas y normas de seguridad.	D	Aunque las políticas están definidas para el tratamiento de información, es importante tener claro que cualquier persona que no tenga el acompañamiento necesario dentro de la compañía en temas de seguridad de la información, puede incumplir con las políticas y normas establecidas. Se debe fortalecer continuamente.	Los diferentes aspectos contemplados en este documento de políticas de seguridad son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores de la Entidad.
18.2.3	Comprobación del cumplimiento.	D	A través de auditorías a los procesos, se comprueba que se esté cumpliendo con las políticas establecidas de seguridad, y adicional se retroalimenta las inconsistencias evidenciadas en el proceso. Es importante tener presente que el personal no solo debe acatar las políticas por las auditorias, sino que también hace parte de sus deberes como funcionarios de la compañía.	el área de Control Interno debe revisar periódicamente los registros de auditoría de la plataforma tecnológica y los sistemas de información con el fin de identificar cumplimiento de las políticas y normas de seguridad dispuestas por la información de la organización.

Fuente: El autor.

9.4 RESUMEN DE LA DECLARACIÓN DE APLICABILIDAD (SOA)

Resumen del estado actual de la declaración de aplicabilidad, se puede observar en las tablas 15 y 16, el porcentaje de los diferentes dominios de control, en los cuales se debe profundizar el trabajo para alcanzar la meta de cumplimiento o por lo menos obtener un porcentaje apropiado de gestión. Se evidencia que trece controles se encuentran por debajo del 50% de conformidad.

Tabla 15. Resumen general del estado actual de la Declaración de Aplicabilidad SoA

Etapa de Determinación de la ISO 27002 - Controles					
Referencia	Proceso Cumple con la norma y está documentado	Proceso se lleva a cabo y se debe documentar	Proceso no cumple con la norma y debe ser rediseñado	Proceso no está en su lugar / no está implementado	Proceso no es aplicable
ISO Controles	26	43	8	34	3

Tabla 16. Resumen de conformidad del estado actual de la Declaración de Aplicabilidad SoA

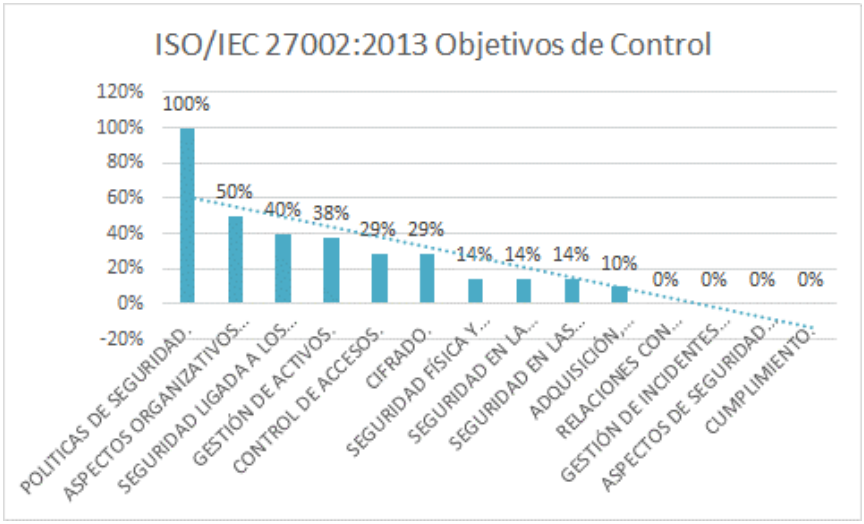
Estado Adecuación Implementación ISO 27002 vs Objetivos de Control				
	ISO/IEC 27002:2013 Objetivos de Control	Cantidad	Conformidad %	Meta
5.	POLITICAS DE SEGURIDAD.	2	100%	100%
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	1	50%	100%
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	3	40%	100%
8.	GESTIÓN DE ACTIVOS.	1	38%	100%
9.	CONTROL DE ACCESOS.	4	29%	100%
10.	CIFRADO.	0	29%	100%
11.	SEGURIDAD FÍSICA Y AMBIENTAL.	6	14%	100%
12.	SEGURIDAD EN LA OPERATIVA.	4	14%	100%
13.	SEGURIDAD EN LAS TELECOMUNICACIONES.	1	14%	100%
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	0	10%	100%
15.	RELACIONES CON SUMINISTRADORES.	0	0%	100%
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	1	0%	100%

Estado Adecuación Implementación ISO 27002 vs Objetivos de Control				
	ISO/IEC 27002:2013 Objetivos de Control	Cantidad	Conformidad %	Meta
17.	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	0	0%	100%
18.	CUMPLIMIENTO.	3	0%	100%

Fuente: El autor.

De acuerdo con el resumen obtenido de la declaración de aplicabilidad, se evidencia en la figura 26, que el único objetivo de control que cumple con las expectativas por encima del 80% es el de políticas de seguridad, debido al trabajo realizado en este proyecto aplicado, en los demás objetivos de control se evidencia un nivel por debajo del 50%. Esta grafica permite observar que se debe ejecutar un plan de acción inmediato.

Figura 26. Estado de implementación objetivos de control ISO 27002:2013



Fuente: El autor

9.5 DEFINICIÓN DE PROYECTOS E INICIATIVAS (SALVAGUARDAS)

De acuerdo con el Instituto Nacional de Ciberseguridad de España, son las medidas necesarias para proteger la información de una organización, un aspecto importante a considerar en la selección e implantación de controles es su tipología o naturaleza, esta puede ser:

- Técnica: Medidas de carácter tecnológico dentro del ambiro de seguridad (antivirus, cortafuegos, sistemas de copias de seguridad, entre otros).
- Organizativa: Medias que se centran en la mejora de la seguridad teniendo en cuenta a las personas (Capacitación, asignación de responsabilidades, procedimientos formales).
- Física: Medidas físicas para proteger la información (acondicionar datacenter o cuarto de servidores frente a riesgos de incendio, inundación, accesos no autorizados, controles de acceso físico, entre otros.
- Legales: Persiguen el cumplimiento legal al que está sujeta la organización en el ámbito de la seguridad de la información.[76]

Teniendo en cuenta la anterior descripción y a partir del proceso que se ha venido realizando (análisis del estado actual de la organización, el análisis del riesgo y la declaración de aplicabilidad) se definen las siguientes iniciativas y proyectos necesarios para alcanzar el nivel de seguridad que Cibjo SAS BIC requiere. En la tabla 17. Se establecen las convenciones para el avance de los planes propuestos a mediano y corto plazo.

[76] INCIBE. Instituto nacional de Ciberseguridad. Protección de la Información.

Tabla 17. Convenciones de estado proyectos e iniciativas Cibjo SAS BIC.

Convenciones
Realizado
Avance
No programado.
Planeado

Fuente: El autor.

A continuación, se presentan los proyectos propuestos para fortalecer la seguridad de la información de Cibjo SAS BIC, en la tabla 18. Adicional se incluye una breve descripción del riesgo de no implementarse, presupuesto, tiempo estimado de ejecución por semestre, responsable de la ejecución y los entregables.

Tabla 18. Proyectos e iniciativas para mejorar la seguridad de la información de la empresa Cibjo SAS BIC.

ID	PROYECTO	DESCRIPCIÓN	RIESGO ACTUAL	PRESUPUESTO	TIEMPO DE EJECUCCIÓN 2023 -2024				RESPONSABLE	ENTREGABLES
					S1	S2	S3	S4		
1	Implementar y robustecer políticas de seguridad específicas.	Fortalecer las buenas prácticas de seguridad de la información mediante la implementación de políticas específicas.	Brechas de seguridad por malas prácticas para el manejo de la información.	$ 0					Especialista de Seguridad Informática.	Implementación de políticas de seguridad específicas y actualización cuando se requiera y periódicamente. Fortalecer con: *Utilización de dispositivos móviles. *Uso de redes wifi y redes externas. *Teletrabajo seguro. *Respuesta a incidentes. *Relación con proveedores. *Dispositivos móviles no corporativos. *Copias de seguridad. *Continuidad de negocio. *Clasificación de la información. *Borrado seguro. *Buenas prácticas en redes sociales. *Gestión de logs. *Uso de técnicas criptográficas.

ID	PROYECTO	DESCRIPCIÓN	RIESGO ACTUAL	PRESUPUESTO	TIEMPO DE EJECUCCIÓN 2023 -2024				RESPONSABLE	ENTREGABLES
					S1	S2	S3	S4		
2	Continuar con respaldo de información Histórica	Salvaguardar información almacenada en discos externos	Perdida de información por daño en medios físicos.	$ 10.000.000					Especialista S.I. Coordinador TIC Auxiliar TIC.	Plan de trabajo, seguimiento a la carga de información histórica. Cargar información histórica en la nube.
3	Concienciación en materia de seguridad de la información a toda la organización.	Sesiones de formación para la toma de conciencia por parte de todos los colaboradores.	Brechas de seguridad por malas prácticas para el manejo de la información. Incidentes de seguridad de la información.	$ 0					Especialista S.I.	Desarrollo de cultura en Seguridad por medio de: Infografías, videos, casos reales, capacitaciones, charlas, inducción, etc.
4	Plan de continuidad de Negocio.	Herramientas para copias de seguridad automáticas de información en SharePoint y WorkSpace en la nube como: Arcserve o Acronis Ciber Project Cloud. (Permite respaldar continuamente las herramientas de office 365 (Exchange, OneDrive, SharePoint, Teams, WorkSpace) Con una sola cuenta puede gestionar el respaldo en los sitios que tenga acceso el administrador del Tenant.	Perdida de información por indisposición del servicio de office 365 y WorkSpace.	$ 10.000.000					Especialista S.I. con apoyo del Coordinador TIC.	Plan de trabajo para el respaldo de información en caliente. Respaldo de información. Documentación. Monitoreo. Pruebas de funcionalidad.
5	Clasificación y tratamiento de la información sensible y confidencial en Office 365	*Configuración del portal de cumplimiento Microsoft office 365.	Exposición de información sensible o confidencial.	$ 7.000.000					Especialista S.I.	Clasificación y etiquetado de la información alojada en SharePoint en colaboración con los usuarios de la organización. (Público, General, Confidencial, Extremadamente confidencial). Esto permite realizar acciones correctas en el contenido adecuado. Identificar la confidencialidad de los datos en toda la organización para aplicar la configuración de protección adecuada de esos datos.
6	Prevención de Perdida de Datos (DLP) en Office 365	Configuración de directivas para la prevención de perdida de datos.	Perdida de información por manipulación de datos de los usuarios.	$ 8.000.000					Especialista S.I.	Data Loss Prevention (prevención de pérdida de datos) garantiza que los usuarios no envíen información delicada o crítica fuera de la red corporativa. Configuración de directivas para la prevención de perdida de datos, permite: identificar, supervisar y proteger automáticamente elementos confidenciales.

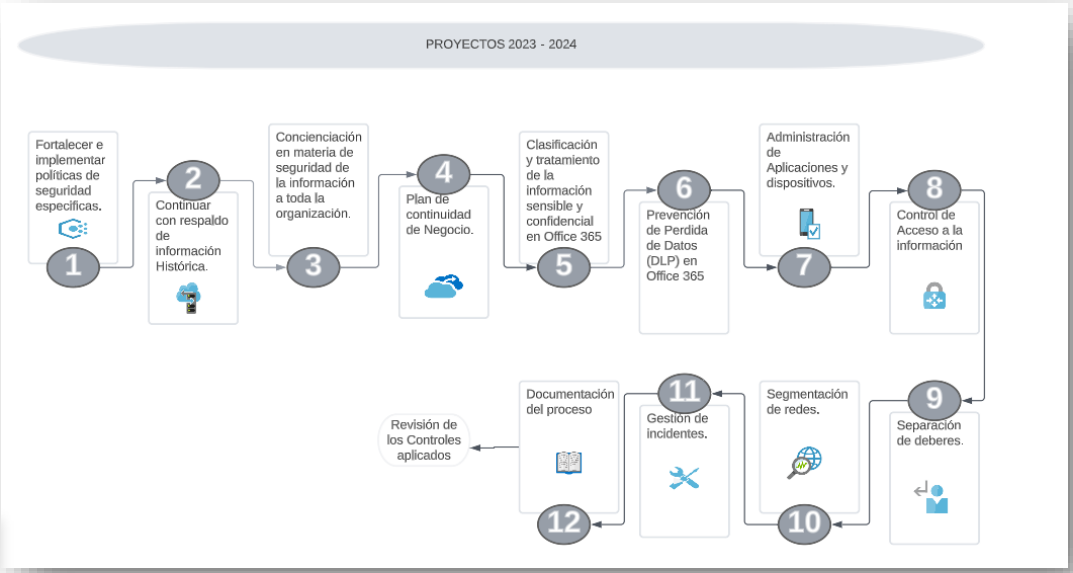
ID	PROYECTO	DESCRIPCIÓN	RIESGO ACTUAL	PRESUPUESTO	TIEMPO DE EJECUCCIÓN 2023 -2024				RESPONSABLE	ENTREGABLES
					S1	S2	S3	S4		
7	Administración de Aplicaciones y dispositivos.	Configuración de identidades y políticas de Azure Active Directory.	Robo, filtración de información por uso de dispositivos no permitidos.	$ 10.000.000					Especialista S.I.	Implementación de: * Único inició de sesión en los dispositivos (Mismo usuario y contraseña en cuenta de office 365 y en el dispositivo). *Configuración de autenticación multifactor para toda la organización. *Directiva de riesgo de inicio de sesión (Bloqueo si detecta riesgo). *Administrar usuarios y dispositivos en conjunto y no por separado. *Configuración de alertas y supervisión.
									Coordinador TIC. Auxiliar TIC	Aplicar la configuración en las cuentas de usuario y dispositivos. Reportar correcto funcionamiento o incidencias.
8	Control de Acceso a la información	Implementación de matriz de acceso para office 365 y WorkSpace de Google (Información histórica digital).	Accesos sin control, información expuesta.	$ 0					Especialista S.I. con apoyo del equipo TIC.	Matriz de acceso: (Implementación de herramienta que permite conocer y administrar los accesos y los permisos que los colaboradores tienen a la información de la empresa para limitar los accesos y proteger la información.
9	Separación de deberes.	Control de todas las herramientas y plataformas de la organización.	Modificación no autorizada o intensional en la información de la organización. Conflicto de intereses.	$ 0					Especialista S.I.	Configuración del Mínimo privilegio permitido a los usuarios en las diferentes herramientas de la organización (ejemplo: Siigo). Un solo administrador en toda la organización. Requiere entrenamiento.
10	Segmentación de redes.	Configuración de Vlan para segmentar: *Red corporativa de visitantes. *Entonos de prueba. *Entornos de respaldo o copias de seguridad.	Ciberataque por conexión inalámbrica. Robo de información.	$ 7.000.000					Especialista S.I. Jefe de Infraestructura.	Establece directrices de configuración y monitoreo. Configuración de red para invitados en Elemento. Expandir configuración a los nuevos proyectos implementados en las diferentes ubicaciones. Configuración de VLAN (Segmento a parte para copias de seguridad). Configuración y limitación de puertos. Diagramas de red y documentación de arquitectura de red.
11	Gestión de incidentes.	Desarrollar e implementar procedimientos que permitan: Detectar, evaluar, solucionar y tratar incidentes de seguridad de la información.	Negligencia ante un incidente de ciberseguridad.	$ 8.000.000					Especialista S.I. con apoyo del equipo TIC.	Implementación de Modelo de Gestión de Incidentes de Seguridad de la información para manejar adecuadamente los incidentes (Preparación, detección y análisis, contención y recuperación, actividades post-incidente).

ID	PROYECTO	DESCRIPCIÓN	RIESGO ACTUAL	PRESUPUESTO	TIEMPO DE EJECUCCIÓN 2023 -2024				RESPONSABLE	ENTREGABLES
					S1	S2	S3	S4		
12	Documentación del proceso.	Documentar los procesos técnicos y administrativos que se llevan a cabo dentro de la operación de tecnología. (TIC y Seguridad).	Procesos desorganizados, errores operativos.	$ 0					Especialista S.I. con apoyo del equipo TIC.	Información documentada de procedimientos, instructivos, formatos de TIC y Seguridad de la Información.
	Recurso Humano (Especialista de Seguridad Informática).	Formula políticas de seguridad informática, específicas y actualizaciones. *Documenta guías de trabajo y procedimientos de seguridad informática. * Identificar y gestionar riesgos de seguridad. *Diseñar estrategias y sistemas defensivos contra intrusos. *Implementa medidas preventivas y correctivas de incidentes. *Trabaja en colaboración con el proceso técnico (TIC) para asegurar que la tecnología, procesos y las capacidades de los usuarios estén alineadas para prevenir riesgos y corregir incidentes oportunamente.		$ 144.000.000					Especialista S. I	Estrategia y directrices de Seguridad de la información. Monitoreo y pruebas de los controles implementados. Mejora continua.
		Total		$ 204.000.000						

Fuente: El autor.

A continuación, en la figura 27, se presenta gráficamente los proyectos relacionados anteriormente, mediante una hoja de ruta, de una forma más sencillas de visualizar para la ejecución en el transcurso de 24 meses, donde se pretende mitigar los riesgos detectados.

Figura 27. Hoja de ruta



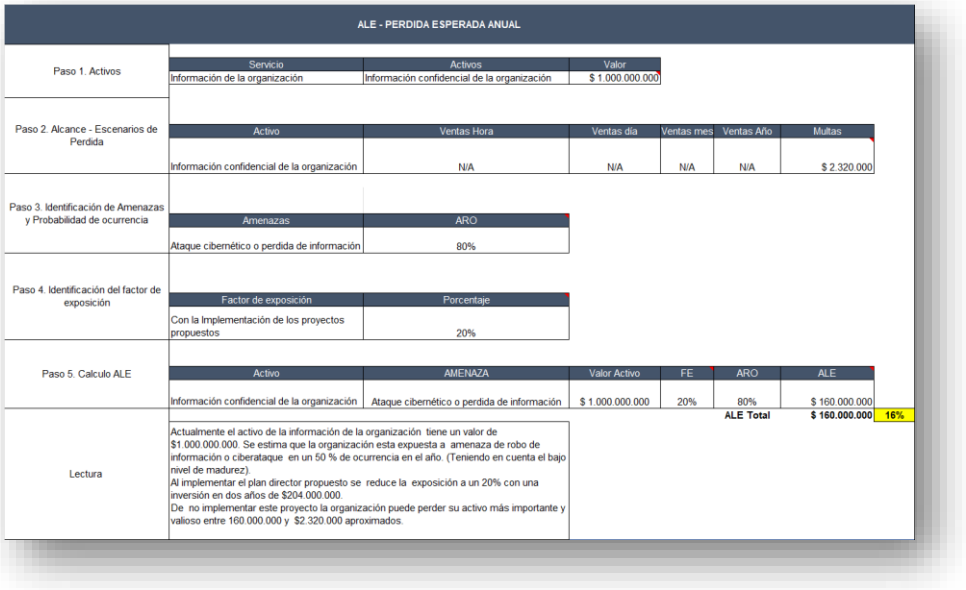
Fuente: El autor.

10 SUSTENTACIÓN DE PROYECTOS E INICIATIVAS PROPUESTOS

10.1 PERDIDA ESPERADA ANUAL

En esta etapa se hace un análisis para sustentar la inversión de los proyectos planteados. Como se ve reflejado en la figura 28, actualmente el activo de la información de la organización tiene un valor de $1.000.000.000. Se estima que está expuesta a amenazas que pueden vulnerar de robo de información o ciberataque en un porcentaje de 80 % de ocurrencia en el año. (Teniendo en cuenta el bajo nivel de madurez y el porcentaje de riesgo calculado). Al implementar el plan director propuesto se reduce la exposición a un 20% por un valor de $204.000.000 para dos años, es decir $101.000.000 anual. De no implementar este proyecto la organización puede perder su activo más importante estimado entre $160.000.000 y $1.000.000.000, peor aún puede sufrir millonarias multas, dependiendo de la gravedad del incidente presentado,

Figura 28. ALE – Perdida Esperada Anual.



ALE - PERDIDA ESPERADA ANUAL

Paso 1. Activos

Servicio	Activos	Valor
Información de la organización	Información confidencial de la organización	$ 1.000.000.000

Paso 2. Alcance - Escenarios de Perdida

Activo	Ventas Hora	Ventas día	Ventas mes	Ventas Año	Multas
Información confidencial de la organización	N/A	N/A	N/A	N/A	$ 2.320.000

Paso 3. Identificación de Amenazas y Probabilidad de ocurrencia

Amenazas	ARO
Ataque cibernético o perdida de información	80%

Paso 4. Identificación del factor de exposición

Factor de exposición	Porcentaje
Con la Implementación de los proyectos propuestos	20%

Paso 5. Calculo ALE

Activo	AMENAZA	Valor Activo	FE	ARO	ALE
Información confidencial de la organización	Ataque cibernético o perdida de información	$ 1.000.000.000	20%	80%	$ 160.000.000
				ALE Total	**$ 160.000.000** **16%**

Lectura

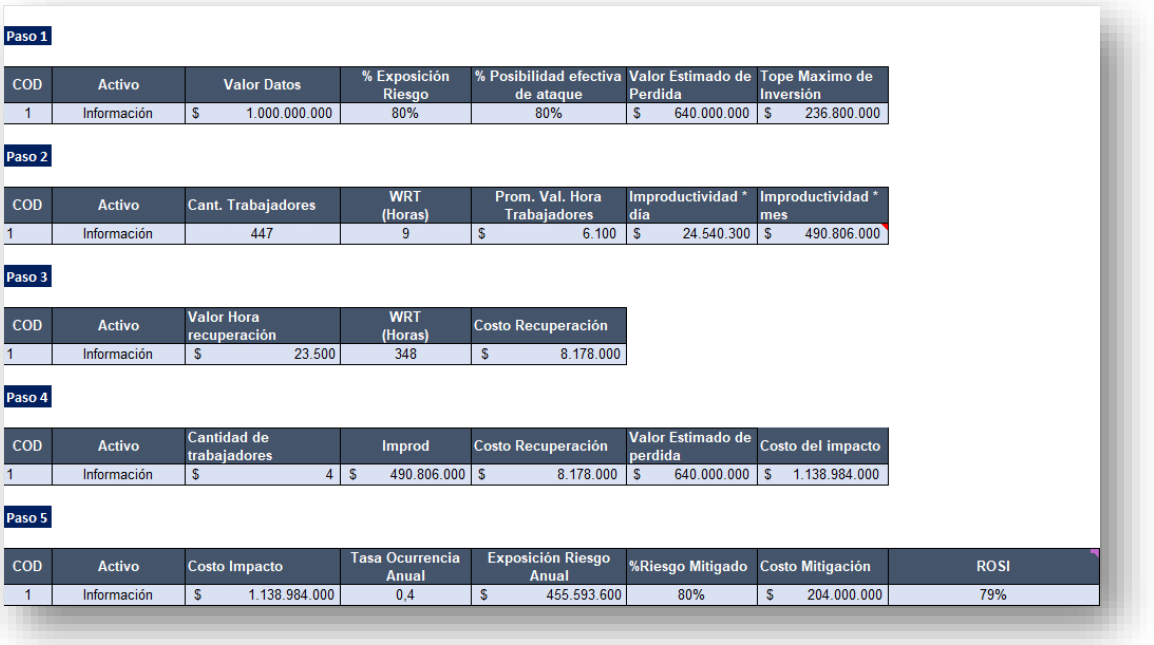
Actualmente el activo de la información de la organización tiene un valor de $1.000.000.000. Se estima que la organización esta expuesta a amenaza de robo de información o ciberataque en un 50 % de ocurrencia en el año. (Teniendo en cuenta el bajo nivel de madurez).
Al implementar el plan director propuesto se reduce la exposición a un 20% con una inversión en dos años de $204.000.000.
De no implementar este proyecto la organización puede perder su activo más importante y valioso entre 160.000.000 y $2.320.000 aproximados.

Fuente: El autor.

10.2 ROSI – RETORNO SOBRE LA INVERSIÓN

De acuerdo con Locher “se determina que una inversión en seguridad es rentable si el efecto de mitigación del riesgo es mayor que los costos estimados”[77]. En la figura 29, se observa el cálculo del retorno sobre la inversión, contemplando aspectos importantes a considerar, entre ellos el valor del activo de la información, el valor estimado de la perdida, el valor de la improductiva de los colaboradores (tomando salarios básicos, costo de recuperación aproximado, estimando cuatro ingenieros dedicados durante dos meses, costo del impacto, sumando la improductividad + costo de recuperación + valor estimado de perdida y por último en el paso cinco obtenemos el ROSI con un 79% de retorno para este proyecto.

Figura 29. ROSI – Retorno sobre la inversión.



Paso 1

COD	Activo	Valor Datos	% Exposición Riesgo	% Posibilidad efectiva de ataque	Valor Estimado de Perdida	Tope Maximo de Inversión
1	Información	$ 1.000.000.000	80%	80%	$ 640.000.000	$ 236.800.000

Paso 2

COD	Activo	Cant. Trabajadores	WRT (Horas)	Prom. Val. Hora Trabajadores	Improductividad * día	Improductividad * mes
1	Información	447	9	$ 6.100	$ 24.540.300	$ 490.806.000

Paso 3

COD	Activo	Valor Hora recuperación	WRT (Horas)	Costo Recuperación
1	Información	$ 23.500	348	$ 8.178.000

Paso 4

COD	Activo	Cantidad de trabajadores	Improd	Costo Recuperación	Valor Estimado de perdida	Costo del impacto
1	Información	$ 4	$ 490.806.000	$ 8.178.000	$ 640.000.000	$ 1.138.984.000

Paso 5

COD	Activo	Costo Impacto	Tasa Ocurrencia Anual	Exposición Riesgo Anual	%Riesgo Mitigado	Costo Mitigación	ROSI
1	Información	$ 1.138.984.000	0,4	$ 455.593.600	80%	$ 204.000.000	79%

Fuente: El autor.

[77] LOCHER C. Methodologies for Evaluating Information Security Investments - What Basel II Can Change in the Financial Industry.

10.3 ACTA DE APROBACIÓN DE PLAN DIRECTOR DE SEGURIDAD

Mediante la presente acta y en condición de Coordinador TIC, en la organización, Cibjo SAS BIC, entendiendo la importancia de garantizar los principios básicos de la información (integridad, disponibilidad, confidencialidad), una vez analizado el contexto de la organización, los riesgos operacionales, organizacionales, se presenta un breve resumen, en la tabla 19, de los proyectos a implementar para mitigar el riesgo, identificado como inaceptable. Los cuáles serán ejecutados en un tiempo de dos años. En algunos proyectos relacionados, el valor es cero, no quiere decir que no tenga valor, si no que, al ser elaborados por el especialista dedicado a esta labor, el presupuesto estaría inmerso en el salario de ese cargo.

Tabla 19. Resumen Proyectos e iniciativas

ID	PROYECTO	PRESUPUESTO
1	Implementar y robustecer políticas de seguridad específicas.	$ 0
2	Respaldo de información Histórica	$ 10.000.000
3	Concienciación en materia de seguridad de la información a toda la organización.	$ 0
4	Plan de continuidad de Negocio.	$ 10.000.000
6	Prevención de Perdida de Datos (DLP) en Office 365	$ 8.000.000
7	Administración de Aplicaciones y dispositivos.	$ 10.000.000

ID	PROYECTO	PRESUPUESTO
8	Control de Acceso a la información	$ 0
9	Separación de deberes.	$ 0
10	Segmentación de redes.	$ 7.000.000
11	Gestión de incidentes.	$ 8.000.000
12	Documentación del proceso.	$ 0
	Recurso Humano (Especialista de Seguridad Informática).	$ 144.000.000
	Total	**$ 204.000.000**

Fuente: El autor.

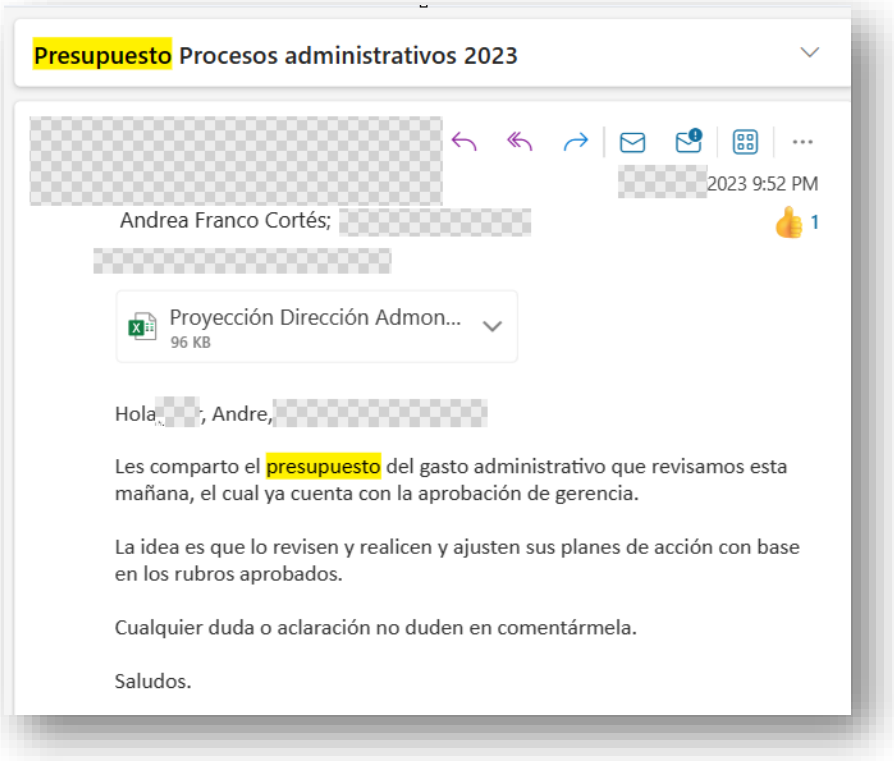
Con la implementación de los anteriores proyectos, se establecerá, indicadores de medición, para evaluar periódicamente la eficacia de los controles aplicados. Adicional se deben realizar auditorías para evaluar la eficacia para la mejora continua.

Firma la presente acta de aceptación, la Gerencia General de Cibjo SAS BIC.
en Bogotá D.C., a los (17) días del mes de (07) de 2023.

_____
Dana Nora Oñatsac
Gerente General Cibjo SAS BIC
C.C. No. 50108403 de Bogotá

Una vez presentado el plan director de seguridad a la alta dirección de la organización Cibjo SAS BIC, la directora administrativa envió por medio del correo electrónico el presupuesto aprobado por la gerencia para el proceso Administrativo, del cual el área de tecnología hace parte. En la figura 30. Se observa la evidencia, a un que para mantener la confidencialidad de la información se distorsiona los nombres y detalles que comprometen a la organización.

Figura 30. Evidencia de aprobación de presupuesto para proyectos propuestos.



Fuente: El autor.

11 CONCLUSIONES

Se identifico que la empresa colombiana Cibjo SAS BIC, carece de controles y buenas prácticas de gestión de seguridad informática para garantizar las características fundamentales de la información. En análisis realizado, es un avance importante, permite a la organización tener claro el punto de partida y conocer los riesgos a los que se expone la organización, tomar medidas inmediatas que mitiguen el riesgo.

Con la implementación del inventario de activos, se concluye que el 33% de activos de la organización son de tipo datos y el 28% de servicios (Software as a service e Infraestructura as a service). Lo que indica que más del 50% de los activos de la son intangibles y el 63% de los activos se encuentran en riesgo inaceptable por lo que urge, establecer un plan de tratamiento del riesgo de manera prioritaria. A su vez se identifica que la aplicación de la metodología Magerit en la empresa Cibjo SAS BIC, permite una adecuada gestión de riesgo contemplando, diferentes aspectos de la tecnología de la información, permitiendo identificar sus activos, evaluarlos, descubrir sus vulnerabilidades para establecer un tratamiento oportuno.

Se concluye que el plan director de seguridad permitirá concentrar los esfuerzos para lograr el objetivo de nivel de madurez 4, donde los procesos se miden y monitorean. De acuerdo con la declaración de aplicabilidad, se requiere documentar el 38% de los procesos del área de tecnología, implementar el 30% de controles y buenas prácticas, basados en la norma ISO 27002:2013

Se concluye que la inversión global de $204.000.000 para proyectos a ejecutar en 24 meses, es relativamente baja, la inversión es de un 20% del valor total de sus activos, por el contrario de no realizarlo, la organización podría tener pérdidas millonarias, posiblemente superiores a su capital, la organización puede mejorar significativamente, simplemente fortaleciendo los temas organizativos y asignando

recurso humano especializado, con una dedicación del 100%, es allí donde la organización presenta falencias al sobrecargar funciones, limitando el rol estratégico, enfocados a la operatividad de la Gerencia TI.

12 RECOMENDACIONES

Se le recomienda a la organización, realizar evaluaciones y pruebas de seguridad de la información con la Metodología NIST (800-115), proceso organizado, planificado, estableciendo alcance, una política para evaluaciones, contemplando los riesgos de ese proceso, informando a la alta dirección los activos objetivos a evaluar, así como los proveedores en los que se tenga alojado los servicios, herramientas a emplear, tipos de pruebas, ¿quién y donde los realizará? acuerdo de confidencialidad de los datos, manejo de incidentes, actividades prohibidas y por ultimo autorización de la organización. Esto permite ir más allá de los hallazgos, obtenidos en entrevistas.

Establecer el Modelo Zero Trust (Cero Confianza) basado en el menor privilegio permitido, forzar a controles de acceso estrictos, inspeccionar y revisar todo. Permitiendo asegurar datos, equipos, sistemas, independientemente de su ubicación. Esto debido a que un gran porcentaje de sus activos se encuentran alojados en la nube y la organización cuenta con la modalidad teletrabajo para sus colaboradores.

Se recomienda a la organización Cibjo SAS, realizar seguimiento y medición periódica por lo menos cada tres meses a los controles implementados, con el fin de analizar y validar el progreso.

Se recomienda a la organización, en definitiva, implementar un proceso o Sistema de Gestión para Seguridad de la información, el cual trabaje mancomunadamente con el proceso TIC, pero con la segmentación y organización de roles, responsabilidades y funciones.

BIBLIOGRAFÍA

ALCALDIA MAYOR DE BOGOTA D.C. Guardianes de la Información. Penetración Testing. Estrategia de Seguridad y privacidad de la información de la Alcaldía de Bogotá. Bogotá D.C: 2018, [Consultado el 14 de marzo de 2023].

ÁLVAREZ MARAÑON, Gonzalo. Seguridad informática para empresas y particulares. [digital]. España: McGraw-Hill, 2004. 442p. [Consultado el 20 de agosto de 2021].

BACA URBINA. Gabriel. Introducción a la seguridad informática. [en línea]. Primera Edición. México: Patria, 2016. 361p. [Consultado el 05 de septiembre de 2021]. Disponible en: E Libro (unad.edu.co)

BIN AZAD, Tariq. Introdution to security. Definig vulnerability. ScienceDirect. [online]. [Consulted on september 29, 2023]. Available in: Technical Vulnerability - an overview | ScienceDirect Topics

CATOIRA, Fernando. Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit framework. Revista seguridad. Cultura de prevención para TI. Revista bimestral. (2013: México) nro. 19. [Consultado el 04 de octubre de 2023]. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

CIBJO SAS BIC. Política de Seguridad de la Información y Ciberseguridad. Versión 1. [digital]. 2023. 12 p. [Consultado el 17 de marzo de 2023]. Disponible en: Información confidencial de la organización.

CIBJO SAS BIC. Informe de Gestión BIC. [digital]. 2022. 107 p. [Consultado el 17 de marzo de 2023]. Disponible en: Información confidencial de la organización.

DAWSON, M. et al. Examining the Role of the Chief Information Security Officer (Ciso) & Security Plan. Journal of Information Systems Technology & Planning, [s. l.], v. 3, n. 6, p. 1–5, 2010. [Consultado el 11 de octubre de 2023]. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=aci&AN=63283579&lang=es&site=ehost-live.

EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. [en línea]. Bogotá: (29 de octubre del 2019). p. 4 – 7. [Consultado el 15 de septiembre de 2021]. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/#:~:text=Actualmente%2C%20el%2045.5%25%20de%20las,sido%20denunciados%20ante%20la%20fiscal%C3%ADa.

ESCRIVÁ GASCO. Gema. Seguridad informática. Macmillan. p. 218p. [digital]. [Consultado el 18 de agosto de 2021].

ICONTEC. Norma Técnica Colombiana NTC-ISO 31000. Gestión del Riesgo Principios y Directrices. [Libro Digital] Bogotá. (22 de febrero de 2011). p.3. [Consultado el 01 de abril de 2023].

ISMS.ONLINE. ISO 27001 Annex A.12.1 Operational procedures and responsabilities. [online]. [Consulted on september 26, 2023]. Available in: https://www.isms.online/iso-27001/annex-a-12-operations-security/

IRWIN L. ISO 21001 Annex A controls explained. [online]. 2023 [Consulted on september 29, 2023]. Available in: ISO 27001 Annex A Controls - A Complete Guide (itgovernance.co.uk)

KASPERSKY. ¿Qué es la inyección de SQL? Definición y explicación [Sitio web]. [Consultado el 04 de octubre 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/sql-injection

LOCHER C. Methodologies for Evaluating Information Security Investments - What Basel II Can Change in the Financial Industry. [online]. 2005. ECIS 2005 Proceedings. 122 [Consulted on september 29, 2023]. Available in: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1136&context=ecis2005

MANDIANT. M-Trends 2023. Mandiant Special Report. [en línea]. 2023, 108 p. [Consultado el 12 de mayo de 2023]. Disponible en: Threat Intelligence Solutions | Cyber Security Services & Training (mandiant.com)

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Magerit – Versión 3.0. Methodology for Information Systems Risks Analysis and Management. Book I – The Method. [Digital Book] Madrid. (12 the October the 2012). p.7 -127. Electronic Administration Collection. NIPO: 630-12-171-8. [Consultado el 28 de marzo de 2023].

NMAP. Nmap: Discover your network. [Sitio web]. [Consultado el 04 de octubre 2023]. Disponible en: https://nmap.org/

GALLARDO URBINI Ignacio Martin, et al. Distributed Cybersecurity Strategy, applying the Intelligence Operations Theory. CISTI (Iberian Conference on

Information Systems & Technologies. [on line]. (22 - 25 JUNE, 2022: Madrid, Spain). [cited 19 Jul 2023]; (17):1–6. Available from: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=aci&AN=162319475&lang=es&site=ehost-live

ISO270001. Norma ISO 27001. ISO27002. [sitio web]. [Consultado el 18 de noviembre de 2023]. Disponible en: https://normaiso27001.es/

GÓMEZ VIEITES. Álvaro. Gestión de incidentes de seguridad informática. [digital]. Madrid: RA-MA, 2015. 124p. [Consultado el 19 de septiembre de 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/62467

INCIBE. Instituto nacional de Ciberseguridad. ¿Qué es el Pentesting?: Auditando la seguridad de tus sistemas. España Digital [en línea]. (04 de julio de 2019). [Consultado el 18 de marzo de 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

INCIBE. Plan director Seguridad. España Digital [en línea]. [Consultado el 19 de marzo de 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

INCIBE. ¿Sabes cómo mejorar la ciberseguridad de tu organización? Implanta un Plan director de Seguridad. [en línea]. [Consultado el 14 de octubre de 2023]. Disponible en: https://www.incibe.es/empresas/blog/sabes-mejorar-ciberseguridad-tu-organizacion-implanta-plan-director

INCIBE. Protección de la Información. [en línea]. [Consultado el 14 de octubre de 2023]. Disponible en:

https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

ISO27000. SGSI. [Sitio web]. [Consultado el 01 de octubre de 2021] Disponible en: https://www.iso27000.es/iso27002.html

ISO27000. ISO 27001. [Sitio web]. [Consultado el 16 de abril de 2023] Disponible en: https://normaiso27001.es/

JAY GONZALEZ Joaquín, KEMP L. Roger. Cybersecurity : Current Writings on Threats and Protection. [online]. (2019): Jefferson, North Carolina: McFarland). ISBN 9781476674407 [cited 20 Sep 2023]; pag.96. Available from: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=e000xww&AN=2011624&lang=es&site=ehost-live.

NIST. Technical Guide to Information Security Testing and Assessment [en línea]. Gaithersburg: 2008, [Consultado el 30 de octubre de 2022]. Disponible en: https://www.infoplc.net/plus-plus/tecnologia/item/110021-ciberseguridad-un-plan-resilencia-empresa-industrial
Technical guide to information security testing and assessment (nist.gov)

KALI. The most advanced penetration testing distribution. [Sitio web]. [Consultado el 03 de octubre 2023]. Disponible en: https://www.kali.org/

KALI. Zaproxy. Tool documentation. [Sitio web]. [Consultado el 04 de octubre 2023]. Disponible en: https://www.kali.org/tools/zaproxy/

KALI. Hydra. [Sitio web]. [Consultado el 04 de octubre 2023]. Disponible en: https://www.kali.org/tools/hydra/

PALACIOS GALLARDO, Margaret Lesly. Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la empresa DEVHUAYRA SAC Huancayo. [en línea]. Trabajo de investigación para Grado Académico de Bachiller en Ingeniería de Sistemas e Informática. Huancayo, Perú. Universidad Continental. Facultad de Ingeniería. Escuela Académico Profesional de Ingeniería de Sistemas e Informática, 2021. 98 p. [Consultado el 15 de marzo de 2023]. Disponible en: https://repositorio.continental.edu.pe/bitstream/20.500.12394/9560/4/IV_FIN_103_TI_Palacios_Gallardo_2021.pdf

PERFORCE. Secure Coding Standards Best Practices. A guide to security in software development [online]. [Consultado el 01 de marzo de 2023]. Disponible en: https://www.perforce.com/p/kw/success/secure-coding-standards-guide

SAFECOM. Guide to Getting Started with a Cybersecurity Risk Assessment. [en línea]. pp. 5. [Consultado el 19 septiembre de 2023]. Disponible en: https://www.cisa.gov/sites/default/files/2023-02/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508-r1.pdf

SANTACRUZ ESPINOSA, Julio Jhovany, et al. Sistema cobit en los procesos de auditorías de os sistemas informáticos. *Journal of science and research: Revista ciencia e investigación.* 2017, nro. 2, pp. 1- 4. [Consultado el 01 de agosto de 2023]. ISSN. 2528-8083. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7344282

TENABLE. Tenable Nessus. [Sitio web]. [Consultado el 04 de octubre 2023]. Disponible en: https://es-la.tenable.com/products/nessus

UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización Seguridad Informática. Administración del Riesgo. [Matriz digital]. (julio de 2022). [Consultado el 18 de marzo de 2023].

URIBE RAYAS. Edgar Felipe. Proceso para la Definición de Servicios Iniciales en un equipo de Respuesta ante Incidencias de Seguridad informática (CSIRT). [en línea]. Zacatecas, 2014, 211p. Tesis de grado (Maestro en Ingeniería de Software). Centro de Investigación en Matemáticas, A.C. [Consultado el 01 de octubre de 2021] Disponible en: deurregof.pdf (unad.edu.co)

VANEGAS GARZÓN, Jair Hernando. Guía de auditoría basada en el análisis de riesgos a un centro de datos aplicando la metodología Magerit 3. [en línea]. Bogotá, Colombia. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Auditoría de Sistemas de Información, 2017. 168 p. [Consultado el 05 de octubre de 2021]. Oracle. Disponible en: content (ucatolica.edu.co)

VIRTUALBOX. Welcome to VirtualBox.org. [Sitio web]. [Consultado el 03 de octubre 2023]. Disponible en: https://www.virtualbox.org

WHOIS. Welcome to Who.is. [Sitio web]. [Consultado el 04 de octubre 2023]. Disponible en: https://who.is/faq

ANEXOS

Anexo A. Modelo de Madurez

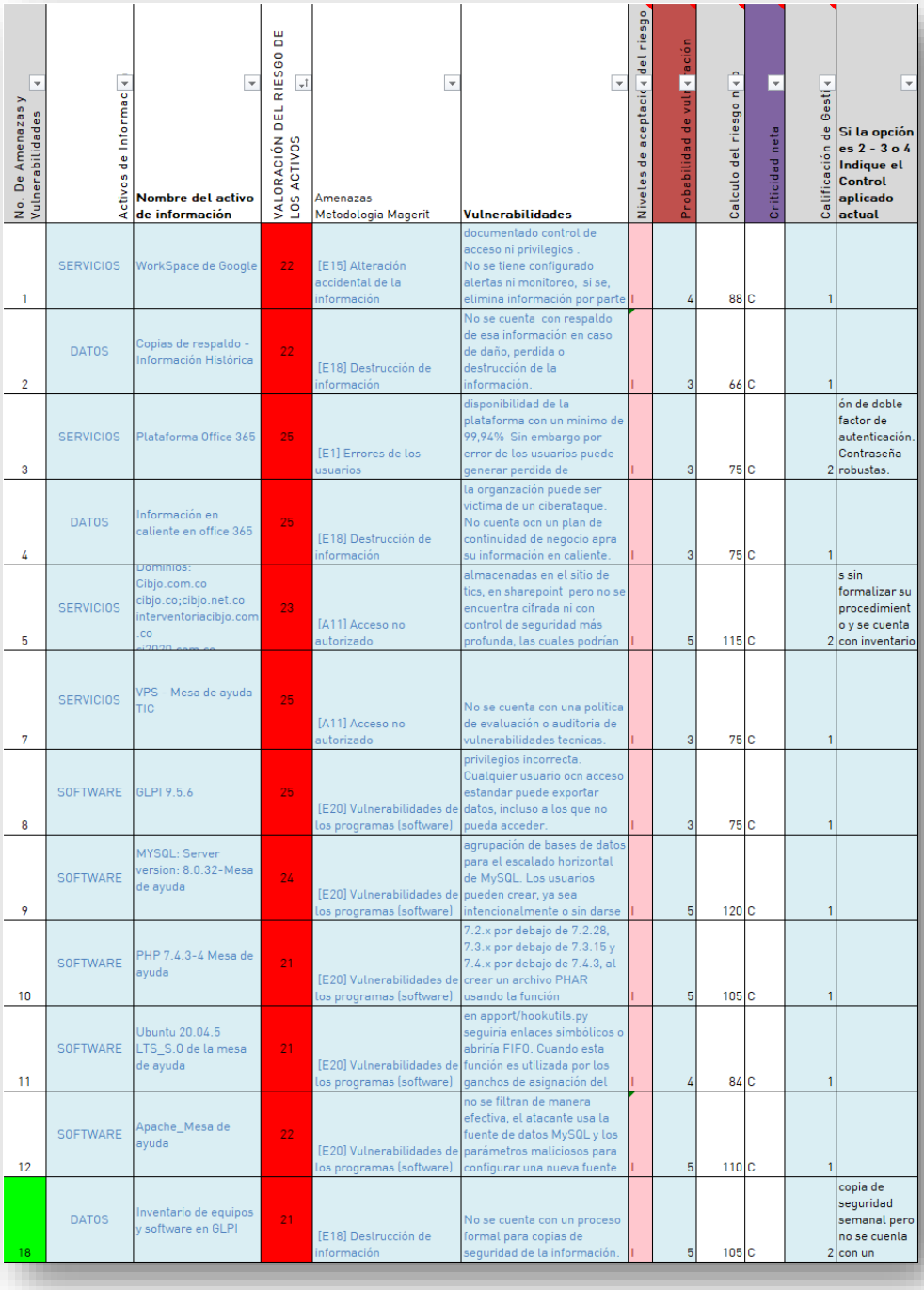
MODELO DE MADUREZ				
Nivel	**Cumplimiento**	**Proceso**	**Riesgos**	**Seguridad**
Nivel 5 Optimizado	**81% 100%**	• Las buenas prácticas se aplican a toda la organización, con base en los resultados de la mejora continua. • Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, así como tomar acciones correctivas o preventivas cuando se detectan fallas. • Se cuenta con herramientas para mejorar la calidad y la efectividad.	• La administración de riesgos es estructurada, administrada y esta implementada en toda la organización. • Se recolectan e implementan de forma oportuna controles adecuados para mitigar riesgos. • La dirección evalúa las estrategias de mitigación de riesgos de manera continua.	• La seguridad de la Información es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio. • Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. • Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. • La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. • Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad.
Nivel 4 Medible	**61% 80%**	• Los procedimientos se han estandarizado, documentado y difundido. • Se monitorean y se miden, aunque no es constante que se tomen acciones correctivas y preventivas.	• Existen procedimientos estándar para la administración y evaluación de riesgos. • Los riesgos identificados tienen un dueño, las áreas con funciones de TI han determinado los niveles de riesgo que la organización está dispuesta a tolerar.	• Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. • La identificación, autenticación y autorización de los usuarios está estandarizada. • Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. • Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización.

MODELO DE MADUREZ					
Nivel	Cumplimiento		Proceso	Riesgos	Seguridad
Nivel 3 Definido	**41%**	**60%**	• Los procedimientos se han estandarizado, documentado y difundido, sin embargo, la responsabilidad del cumplimiento recae en cada individuo, es probable que se detecten desviaciones a los estándares establecidos.	• Existe política de administración de riesgos para toda la organización. • La administración de riesgos sigue un proceso definido y está documentado.	• Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. • Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. • Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. • Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. • Existe entrenamiento en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.
Nivel 2 Repetible	**21%**	**40%**	• Los procesos siguen un patrón regular, son utilizados por diferentes áreas para llevar a cabo la misma tarea, aun cuando estos no se encuentren totalmente documentados. • No hay entrenamiento o comunicación formal de los procedimientos estándar.	• Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. • Los procesos de mitigación de riesgos están empezando a ser implementados donde se identifican riesgos.	• La seguridad de TI es vista como responsabilidad y disciplina de TI, el negocio no ve la seguridad de TI como parte de su propia disciplina. • Las responsabilidades sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. • Las políticas de seguridad de la información se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas.
Nivel 1 Inicial	**1%**	**20%**	• No existen procesos estándar, en su lugar existen enfoques ad hoc que tienden a ser aplicados. • Existe un enfoque reactivo hacia la planeación de la infraestructura. • En general la administración no está estructurada.	• Los riesgos de TI se toman en cuenta de manera ad hoc. • Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. • Los riesgos relativos a TI que afectan las operaciones del día a día, son rara vez discutidas con la gerencia.	• La organización reconoce la necesidad de seguridad para TI, así como la existencia problemas que requieren ser resueltos. • La conciencia de la necesidad de seguridad depende principalmente del individuo.

MODELO DE MADUREZ				
Nivel	**Cumplimiento**	**Proceso**	**Riesgos**	**Seguridad**
Nivel 0 Inexistente	**0% 0%**	• Carencia de procesos que apoyan la gestión del área y de seguridad de la información. • La organización no ha identificado situaciones que deban ser tratadas.	• No se realiza evaluación de riesgos a los procesos. • No se ha considerado la gestión de riesgos para adquirir soluciones de TI y para prestar servicios de TI.	• La organización no reconoce la necesidad de la seguridad para TI. • Las medidas para soportar la administrar la seguridad de TI no están implementadas. • La organización no toma en cuenta los impactos y las vulnerabilidades de seguridad.

Fuente: AUDITSI

Anexo B. Inventario de activos



No. De Amenazas y Vulnerabilidades	Activos de Informac	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptació del riesgo	Probabilidad de vul ación	Calculo del riesgo n	Criticidad neta	Calificación de Gest	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual
1	SERVICIOS	WorkSpace de Google	22	[E15] Alteración accidental de la información	documentado control de acceso ni privilegios . No se tiene configurado alertas ni monitoreo, si se, elimina información por parte	I	4	88	C	1	
2	DATOS	Copias de respaldo - Información Histórica	22	[E18] Destrucción de información	No se cuenta con respaldo de esa información en caso de daño, perdida o destrucción de la información.	I	3	66	C	1	
3	SERVICIOS	Plataforma Office 365	25	[E1] Errores de los usuarios	disponibilidad de la plataforma con un minimo de 99,94% Sin embargo por error de los usuarios puede generar perdida de	I	3	75	C	2	ón de doble factor de autenticación. Contraseña robustas.
4	DATOS	Información en caliente en office 365	25	[E18] Destrucción de información	la organzación puede ser victima de un ciberataque. No cuenta ocn un plan de continuidad de negocio apra su información en caliente.	I	3	75	C	1	
5	SERVICIOS	Dominios: Cibjo.com.co cibjo.co;cibjo.net.co interventoriacibjo.com .co	23	[A11] Acceso no autorizado	almacenadas en el sitio de tics, en sharepoint pero no se encuentra cifrada ni con control de seguridad más profunda, las cuales podrían	I	5	115	C	2	s sin formalizar su procedimient o y se cuenta con inventario
7	SERVICIOS	VPS - Mesa de ayuda TIC	25	[A11] Acceso no autorizado	No se cuenta con una politica de evaluación o auditoria de vulnerabilidades tecnicas.	I	3	75	C	1	
8	SOFTWARE	GLPI 9.5.6	25	[E20] Vulnerabilidades de los programas (software)	privilegios incorrecta. Cualquier usuario ocn acceso estandar puede exportar datos, incluso a los que no pueda acceder.	I	3	75	C	1	
9	SOFTWARE	MYSQL: Server version: 8.0.32-Mesa de ayuda	24	[E20] Vulnerabilidades de los programas (software)	agrupación de bases de datos para el escalado horizontal de MySQL. Los usuarios pueden crear, ya sea intencionalmente o sin darse	I	5	120	C	1	
10	SOFTWARE	PHP 7.4.3-4 Mesa de ayuda	21	[E20] Vulnerabilidades de los programas (software)	7.2.x por debajo de 7.2.28, 7.3.x por debajo de 7.3.15 y 7.4.x por debajo de 7.4.3, al crear un archivo PHAR usando la función	I	5	105	C	1	
11	SOFTWARE	Ubuntu 20.04.5 LTS_S.0 de la mesa de ayuda	21	[E20] Vulnerabilidades de los programas (software)	en apport/hookutils.py seguiría enlaces simbólicos o abriría FIFO. Cuando esta función es utilizada por los ganchos de asignación del	I	4	84	C	1	
12	SOFTWARE	Apache_Mesa de ayuda	22	[E20] Vulnerabilidades de los programas (software)	no se filtran de manera efectiva, el atacante usa la fuente de datos MySQL y los parámetros maliciosos para configurar una nueva fuente	I	5	110	C	1	
18	DATOS	Inventario de equipos y software en GLPI	21	[E18] Destrucción de información	No se cuenta con un proceso formal para copias de seguridad de la información.	I	5	105	C	2	copia de seguridad semanal pero no se cuenta con un

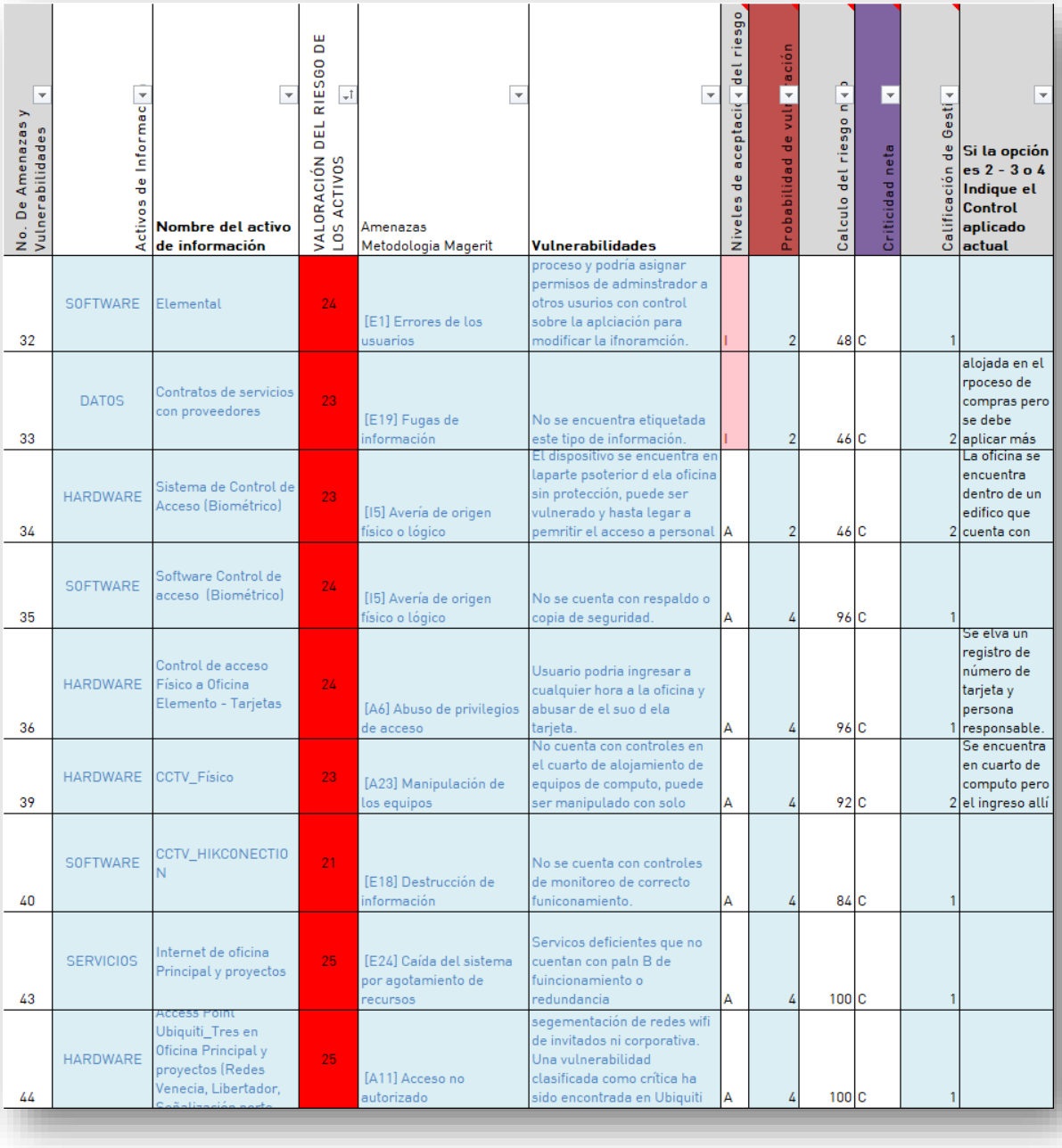
Fuente: El autor.

Anexo B. Inventario de activos. (Continuación)

No. De Amenazas y Vulnerabilidades	Activos de Informaci	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptació del riesgo	Probabilidad de vul ación	Calculo del riesgo n)	Criticidad neta	Calificación de Gesti	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual
20	DATOS	Archivo de password Escritorios Remotos	21	[E19] Fugas de información	No cuenta con un etiquetado de información que permita aplicar más controles sobre informaicón sensible	I	3	63	C	2	restringida para ciertos usuarios d ela organziación pero hace falta delimitarla apra los	32
21	DATOS	Archivo de Licencias Office 365	24	[A18] Destrucción de información	Información que no cuenta con respaldo o copias de seguridad.	I	2	48	C	2	restringida para ciertos usuarios de la organziación pero hace falta un	24
22	DATOS	Archivo de Licencias y vencimiento	22	[E19] Fugas de información	No cuenta con un etiquetado de información que permita aplicar más controles sobre información sensible	I	2	44	C	2	restringida para ciertos usuarios de la organziación pero hace	22
23	DATOS	Planner de Licenciamiento	23	[E3] Errores de monitorización (log)	por falta de monitoreo se puede olvidar o pasar por alto la renovaicón de un servicio importante para la organziación.	I	3	69	C	3	semanalment e y se actuiliza con cada renovación o	23
24	HARDWARE	Discos duros externos (Información Histórica digital)	23	[A23] Manipulación de los equipos	Daño mecanico	I	4	92	C	2	Se mantienen almacenadso en un cuarto bajo llave.	46
25	SOFTWARE	Consola de Antivirus	23	[E2] Errores del administrador	Por configuracion deficiente y falta monitoreo de la consola, no se detecten intrusos o incidentes de seguridad.	I	3	69	C	1		69
26	HARDWARE	Equipos de Computo	23	[A6] Abuso de privilegios de acceso	Un malware que pueda contagiar dañar la información sincornizada localmente y se replique a la nube.	I	2	46	C	3	resticicone de derechos de administrador , software para	15
27	SOFTWARE	Sistema Operativo Windows 10 profesional	21	[E20] Vulnerabilidades de los programas (software)	vulnerabilidad de Carga sin restricciones de archivo con tipo peligroso que podría causar la ejecución remota de código cuando el atacante	I	2	42	C	1		42
28	SOFTWARE	Sistema Operativo Windows 11 profesional	24	[E20] Vulnerabilidades de los programas (software)	vulnerabilidad de Asignación incorrecta de permisos para recursos críticos que podría causar una escalada de privilegios locales cuando un	I	2	48	C	1		48
29	SERVICIOS	Servidor Escritorios remotos (Acceso).	23	[A11] Acceso no autorizado	El servidor puede ser detectado por la dirección publicada y sufrir un ataque mediante un acceos no autorizado.	I	2	46	C	3	medio de VPN. Herrameitnas de seguridad del	15
30	SOFTWARE	Windows server 2019	21	[E20] Vulnerabilidades de los programas (software)	A CWE-798: Existe una vulnerabilidad de uso de credenciales codificadas que podría causar una escalada	I	2	42	C	2	Se realizán actualziacion es exporadicas	21

Fuente: El autor.

Anexo B. Inventario de activos. (Continuación)



No. De Amenazas y Vulnerabilidades	Activos de Informac	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptació del riesgo	Probabilidad de vul ación	Calculo del riesgo n p	Criticidad neta	Calificación de Gesti	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual
32	SOFTWARE	Elemental	24	[E1] Errores de los usuarios	proceso y podria asignar permisos de adminstrador a otros usurios con control sobre la aplciación para modificar la ifnoramción.	I	2	48	C	1	
33	DATOS	Contratos de servicios con proveedores	23	[E19] Fugas de información	No se encuentra etiquetada este tipo de información.	I	2	46	C	2	alojada en el rpoceso de compras pero se debe aplicar más
34	HARDWARE	Sistema de Control de Acceso (Biométrico)	23	[I5] Avería de origen físico o lógico	El dispositivo se encuentra en laparte psoterior d ela oficina sin protección, puede ser vulnerado y hasta legar a pemritir el acceso a personal	A	2	46	C	2	La oficina se encuentra dentro de un edifico que cuenta con
35	SOFTWARE	Software Control de acceso (Biométrico)	24	[I5] Avería de origen físico o lógico	No se cuenta con respaldo o copia de seguridad.	A	4	96	C	1	
36	HARDWARE	Control de acceso Físico a Oficina Elemento - Tarjetas	24	[A6] Abuso de privilegios de acceso	Usuario podria ingresar a cualquier hora a la oficina y abusar de el suo d ela tarjeta.	A	4	96	C	1	Se elva un registro de número de tarjeta y persona responsable.
39	HARDWARE	CCTV_Físico	23	[A23] Manipulación de los equipos	No cuenta con controles en el cuarto de alojamiento de equipos de computo, puede ser manipulado con solo	A	4	92	C	2	Se encuentra en cuarto de computo pero el ingreso allí
40	SOFTWARE	CCTV_HIKCONECTIO N	21	[E18] Destrucción de información	No se cuenta con controles de monitoreo de correcto funiconamiento.	A	4	84	C	1	
43	SERVICIOS	Internet de oficina Principal y proyectos	25	[E24] Caída del sistema por agotamiento de recursos	Servicos deficientes que no cuentan con paln B de fuincionamiento o redundancia	A	4	100	C	1	
44	HARDWARE	Access Point Ubiquiti_Tres en Oficina Principal y proyectos (Redes Venecia, Libertador, Señalización norte	25	[A11] Acceso no autorizado	segementación de redes wifi de invitados ni corporativa. Una vulnerabilidad clasificada como crítica ha sido encontrada en Ubiquiti	A	4	100	C	1	

Fuente: El autor.

Anexo B. Inventario de activos. (Continuación)

No. De Amenazas y Vulnerabilidades	Activos de Informac	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptació del riesgo	Probabilidad de vul ación	Calculo del riesgo n	Criticidad neta	Calificación de Gesti	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual
45	HARDWARE	Repetidores wifi de proveedor de internet (AMV Cauca, redes Venecia, TM AV68).	24	[A11] Acceso no autorizado	segementación de redes wifi de invitados ni corporativa. Una vulnerabilidad clasificada como crítica ha sido encontrada en Ubiquiti	A	4	96	C	1	
47	HARDWARE	Impresoras en oficina principal y proyectos.	25	[A11] Acceso no autorizado	inclusión de archivos transversales y locales en FPProducerInternetServer.exe en Ricoh MarcomCentral, anteriormente PTI Marketing,	A	4	100	C	1	
48	SERVICIOS	Vigilancia Electrónica (Redes Venecia, Señalización norte, Calarcá, TM AV68,	24	[A5] Suplantación de la identidad del usuario	No se cuenta con un control o registro d elas personas autorizadas para reportar o autorizar en este servicio	A	4	96	C	1	
49	HARDWARE	Servidor de alojamiento (Biométrico y videoconferencia).	22	[A11] Acceso no autorizado	Puede ser accedio remotamente, puede ser explotado el puerto abierto.	A	4	88	C	1	
50	SERVICIOS	Servicios Públicos: Agua, luz, teléfono y gas en Oficina Elemento y	22	[A24] Denegación de servicio	Por olvido de pago.	A	4	88	C	1	
51	INSTALACIONES	Oficinas físicas Proyectos.	25	[A11] Acceso no autorizado	Robo por falta de vigilancia.	A	4	100	C	1	
53	SERVICIOS	Sigeslab: Alojamiento	25	[E2] Errores del administrador	No se tiene el control de acceso de ese servicio ppr parte del rpoceso de tecnologia.	A	3	75	C	1	
54	SOFTWARE	Sigeslab: Sistema operativo Windows server estándar 2016	25	[E20] Vulnerabilidades de los programas (software)	A CWE-798: Existe una vulnerabilidad de uso de credenciales codificadas que podría causar una escalada	A	2	50	C	1	
55	SOFTWARE	Sigeslab: SQL Server estándar 2016	24	[E20] Vulnerabilidades de los programas (software)	Se encontró una falla de inyección SQL en la API relacionada con las erratas de katello. Un atacante	A	2	48	C	1	
56	SERVICIOS	Pagina web Transversa del Sisga	22	[A24] Denegación de servicio	La pagian puede ser atacada por metodo de ataque denegación de servicio, no se cuenta con información a detalle de comoe sta configurada, que se publica.	A	4	88	C	1	

Fuente: Elaboración propia.

Anexo B. Inventario de activos. (Continuación)

No. De Amenazas y Vulnerabilidades	Activos de Informac	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptaci del riesgo	Probabilidad de vul acion	Calculo del riesgo n p	Criticidad neta	Calificación de Gesti	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual
57	SERVICIOS	Plataformas de Gmail :CIBJO.co y CIBJO.com.co	22	[A7] Uso no previsto	Debido a al falta de control de acceso de estos servicios.	A	2	44	C	2	Se cuenta con registro de los usuarios.
58	HARDWARE	Vehículos	21	[A25] Robo	Es posible hackear el GPS para evitar el rastreo en tiempo real	A	2	42	C	2	Se cuenta con registro de los vehiculos, asignación al
59	DATOS	Contratos (Servicios públicos, vehículos, comunicaciones (internet, telefonía móvil y fija)	21	[E19] Fugas de información	Filtración deinformación por falta de controles más estrictos.	A	4	84	C	2	La información se almacena en el proceso de
60	DATOS	Formularios control operacional vehículos (4).	24	[E19] Fugas de información	Filtración deinformación por falta de controles más estrictos.	A	2	48	C	2	La información se almacena en el proceso
61	DATOS	Inventario de Topografía y laboratorio	22	[E15] Alteración accidental de la información	Filtración deinformación por falta de controles más estrictos.	A	3	66	C	2	
62	DATOS	Programas de mantenimiento de (topografía, laboratorio, vehículos	24	[E15] Alteración accidental de la información	Usuarios de otros procesos pueden legar a editar y/o manipular la información.	A	3	72	C	2	La información se almacena en el proceso
63	DATOS	Sitio de Infraestructura de SharePoint	22	[E18] Destrucción de información	CVE-2023-28288Vulnerabilidad de suplantación de identidad de Microsoft SharePoint Server	A	2	44	C	2	Se implementa herramienta de kaspersky
64	HARDWARE	Swtchs Administrable HP (Dos).	22	[A11] Acceso no autorizado	Switchs no administrados ni confgurados con los controles minimos de seguridad.	A	4	88	C	1	
65	SOFTWARE	Software Elemental	22	[A6] Abuso de privilegios de acceso	Persona a cargo del porceso es quien adminsitra la herramienta y asignación de usuarios.	A	3	66	C	1	
66	SOFTWARE	Base de datos SQL Express de Elemental	24	[E20] Vulnerabilidades de los programas (software)	Se encontró una falla de inyección SQL en la API relacionada con las erratas de katello. Un atacante	A	3	72	C	1	

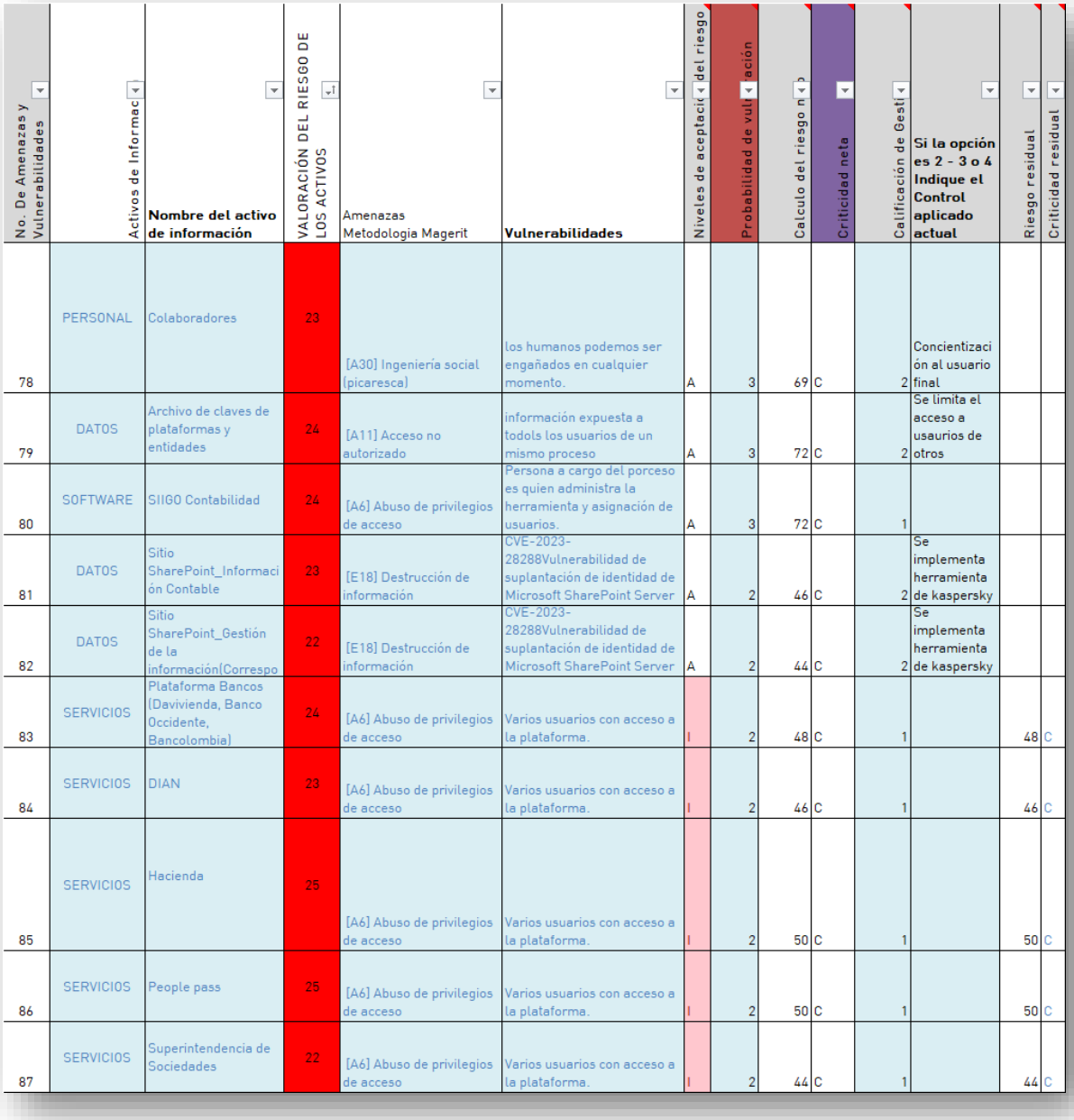
Fuente: El autor.

Anexo B. Inventario de activos. (Continuación)

No. De Amenazas y Vulnerabilidades	Activos de Informac	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptaci del riesgo	Probabilidad de vul acion	Calculo del riesgo n	Criticidad neta	Calificación de Gesti	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual
67	SERVICIOS	Herramienta CompuTrabajo.	23	[E1] Errores de los usuarios	Exposición de información.	A	4	92	C	1	
68	SERVICIOS	Plataforma Colegio del Riesgo Sura	24	[E2] Errores del administrador	Se puede observar al información de otras empresas cuando se cambia de una organización a otra	A	3	72	C	1	
69	SERVICIOS	Herramienta mi planilla	24	[A6] Abuso de privilegios de acceso	Se comparte credenciales de acceso del mismo proceos.	A	3	72	C	1	
70	SERVICIOS	Plataforma Sena	24	[A6] Abuso de privilegios de acceso	Se comparte credenciales de acceso del mismo proceos.	A	3	72	C	1	
71	SOFTWARE	Siigo Nomina	24	[A6] Abuso de privilegios de acceso	Persona a cargo del porceso es quien admnsitra la herramienta y asignación de usuarios.	A	3	72	C	1	
72	SERVICIOS	Herramienta Biblioinstrumentos	21	[A6] Abuso de privilegios de acceso	Persona a cargo del porceso es quien administra la herramienta y asignación de usuarios.	A	3	63	C	1	
73	DATOS	Bases de datos BD_GENERAL	23	[A5] Suplantación de la identidad del usuario	Información no etiquetada como sensible.	A	3	69	C	1	
74	SERVICIOS	Herramienta Data Riesgos	21	[E1] Errores de los usuarios	Información consultada requeire temrinos de confidencialidad.	A	3	63	C	1	
75	DATOS	Sitio SharePoint_Talento Humano	24	[E18] Destrucción de información	CVE-2023-28288Vulnerabilidad de suplantación de identidad de Microsoft SharePoint Server	A	2	48	C	2	Se implementa herramienta de kaspersky
76	SOFTWARE	VPN a Servidor de Siigo Nomina.Forticlient 7.0.3	23	[A11] Acceso no autorizado	Una exposicion de información confidencial a una vulnerabilidad de actor no autorizado [CWE-200] en	A	2	46	C	1	
77	SOFTWARE	Software RFI	24	[A6] Abuso de privilegios de acceso	Persona a cargo del porceso es quien administra la herramienta y asignación de usuarios.	A	3	72	C	1	

Fuente: El autor.

Anexo B. Inventario de activos. (Continuación)



No. De Amenazas y Vulnerabilidades	Activos de Informac	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptació del riesgo	Probabilidad de vul ación	Calculo del riesgo n b	Criticidad neta	Calificación de Gesti	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
78	PERSONAL	Colaboradores	23	[A30] Ingeniería social (picaresca)	los humanos podemos ser engañados en cualquier momento.	A	3	69	C	2	Concientización al usuario final		
79	DATOS	Archivo de claves de plataformas y entidades	24	[A11] Acceso no autorizado	información expuesta a todols los usuarios de un mismo proceso	A	3	72	C	2	Se limita el acceso a usaurios de otros		
80	SOFTWARE	SIIGO Contabilidad	24	[A6] Abuso de privilegios de acceso	Persona a cargo del porceso es quien administra la herramienta y asignación de usuarios.	A	3	72	C	1			
81	DATOS	Sitio SharePoint_Información Contable	23	[E18] Destrucción de información	CVE-2023-28288Vulnerabilidad de suplantación de identidad de Microsoft SharePoint Server	A	2	46	C	2	Se implementa herramienta de kaspersky		
82	DATOS	Sitio SharePoint_Gestión de la información(Correspo	22	[E18] Destrucción de información	CVE-2023-28288Vulnerabilidad de suplantación de identidad de Microsoft SharePoint Server	A	2	44	C	2	Se implementa herramienta de kaspersky		
83	SERVICIOS	Plataforma Bancos (Davivienda, Banco Occidente, Bancolombia)	24	[A6] Abuso de privilegios de acceso	Varios usuarios con acceso a la plataforma.	I	2	48	C	1		48	C
84	SERVICIOS	DIAN	23	[A6] Abuso de privilegios de acceso	Varios usuarios con acceso a la plataforma.	I	2	46	C	1		46	C
85	SERVICIOS	Hacienda	25	[A6] Abuso de privilegios de acceso	Varios usuarios con acceso a la plataforma.	I	2	50	C	1		50	C
86	SERVICIOS	People pass	25	[A6] Abuso de privilegios de acceso	Varios usuarios con acceso a la plataforma.	I	2	50	C	1		50	C
87	SERVICIOS	Superintendencia de Sociedades	22	[A6] Abuso de privilegios de acceso	Varios usuarios con acceso a la plataforma.	I	2	44	C	1		44	C

Fuente: El autor.

Anexo B. Inventario de activos. (Continuación)

No. De Amenazas y Vulnerabilidades	Activos de Informac	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptaci del riesgo	Probabilidad de vuli ación	Calculo del riesgo n	Criticidad neta	Calificación de Gesti	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
96	DATOS	Sitio SharePoint_Informaci ón Comercial	25	[E18] Destrucción de información	CVE-2023-28288Vulnerabilidad de suplantación de identidad de Microsoft SharePoint Server	I	2	50	C	2	Se implementa herramienta de kaspersky	25	C
97	DATOS	Sitio SharePoint_Informaci ón Licitaciones	25	[E18] Destrucción de información	CVE-2023-28288Vulnerabilidad de suplantación de identidad de Microsoft SharePoint Server	I	2	50	C	2	Se implementa herramienta de kaspersky	25	C
98	SOFTWARE	Adobe Creative Cloud	22	[E20] Vulnerabilidades de los programas (software)	Adobe Creative Cloud Desktop versión 2.7.0.13 (y anteriores) está afectado por una vulnerabilidad de	I	2	44	C	2	Herrameinta de seguridad para la detección de	22	C
99	SERVICIOS	Canva	22	[E1] Errores de los usuarios	Eklimnación de información.	I	2	44	C	1		44	C
100	SERVICIOS	Youtube	22	[E18] Destrucción de información	El complemento El complemento de WordPress de YouTube Video Inserter es vulnerable a las secuencias	I	2	44	C	1		44	C
101	SERVICIOS	Instagram	25	[E18] Destrucción de información	Múltiples secuencias de comandos entre sitios (XSS) almacenadas en el complemento MyThemeShop	I	2	50	C	1		50	C
102	SERVICIOS	LinkedIn	22	[E18] Destrucción de información	Desbordamiento de búfer en el control ActiveX IEToolbar.IEContextMenu.1 en LinkedInIEToolbar.dll en	I	2	44	C	1		44	C

Fuente: El autor.

Anexo C. Valoración del riesgo

Nombre	Riesg	AUTE	TRA	CONF	INTE	DISP	VALO
WorkSpace de Google	CRITICO	25	20	25	20	20	22
Copias de respaldo - Información Histórica	CRITICO	25	20	25	20	20	22
Plataforma Office 365	CRITICO	25	25	25	25	25	25
Información en caliente en office 365	CRITICO	25	25	25	25	25	25
Dominios: Cibjo.com.cocibjo.co;cibjo.net.cointerve	CRITICO	25	20	20	25	25	23
VPS - Mesa de ayuda TIC	CRITICO	25	25	25	25	25	25
GLPI 9.5.6	CRITICO	25	25	25	25	25	25
MYSQL: Server version: 8.0.32-Mesa de ayuda	CRITICO	25	25	25	25	20	24
PHP 7.4.3-4 Mesa de ayuda	CRITICO	20	20	20	25	20	21
Ubuntu 20.04.5 LTS_S.O de la mesa de ayuda	CRITICO	25	15	20	25	20	21
Apache_Mesa de ayuda	CRITICO	25	20	20	25	20	22
Inventario de equipos y software en GLPI	CRITICO	25	20	20	25	15	21
Archivo de password Escritorios Remotos	CRITICO	25	20	20	25	15	21
Archivo de Licencias Office 365	CRITICO	25	25	25	25	20	24
Archivo de Licencias y vencimiento	CRITICO	25	20	20	25	20	22
Planner de Licenciamiento	CRITICO	25	20	25	20	25	23
Discos duros externos (Información Histórica digita	CRITICO	20	20	25	25	25	23
Consola de Antivirus	CRITICO	20	20	25	25	25	23
Equipos de Computo	CRITICO	25	15	25	25	25	23
Sistema Operativo Windows 10 profesional	CRITICO	20	20	25	20	20	21
Sistema Operativo Windows 11 profesional	CRITICO	25	25	25	20	25	24
Servidor Escritorios remotos (Acceso).	CRITICO	20	25	20	25	25	23
Windows server 2019	CRITICO	20	20	15	25	25	21
SIIGO	CRITICO	25	25	15	20	20	21
Elemental	CRITICO	25	25	25	25	20	24
Contratos de servicios con proveedores	CRITICO	25	20	25	25	20	23
Sistema de Control de Acceso (Biométrico)	CRITICO	25	20	25	25	20	23
Software Control de acceso (Biométrico)	CRITICO	25	25	25	25	20	24
Control de acceso Físico a Oficina Elemento - Tarj	CRITICO	25	25	25	25	20	24
CCTV_Físico	CRITICO	20	25	20	25	25	23
CCTV_HIKCONECTION	CRITICO	25	25	20	25	9	21
Internet de oficina Principal y proyectos	CRITICO	25	25	25	25	25	25
Access Point Ubiquiti_Tres en Oficina Principal y pr	CRITICO	25	25	25	25	25	25
Repetidores wifi de proveedor de internet (AMV Ca	CRITICO	25	20	25	25	25	24
Impresoras en oficina principal y proyectos.	CRITICO	25	25	25	25	25	25

Fuente: El autor.

Anexo C. Valoración del riesgo – continuación.

Nombre	Riesg	AUTE	TRA	CONF	INTE	DISP	VALO
Vigilancia Electrónica (Redes Venecia, Señalizació	CRITICO	20	25	25	25	25	24
Servidor de alojamiento (Biométrico y videoconfer	CRITICO	20	25	25	25	15	22
Servicios Públicos: Agua, luz, teléfono y gas en Ofi	CRITICO	25	15	20	25	25	22
Oficinas físicas Proyectos.	CRITICO	25	25	25	25	25	25
Sigeslab: Alojamiento	CRITICO	25	25	25	25	25	25
Sigeslab: Sistema operativo Windows server estár	CRITICO	25	25	25	25	25	25
Sigeslab: SQL Server estándar 2016	CRITICO	25	25	25	25	20	24
Pagina web Transversa del Sisga	CRITICO	25	20	20	25	20	22
Plataformas de Gmail :CIBJO.co y CIBJO.com.co	CRITICO	25	20	20	25	20	22
Vehículos	CRITICO	25	20	20	25	15	21
Contratos (Servicios públicos, vehículos, comunica	CRITICO	25	20	20	25	15	21
Formularios control operacional vehículos (4).	CRITICO	25	25	25	25	20	24
Inventario de Topografía y laboratorio	CRITICO	25	20	20	25	20	22
Programas de mantenimiento de (topografía, labo	CRITICO	25	25	25	25	20	24
Sitio de Infraestructura de SharePoint	CRITICO	25	20	25	25	15	22
Swtchs Administrable HP (Dos).	CRITICO	25	20	25	25	15	22
Software Elemental	CRITICO	25	20	25	25	15	22
Base de datos SQL Express de Elemental	CRITICO	25	25	25	25	20	24
Herramienta CompuTrabajo.	CRITICO	25	20	25	25	20	23
Plataforma Colegio del Riesgo Sura	CRITICO	25	20	25	25	25	24
Herramienta mi planilla	CRITICO	25	20	25	25	25	24
Plataforma Sena	CRITICO	25	25	20	25	25	24
Siigo Nomina	CRITICO	25	25	25	25	20	24
Herramienta Biblioinstrumentos	CRITICO	25	20	20	25	15	21
Bases de datos BD_GENERAL	CRITICO	25	20	20	25	25	23
Herramienta Data Riesgos	CRITICO	20	20	20	25	20	21
Sitio SharePoint_Talento Humano	CRITICO	25	25	25	20	25	24
VPN a Servidor de Siigo Nomina.Forticlient 7.0.3	CRITICO	20	25	20	25	25	23
Software RFI	CRITICO	25	25	25	25	20	24
Colaboradores	CRITICO	25	20	25	25	20	23
Archivo de claves de plataformas y entidades	CRITICO	25	25	25	25	20	24
SIIGO Contabilidad	CRITICO	25	25	25	25	20	24
Sitio SharePoint_Información Contable	CRITICO	25	20	25	25	20	23
Sitio SharePoint_Gestión de la información(Corres	CRITICO	20	20	25	25	20	22
Plataforma Bancos (Davivienda, Banco Occidente,	CRITICO	25	25	25	25	20	24

Fuente: El autor.

Anexo C. Valoración del riesgo – continuación.

Nombre	Riesg	AUTE	TRA	CONF	INTE	DISP	VALO
Base de datos de Clientes	CRITICO	20	20	25	25	20	22
Propuestas de negocios	CRITICO	25	25	25	25	25	25
Sitio SharePoint_Información Comercial	CRITICO	25	25	25	25	25	25
Sitio SharePoint_Información Licitaciones	CRITICO	25	25	25	25	25	25
Adobe Creative Cloud	CRITICO	25	25	25	20	15	22
Canva	CRITICO	25	25	25	20	15	22
Youtube	CRITICO	25	25	25	20	15	22
Instagram	CRITICO	25	25	25	25	25	25
LinkedIn	CRITICO	20	20	25	25	20	22
Hosting: IONOS 1 & 1Goodadymi.com.coColombia	BAJO	9	9	9	9	9	9
Anydesk	APRECIAB	20	9	20	9	15	15
Formulario Ficha de alistamiento Equipos de Com	APRECIAB	9	9	9	15	15	11
Formulario Registro de Mantenimiento de Equipos	APRECIAB	9	9	9	15	15	11
Inducción TIC	APRECIAB	9	9	9	9	15	10
CIBJOBot	APRECIAB	9	9	15	9	9	10
Inventario de Licencias Office 365	APRECIAB	15	9	9	15	20	14
Control de acceso Físico a Oficina Elemento - Bas	APRECIAB	15	15	15	20	9	15
Control de acceso Físico a Oficina WeWork- Bases	APRECIAB	15	15	15	20	9	15
Dispositivos de Video Conferencia Devio	APRECIAB	9	9	9	15	15	11
Software Devio_Dispositivos de Video Conferencia	APRECIAB	9	9	9	15	15	11
Archivo control de impresoras	APRECIAB	15	15	9	15	15	14
Sigeslab: Software para gestión de laboratorio	APRECIAB	9	25	9	20	9	14
Herramienta mesa de ayuda GLPI_Solicitudes de	IMPORTAN	20	20	20	20	20	20
Pagina web cibjo.co	IMPORTAN	20	20	20	20	20	20
Documentos de Sistema de Gestión Integrada	IMPORTAN	20	20	20	20	20	20
AlertaBot	APRECIAB	9	15	9	20	9	12
Herramienta Muraby	IMPORTAN	20	20	20	20	20	20
Sitio SharePoint_Gestión integrada e Innovación	IMPORTAN	20	20	20	20	20	20
Sitio SharePoint_Intranet	IMPORTAN	20	20	20	20	20	20
Sitio SharePoint_Proyecto Pilo	IMPORTAN	9	20	9	20	20	16
Formulario en Survey 123 _Solicitudes de Calidad	IMPORTAN	20	20	15	25	20	20
Software Visio	APRECIAB	9	9	9	20	9	11
Sitio SharePoint_Compras	IMPORTAN	20	15	15	20	20	18
Formulario en Survey 123 _Requisiciones de Com	IMPORTAN	25	25	20	9	9	18
Tarjeta de crédito de Compras	IMPORTAN	20	15	20	25	20	20

Fuente: El autor.

Anexo C. Valoración del riesgo – continuación.

Nombre	Riesg	AUTE	TRA	CONF	INTE	DISP	VALO
Base de datos de Proveedores	IMPORTAN	20	15	25	20	20	20
Base de datos de Contratistas	IMPORTAN	20	20	15	15	15	17
Pagina CCI (Cámara Colombiana de Infraestructur	IMPORTAN	9	9	25	25	25	19
Caja menor	IMPORTAN	20	15	25	20	20	20
Información Histórica en físico	IMPORTAN	20	15	25	20	20	20
Información Histórica Digital	IMPORTAN	15	25	9	15	15	16
Alojamiento información Física en Airon Montain	IMPORTAN	15	20	15	20	25	19
Alojamiento información Física en Oficina (Archivo	IMPORTAN	15	9	15	25	15	16
Sitio SharePoint_Información Gestión de la Inform	IMPORTAN	20	25	15	15	9	17
Sitio SharePoint_Información Jurídica.	IMPORTAN	20	20	9	25	25	20
Formulario en Survey 123 _Solicitudes a proceso	IMPORTAN	25	25	25	9	9	19
Licencias de Arcgis	IMPORTAN	25	15	20	20	20	20
Licencias de Autodesk	IMPORTAN	15	20	25	20	20	20
Licencia HDM4	IMPORTAN	20	20	20	20	15	19
Licencia DOCS	IMPORTAN	20	15	25	25	9	19
Licencia Integromat	IMPORTAN	20	20	25	25	9	20
Licencia Nero	IMPORTAN	20	20	15	25	20	20
Global Maper	IMPORTAN	20	9	20	15	15	16
Circuito de Video en proyecto Sisga	IMPORTAN	20	9	20	15	15	16
Sitio SharePoint_Información Gerencia General	IMPORTAN	20	9	20	15	15	16
Sitio SharePoint_Programa Transferencia y Ética	IMPORTAN	20	9	20	15	15	16
Firma digital_Gerencia	IMPORTAN	20	9	20	15	15	16
Firma digital_Director Técnico	IMPORTAN	9	20	9	25	20	17
Firma digital_Director Proyecto Sisga.	IMPORTAN	25	20	9	25	20	20
Sitio SharePoint_Proyectos	IMPORTAN	15	15	15	25	15	17
Sitio SharePoint_Comites (Brigadas, Comco, Copa	IMPORTAN	20	20	15	15	9	16

Fuente: El autor.

Anexo D. Política de Seguridad de la Información y Ciberseguridad

1. OBJETIVO

Establecer las directrices de la organización para garantizar los principios fundamentales de la información (Disponibilidad, integridad y confidencialidad) para el buen uso y privacidad de los datos, alineados con la dirección estratégica organizacional, contemplando: Políticas, procedimientos, controles, mejores prácticas, tomando como referente, requisitos legales, técnicos de la norma ISO/IEC 27001-2013, ISO/IEC 27002-2013 y MINTIC.

Como objetivo específico de la política se define:

- Identificar, establecer e implementar actividades de control para minimizar el riesgo de los procesos y áreas críticas, mediante una adecuada gestión de estos, garantizando la continuidad del negocio.

2.ALCANCE

La política de Seguridad de la Información aplica a toda la organización y a sus agentes implicados. Es responsabilidad de cada parte cumplirla teniendo en cuenta los principios, controles y procedimientos.

3.DOCUMENTOS DE REFERENCIA

- ISO/IEC 27001-2013: Técnicas de seguridad. Sistema de gestión de la seguridad de la información
- ISO/IEC 27002-2013: Técnicas de seguridad. Código de practica para controles de seguridad de la información.
- MINTIC: Guía – Seguridad de la información MiPymes.

4.DEFINICIONES

- **Activo de información:** Cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización y que vale la pena identificar, clasificar y proteger de acuerdo con su valor, criticidad y nivel de exposición.
- **Amenaza:** Causa potencial de un incidente que puede provocar daños a un sistema o a la organización.
- **Ciberseguridad:** Es la practica para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas de información, dispositivos, aplicaciones que se encuentren interconectados en el ciberespacio.
- **Ciberespacio:** Mundo no físico, donde cualquier persona puede estar interconectada con un dispositivo tecnológico.
- **Clasificación de la información:** Ejercicio por el cual se determina que la información pertenece a un nivel, estipulado por la organización para asegurar para que la información reciba la protección adecuada.
- **Control:** Políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de ciberseguridad y seguridad de la información por debajo del nivel de riesgo asumido. también utilizado como sinónimo de salvaguarda o contramedida.
- **Custodio:** Cargo, proceso o equipo de trabajo, encargado para administrar y hacer efectivos los controles de seguridad como copias de seguridad, asignación de privilegios de acceso, modificación y eliminación.
- **Confidencialidad:** Característica de la información que determina que la información solo esté disponible para individuos, entidades o procesos autorizados.
- **Disponibilidad:** Característica de la información para que se accesible y utilizable cuando se requiera por los usuarios y procesos autorizados.
- **Evaluación del riesgo:** Proceso global de identificación, análisis y

estimación del riesgo.

- **Guía:** Es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
- **Impacto:** El costo para la organización de un incidente, financiero, reputacional, implicaciones legales, etc.
- **Incidente de seguridad de la información:** Evento de seguridad de la información inesperado o no deseado que puede comprometer la operación del negocio o amenazar la seguridad de la información.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo d ellos activos.
- **Inventario de Activos:** Listado de todos aquellos recursos (físicos, información, software, documentos, servicios, personas, intangibles, etc.) que tengan valor para la organización y necesiten ser protegidos.
- **Información**: Datos relacionados que tienen significado para la organización, la cual necesita una protección adecuada.
- **Mejor Práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad.
- **Plan de Continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico, en este caso la Seguridad de la Información.

- **Política de Seguridad de la Información y la Ciberseguridad**: Documento donde se establecen las directrices y los lineamientos relacionados a la protección, manejo seguro de la información. como el desarrollo de capacidades empresariales para defender y anticipar de amenazas informáticas de los activos expuestos en CIBJO SAS BIC y sus consorcios.
- **Privacidad:** Propiedad de la información que garantiza el uso adecuado de la misma, así esté legítimamente autorizado a manejarla.
- **Procedimiento:** Definen específicamente, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Delinean los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema especifico.
- **Reducción del riesgo:** Acciones que se toman para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Responsable de la información:** Es el colaborador para quien la información fue creada con el objetivo de realizar sus funciones en el negocio y que tiene la responsabilidad de administrarla, clasificarla y evaluar los riesgos que pueden afectarla. También es el primer responsable de implantar la Política de Seguridad de la Información y Ciberseguridad dentro de su área y para poder realizarlo debe conocer el valor de su información, los usuarios que deben tener acceso a ella y los privilegios que requieren para su uso.
- **Riesgo:** Posibilidad de un resultado negativo derivado de fallas en la seguridad de sistemas tecnológicos o asociados.
- **Riesgo de seguridad de la información:** Potencial para que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- **Seguridad de la información:** “Preservación de la confidencialidad, la integridad y disponibilidad de la información, abarca también la autenticidad,

responsabilidad, fiabilidad y no repudio."[78]

- **Sistema de gestión de seguridad de la información:** Conjunto de elementos interrelacionados (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **Tratamiento de riesgos:** Proceso de modificar el riesgo, mediante la implementación de controles.
- **Usuario:** Persona, organización, cargo, proceso, equipo de trabajo que genere, obtenga, transforme, conserve o utilice la información en papel o medio digital, físicamente, a través de las redes de datos y los sistemas de información de la organización para propósitos propósito de su labor.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. POLITICA

COBJO SAS BIC y sus consorcios reconocen la importancia de proteger adecuadamente la información de amenazas que vulneren la continuidad del negocio, alineado con las estrategias para alcanzar los objetivos y necesidades de la organización y promoviendo una cultura de cumplimiento y buen uso. Basado en esto, establece el desarrollo de actividades de control para la protección de los activos de información, gestión de riesgos de seguridad de la información, conductas y aplicabilidad, definidos en esta política y que deben ser adoptados por los agentes implicados, que en el ejercicio de sus funciones utilicen información y servicios tecnológicos, a su vez es responsabilidad de estos agentes, reportar los

[78] EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. Bogotá, 2019. p. 33.

incidentes de los que pudiera tener conocimiento, a través de los canales de comunicación establecidos.

De acuerdo con lo anterior, se determinan las siguientes premisas:

- Minimizar el riesgo de las funciones más importantes de la organización.
- Cumplir los principios de seguridad de la información.
- Mantener la confianza de sus clientes, socios y colaboradores.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los agentes implicados de la organización.

6.POLÍTICAS DE SEGURIDAD ESPECIFICAS

6.1 EVALUACIÓN Y CAPACIDAD DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

La organización deberá contar con un proceso para identificar, evaluar, documentar, gestionar y mitigar los riesgos de Seguridad de la Información; dicho proceso se hará por lo menos una vez al año o cuando ocurra algún evento especial, en donde se identificarán riesgos y se evaluará su probabilidad.

La alta Dirección y el profesional TIC deberán alinearse con la gestión de Riesgos de Seguridad de la Información, para identificar el nivel de tolerancia y la capacidad máxima de aceptación del riesgo, considerando el efecto de la naturaleza de sus operaciones y líneas de negocio.

6.2 CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Todos los colaboradores de la organización deben garantizar y asegurar, la confidencialidad, integridad, disponibilidad y privacidad de la información, de tal manera que:

- Solo sea accedida por el personal autorizado.
- Este disponible en el momento que sea requerida.
- Sea accedida legítimamente y utilizada para lo que se autorizó, de acuerdo a la función del solicitante.
- La información no publicable a terceros, alojada en el sistema informático de la organización (SharePoint, Intranet, OneDrive, WorkSpace y demás herramientas) a excepción del contenido público de la página web debe ser tratada de manera que se garantice su confidencialidad.
- Cibjo SAS BIC y sus Consorcios protegerán la privacidad y confidencialidad del tratamiento y protección de datos personales de sus clientes, colaboradores y partes interesadas, que recopile en sus bases de datos de información, conforme a la ley 1581 de 2012 y de acuerdo con lo establecido en la *política de tratamiento y protección de datos personales*. Esta política es apoyada por los acuerdos de confidencialidad de la información que se firma con los proveedores e internamente con colaboradores de la organización.
- No se permite el envío de información que sea considerada confidencial o reservada a terceros, ni entre usuarios de la misma organización de diferentes procesos; en caso de ser requerido, se deberá solicitar por medio de mesa de ayuda junto con la autorización del jefe directo para así llevar a cabo la gestión.
- Cuando se devuelva un equipo al proveedor o se liberen dispositivos de almacenamiento, es responsabilidad del equipo TIC, asegurarse que la

información contenida en estos sea eliminada totalmente. Cuando se presente daño físico del dispositivo de almacenamiento, se deberán realizar acciones sobre este que imposibilite la recuperación de información.

- Es responsabilidad del usuario almacenar la información en las herramientas corporativas en la nube (SharePoint, One Drive) dispuestas para tal fin. El equipo TIC no se responsabiliza por información almacenada localmente en los equipos asignados.
- En los casos de sincronización de las herramientas como One Drive y SharePoint en los equipos corporativos, es responsabilidad del usuario el monitoreo continuo del correcto funcionamiento para garantizar que efectivamente la información esta alojada en la nube y no en el equipo localmente.
- No está permitido la sincronización de las herramientas corporativas de office 365 y WorsSpace de Google en los equipos personales de los usuarios.
- Los dispositivos asignados deben ser utilizados exclusivamente para actividades laborales.
- Es responsabilidad de los jefes, directores de procesos o proyectos, verificar al retiro de un colaborador o contratista de la organización, que el trabajo realizado se encuentre almacenado en la nube.

6.3 CONTROLAR Y MITIGAR

CIBJO SAS BIC, debe contar con controles generales de accesos, privilegios y actualizaciones en los siguientes aspectos mínimos:

6.4 CONTROL DE ACCESO FÍSICO: (OFICINAS E INSTALACIONES FÍSICAS).

- Para el acceso de la oficina en el Edificio Elemento, se deberá enviar un correo electrónico al jefe de infraestructura con los datos de las personas a

autorizar el ingreso (Nombre completo, número de identificación, proyecto, cargo). Para el caso de un usuario frecuente, se deberá gestionar la asignación de tarjeta de acceso y registro en el dispositivo biométrico para tal fin.

- Para usuarios frecuentes en edificio elemento, el jefe de infraestructura registra el usuario en la herramienta de control de acceso (Biométrico u otro) para así asignar o denegar el acceso a la oficina.
- El cuarto de datos de la oficina Elemento deberá permanecer cerrado con llave y acceso restringido, cuando sea requerido el acceso de terceros a este, el usuario deberá solicitar el acceso por mesa de ayuda para su registro y control; una vez aprobado el acceso, el tercero debe ser acompañado por un responsable del área TIC.
- Los responsables del área TIC serán los encargados de agendar y organizar al personal de mantenimiento preventivo y correctivo de los equipos de cómputo y dispositivos activos.
- En las oficinas de los proyectos o campamentos, se debe contar como mínimo, con un gabinete de telecomunicaciones para el alojamiento seguro de los dispositivos activos, el cual deberá permanecer cerrado con llave y acceso restringido; cuando se requiera el acceso de terceros, el usuario solicitará el permiso a través de la mesa de ayuda con la debida justificación y la aprobación del director del proyecto.
- El personal del área TIC es el único autorizado para mover, cambiar o extraer equipos del centro de cómputo de la oficina Elemento u otras oficinas de la organización.
- No está permitido el ingreso y consumo de alimentos o bebidas en el centro de cómputo de la oficina Elemento u otras oficinas donde aplique.
- Por ningún motivo se almacenarán equipos o elementos que no tengan una función de telecomunicaciones o administración de servicios en el centro de cómputo en la oficina Elemento u otras oficinas donde aplique.

6.5 CONTROL DE ACCESO LÓGICO

CIBJO SAS BIC y sus consorcios garantizarán la seguridad en el intercambio de información, por medio de los únicos medios autorizados para enviar y recibir mensajes los cuales corresponden al correo corporativo y mensajería instantánea Teams, se prohíbe el uso de correos personales, plataformas gratuitas para envió de información corporativa y creación de correos alternos, utilizando el nombre de la compañía o del contrato para el cual se encuentra laborando.

El responsable del proceso de TIC será encargado de asignar los recursos informáticos corporativos y brindar la capacitación para el correcto uso de estos.

Es responsabilidad de los jefes, directores de procesos o proyectos:

- Solicitar los recursos tecnológicos requeridos al ingreso de un colaborador, especificando a que sitios debe tener accesos y su nivel de permiso (lectura o edición) por medio del formato de *requisición F-CC-03* con una antelación mínima de cinco (5) días hábiles.
- Reportar por mesa de ayuda, cuando un usuario cambie de proyecto o proceso dentro de la organización, para realizar el cambio respectivo de los accesos a los diferentes sitios y centros de costos.
- Reportar inmediatamente al área de tecnología por medio de mesa de ayuda, la fecha de retiro de un colaborador, con el fin de denegar los accesos correspondientes.

Es deber de los usuarios:

- Bloquear la sesión cuando el equipo se quede desatendido, con el objetivo de evitar el acceso a este por parte de otra persona.
- Mantener el puesto de trabajo siempre limpio y ordenado, se prohíbe el consumo de bebidas y alimentos en este.

- Utilizar las cuentas de usuario y recursos de cómputo, para ingreso a los sistemas informáticos y exclusivamente para actividades corporativas y laborales, ya que estas son propiedad de CIBJO SAS BIC.
- No compartir las cuentas de acceso a los sistemas y recursos de las tecnologías de información, ya que son para uso exclusivo de único usuario e intransferibles.
- No suministrar el número ID de la herramienta de acceso remoto (Anydesk) a personal diferente del proceso TIC.
- Las solicitudes de soporte técnico se deben registrar en el canal dispuesto para ello: https://cibjo.net.co/

La contraseña para ingresar a Office 365, debe cumplir con:

- Una longitud mínima de 8 caracteres.
- Su configuración debe constar de la combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
- Debe tener una duración mínima de sesenta (60) días.
- No se debe incluir el nombre de usuario o datos asociados al correo asignado.

6.6 CONTROL DE NAVEGACIÓN

- Se deniega el acceso web a plataformas que no correspondan al contexto corporativo como redes sociales, TV en línea, radio en línea, descarga de música, páginas con contenido violento y sexual.

  Como excepción, algunas redes sociales serán permitidas para los procesos de comunicaciones y mercadeo, talento y gestión comercial, en el caso que otro proceso requiera de estas, deberá justificar su uso de acuerdo con sus funciones.

- El proceso de TIC no es responsable por el contenido de datos ni por el tráfico que circule en las plataformas corporativas, la responsabilidad recae directamente sobre el usuario que los genere o solicite, sin embargo, se tomaran medidas para salvaguardar la información.
- Toda solicitud de acceso a información o servicios no incluidos en la configuración inicial de usuario deberá ser solicitada por escrito en mesa de ayuda, justificar el motivo, tipo de permiso (visitante -lector, Integrante - permisos para editar) junto con la aprobación del jefe de área o director de proyecto.
- Los responsables del proceso TIC tendrán la facultad de interrumpir las actividades de los demás usuarios cuando se presenten situaciones que así lo ameriten, ya sea por casos de contingencia, auditoria, monitoreo y/o restablecimiento de servicios.

- Los usuarios deberán solicitar apoyo al proceso de TIC, registrando en mesa de ayuda, cualquier duda, inconveniente o cambio en el manejo de los recursos de cómputo de la organización.

6.7 PROTECCIÓN DE EQUIPOS

Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos informáticos de acuerdo con lo mencionado en este documento:

- El cableado estructurado debe ser protegido contra intercepción, interferencias y posibles daños.
- Los usuarios no están autorizados para mover, readecuar, suprimir o modificar las conexiones eléctricas y de datos.
- Los equipos de cómputo de escritorio deben ser protegidos contra fallas de suministro eléctrico con un sistema de energía ininterrumpido (UPS) o estabilizador.

- Los mantenimientos preventivos periódicos de los equipos de cómputo se deben ejecutar según se acuerde con el proveedor del servicio de alquiler del equipo.
- Los usuarios no están autorizados para realizar limpieza profunda o mantenimiento al equipo asignado.
- Con el fin de evaluar las condiciones técnicas y de funcionalidad de los equipos, anualmente se verificará el estado de obsolescencia; acorde a los resultados obtenidos se tomarán acciones para repotenciar o remplazar los dispositivos, teniendo como base los requerimientos mínimos establecidos para la organización definidos en la ficha técnica, de acuerdo con el *instructivo alistamiento de equipos de cómputo I-TI-01.*
- Una vez asignado el equipo corporativo al usuario, no se acepta el uso de equipos personales para ejecutar su trabajo en la organización.
- Gestión de medios removibles: No está permitido el uso de dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores como memorias USB o discos duros externos, a excepción de los cargos de topografía o comunicaciones y mercado, quienes deben conectar sus herramientas para la ejecución de sus funciones.

  En el caso que el colaborador necesite ser excluido de este lineamiento, deberá diligenciar el *acta de indemnidad*.

- CIBJO SAS BIC y sus consorcios garantizará la adecuada disposición final de los RAEE, el cual se encuentra establecido en el Plan de Gestión de Residuos.

6.8 CONTROL DE USO DE SOFTWARE

- CIBJO SAS BIC cumple con los derechos de autor de software, ya que los programas instalados en los equipos corporativos cuentan con su debida licencia, son de uso libre o en su defecto se instalan versiones de prueba.

- El software licenciado o adquirido por la organización, no debe proporcionarse a personas u organizaciones externas o usarse con fines de lucro.
- Cualquier solicitud para instalación de software en equipos de cómputo, debe ser solicitada en la mesa de ayuda; el responsable del caso deberá estudiar dicha solicitud y verificar si cuenta con aprobación o rechazo.
- En ninguna circunstancia el usuario está autorizado para instalar software en el equipo corporativo asignado.

6.9 SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN SITUACIONES DE CONTINGENCIA

El responsable de Seguridad de la información de la organización deberá implementar planes de continuidad del negocio que garanticen los principios básicos de la Seguridad de la Información.

6.10 SUPERVISAR LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Alta Dirección debe aprobar y revisar periódicamente la “Gestión de Seguridad de la Información” para asegurarse de que las políticas, procesos y sistemas se aplican eficazmente.

6.11 GESTIONAR EL CAMBIO

Una vez evaluado el riesgo y se requiera la planificación de actividades que permitan subsanar una brecha o mejora, se debe seguir el procedimiento de *gestión del cambio**,** P-GI-06.*

6.12 REALIZAR SEGUIMIENTO

El profesional TIC debe monitorear regularmente la evolución de los controles implementados con el fin de verificar su eficacia.

6.13 INVESTIGACIÓN Y SANCIONES

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la empresa CIBJO SAS BIC, sus consorcios y sus agentes implicados, el incumplimiento de esta y demás actividades que se deriven de ella traerá consigo las consecuencias disciplinarias y legales que apliquen de acuerdo con el *Reglamento Interno de Trabajo de la organización, código de ética y conducta DG-GE-03* y legislación colombiana.

7. CONTROL DE CAMBIOS

Versión	**Fecha**	**Cambios realizados**
01	Diciembre/2022	Versión inicial

Anexo E. Socialización de política de Seguridad de la Información y Ciberseguridad.

Fuente. El autor.

Anexo F. Formato F-7-9-1 Proyecto Aplicado

1. INFORMACIÓN GENERAL DE LA PROPUESTA DE TRABAJO DE GRADO PROYECTO APLICADO (SE EXCLUYE PROYECTO EMPRENDIMIENTO EMPRESARIAL)

Fecha:	21/04/2023
Título de la propuesta:	Plan de Seguridad Informática para Empresa Colombiana de Ingeniería Civil CIBJO SAS BIC

INTEGRANTES DE LA PROPUESTA DE INVESTIGACIÓN (MÀXIMO 3 ESTUDIANTES)

bre del iante:	Andrea Franco Cortés								
ficación	C.C.	X	C.E		OTRO		Número:	52906406	
ama Académico	Especialización en Seguridad informática						No. de Créditos Aprobados:		
							% de créditos aprobados		
o electrónico	afrancoco@unadvirtual.edu.co		Teléfono / Celular	7566568		313225838			
ción encia:	Calle 42 F Sur # 72 I 76 Int:3 Apto: 102			Municipio / Departamento		Bogotá Cundinamarca			
TRO:	Bogotá - Cundinamarca			ZONA:		CEAD José Acevedo y Gómez			

bre del estudiante:									
ficación	C.C.		C.E		OTRO		Número:		
ama Académico							No. de Créditos Aprobados:		
							% de créditos aprobados		
o electrónico			Teléfono / Celular						
ción residencia:				Municipio / Departamento					
TRO:				ZONA:					

bre del estudiante:									
ficación	C.C.		C.E		OTRO		Número:		
ama Académico							No. de Créditos Aprobados:		
							% de créditos aprobados		
o electrónico			Teléfono / Celular						
ción residencia:				Municipio / Departamento					
TRO:				ZONA:					

2. DATOS ESPECÍFICOS DEL PROYECTO

Duración del proyecto (meses)	**12**
Línea de Investigación de escuela o Línea de profundización del programa	Infraestructura Tecnológica y Seguridad en Redes
Escuela	Escuela de Ciencias Básicas, Tecnología e Ingeniería
Descriptores palabras claves	Vulnerabilidades, riesgos, amenazas, ataques, ciberespacio, SoA.

3. RESUMEN

En el presente proyecto se concibe la problemática actual de brechas y vulnerabilidades de seguridad Informática de una mediana empresa colombiana, CIBJO SAS BIC, de ingeniería civil con 44 años de experiencia y presencia en el 90 % en el territorio colombiano, experta en todo el ciclo de vida de proyectos de ingeniería civil, participa en la planeación, construcción, operación y mantenimiento de cualquier iniciativa. Certificada con las normas ISO 9001, 14001, 45001. Conformada por 500 colaboradores con la visión de en el año 2026 alcanzar los 800 para convertirse en una grande empresa.

Mediante una auditoria al área de Tecnología de la organización con una entidad externa, basada en los criterios definidos según las mejores prácticas por cada componente de control (ISO 27001: Sistema Gestión de Seguridad de la Información), los cuales se encuentran orientados a percibir el ambiente de control de T.I. y S.I. en la organización. La evaluación se basó en la aplicación de técnicas de entrevistas, y se soportó con análisis documental, sin ejecución de pruebas. Como resultado se obtuvo el diagnostico, mediante la calificación según el Modelo de Madurez de COBIT.

Se identificó el estado actual de la Seguridad Informática de la organización, en el Nivel de madurez 1: Los procesos son ad-hoc, es decir, no se tiene definido un orden para la ejecución de las tareas.

Tomando como punto de partida el diagnostico actual de la organización, se reconoce la importancia de mejorar la seguridad informática en la organización. Con este proyecto se presenta un Plan de Seguridad Informática para implantar los controles de seguridad requeridos adoptando las mejores prácticas, tomando como referente la familia de la norma ISO 27001:2013, ISO 27002 que permita gestionar los riesgos y llevar a la organización a un nivel aceptable.

4. PLANTEAMIENTO DEL PROBLEMA

Con el crecimiento acelerado de la tecnología y la necesidad de interconexión de los dispositivos, las empresas basan sus actividades en sistemas de información apoyadas en la tecnología. Según Alberto Samuel Yahai, presidente ejecutivo CCIT “El cibercrimen ha experimentado un crecimiento durante los últimos años casi de forma paralela al uso de las nuevas tecnologías y las pérdidas generadas por los ciberataques sitúan a esta problemática como una de las principales economías ilegales en el País” Esto preocupa tanto a las empresas como a los usuarios debido a que son de los ataques con mayor potencial de daño económico e informático que puede producir perdidas en la fiabilidad de sus datos o información. Estas son las consecuencias negativas del desarrollo acelerado de la tecnología y el internet de las cosas. En la empresa CIBJO, se ha detectado la dificultad en la gestión de los sistemas de información, al no tener un modelo de seguridad informática implementado, se presentan brechas de seguridad, vulnerabilidades expuestas que pueden ser explotadas.

¿Cómo mejorar la gestión de la Seguridad Informática en una organización?

5. JUSTIFICACIÓN

Con la ejecución de este proyecto, se beneficia considerablemente toda la organización, permitiéndole identificar los riesgos, establecer políticas, procedimientos, controles, contemplando los principios básicos para la protección adecuada de la información que brinden un nivel de seguridad aceptable. De no tomarse las medidas pertinentes e inmediatas CIBJO SAS BIC, no estará preparada a nivel de infraestructura física ni lógica para responder a un incidente digital o ciberataque que puede ocurrir en cualquier memento. Es el caso de esta organización y de otras empresas colombianas que ven sin preocupación la posibilidad de convertirse en el blanco de algún ataque cibernético.

6. OBJETIVO GENERAL

Proponer un Plan de Seguridad Informática para la empresa CIBJO SAS BIC, mediante aplicación de controles y buenas prácticas de seguridad que permita reducir los riesgos y llevarlos a un nivel aceptable.

7. OBJETIVOS ESPECÍFICOS

- Analizar la situación actual de la empresa CIBJO SAS BIC para establecer el nivel de madurez deseado.
- Elaborar inventario de activos y evaluar el riesgo para su tratamiento y minimizar la exposición de este.
- Proponer Plan Estratégico de Seguridad Informática, mediante controles y proyectos alineados a la organización.
- Sustentar proyectos propuestos a la Alta Dirección de la organización para aprobación y ejecución.

8. MARCO CONCEPTUAL Y TEÓRICO

En el mundo moderno donde ha incrementado exponencialmente la interacción con dispositivos tecnológicos y la conectividad de redes, así como el uso de diversas plataformas, sistemas operativos, entre otros que favorecen la productividad, el comercio, son muchos los beneficios que se obtienen de la tecnología, especialmente para las organizaciones empresariales. Álvarez redacta que en el "Reglamento 460/2004 de la comunidad europea sobre la creación de la Agencia Europea de la seguridad de las redes y la información "Las redes y sistemas de información se han convertido en un factor esencial del desarrollo económico y social, como ha ocurrido el suministro del agua y la electricidad, por consiguiente, su disponibilidad, es un asunto que preocupa cada vez más a la sociedad" [79]

Así mismo existe un riesgo al interactuar en la red más grande del mundo conocida como internet, generando potenciales amenazas. Álvarez afirma que "Por desgracia paralelamente el al crecimiento del uso de la informática y las redes de comunicaciones, se multiplica el número de incidentes de seguridad, cuan mayor es el volumen de información procesado mayor es el riesgo derivado de su perdida" [80]

Según Uribe: Un gran problema es que de manera frecuente surgen nuevos tipos de incidentes relacionados con la seguridad informática. Debido a ello se ve la necesidad crear grupos con el objetivo de ayudar a mitigar los incidentes de seguridad informática y que posteriormente se preocuparon por prevenirlos son los CSIRTs. Han sido adoptados por diferentes países en el mundo como una de las opciones más viables para combatir a las organizaciones criminales. Sin embargo, se identificó que no existen muchas publicaciones acerca de cómo crear o establecer servicios en un CSIRT.[81]

Se pregunta Baca ¿Por qué hay personas mal intencionadas que buscan dañar, robar o destruir la información de las empresas o de los usuarios de un ordenador? En diversos casos se

[79] ÁLVAREZ MARAÑON, Gonzalo. Seguridad informática para empresas y particulares. [digital]. España: McGraw-Hill, 2004. 442p. [Consultado el 20 de agosto de 2021].
[80] Ibid., p. 31

[81] URIBE RAYAS, Edgar Felipe. Proceso para la Definición de Servicios Iniciales en un equipo de Respuesta ante Incidencias de Seguridad informática (CSIRT). Zacatecas: 2014. p.2. [en

presume que solo es para demostrar que socialmente son mucho más ingeniosos y creativos que la "gente buena" que esta del otro lado de la mesa. Desde luego hay unos que lo ejecutan por dinero, por ejemplo, robar secretos tecnológicos a otras empresas para venderlos al mejor postor o competencia o extraer números de cuentas o claves bancarias para vaciar cuentas, hacer trasferencias bancarias y miles de acciones maliciosas más.
[82]

Existen diferentes tipos de ataques, de acuerdo con Gómez:
Ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, ataques pasivos, que limitan a registrar el uso de los recursos y/o acceder a la información guardada o trasmitida por el sistema.
Gómez También nos relaciona algunos de los ataques:

• Actividades de reconocimiento de sistemas: Persiguen obtener información previa sobre las organizaciones, redes y sistema informáticos, realizando un escaneo de puertos para determinar servicios que se encuentren activos. "Los atacantes utilizarán esta información para tratar de explorar las vulnerabilidades potenciales del sistema"
• Detección de vulnerabilidades e los sistemas: Tratan de detectar y documentar las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como exploits).
• Robo de información mediante la interceptación de mensajes: Tratando e interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores, vulnerando de este modo la confidencialidad y la privacidad de los usuarios.
• Modificación del contenido y secuencia de los mensajes transmitidos: Los intrusos tratan de enviar mensajes y documentos que ya habían sido enviado por el sistema, tras haberlos modificado de forma maliciosa (ejemplo para generar nueva transferencia bancaria) se conocen como ataques de repetición.
• Ataques de suplantación de identidad: La más conocida denominada IP Spoofing (enmascaramiento de la dirección IP), Mediante la cual el atacante consigue modificar la cabecera de los paquetes enviados para similar que proceden de un equipo distinto al que verdaderamente lo ha originado.
• Captura de cuentas de usuario y contraseñas: También es posible suplantar la identidad de los usuarios mediante herramientas que permitan capturar sus contraseñas, como programas de software espía. [83]

Los anteriores son una pequeña lista, en realidad hay una gran cantidad de diferentes técnicas y modalidades de ataques para los cuales los especialistas, administradores de sistemas informáticos deben estar preparados y capacitarse continuamente para batallar ante esta problemática.

Según Baca: Es esencial que los futuros expertos en informática conozcan y se preparen en cómo controlar y mejorar la seguridad informática de una empresa y la propia. Se deben capacitar no sólo los riesgos físicos y lógicos a los que están expuestos todos los sistemas informáticos empresariales y computadoras personales, sino la forma en que puede disminuirse la probabilidad de ocurrencia de tales riesgos. De igual modo existen mecanismos que se han ideado para proteger de riesgos lógicos, las transacciones económicas internacionales, así como las que protecciones comunes toda empresa debe adquirir para resguardar sus datos, como los firewalls y una serie de dispositivos que pueden rastrear y detectar cualquier vulnerabilidad que tenga el sistema informático, con los cuales dicha vulnerabilidad pueda

[82] BACA URBINA. Gabriel. introducción a la seguridad informática. México: Patria, 2016. p. 9.
[83] GÓMEZ VIEITES. Álvaro. Gestión de incidentes de seguridad informática. RA-MA, 2016. p. 26

disminuirse. Además, de realizar auditorías informáticas e informática forense. [84] De acuerdo con Escrivá la mayoría de los expertos coinciden en que no existe ningún sistema totalmente seguro e infalible al 100%, se debe tratar de proteger la información y el sistema que la utiliza para ofrecer un nivel de seguridad razonable.
Para que se pueda considerar razonablemente seguro se debe garantizar que se cumplen los principios básicos de la seguridad informática:
• Integridad: Es un principio básico, consiste en garantizar que la información solo pueda ser alterada por las personas autorizadas o usuarios legítimos.
• Confidencialidad: Garantiza que la información solo es accesible e interpretada por personas o sistemas autorizados.
• Disponibilidad: Asegurar que la información es accesible en el momento adecuado para los usuarios legítimos. [85]

Se concluye que toda organización independientemente de su tamaño o core de negocio debería implementar un Sistema de Gestión de Seguridad Informática el cual permitirá identificar los riesgos y gestionar los controles necesarios de una manera adecuada para que su sistema sea lo razonablemente seguro.

9. METODOLOGÍA

El desarrollo del proyecto se llevará a cabo mediante la ejecución de cuatro etapas principales, las cuales contemplan actividades puntuales:

Etapa 1. Análisis y evaluación del estado actual de la organización:

- Basados en el diagnostico que ya posee la organización, conociendo el nivel de madurez actual se contextualiza para fortalecer cada dominio evaluado.

Etapa 2. Análisis del Riesgo:

- Identificación de activos y valoración de estos.
- Evaluación del riesgo mediante metodología Magerit.
- Análisis de los controles ISO/IEC 27001:2013
- Recomendaciones técnicas para el análisis de vulnerabilidades de los sistemas de información con herramientas opensource.

Etapa 3. Plan director:

- Estructurar Política de Seguridad de la Información.
- Priorizar y proponer proyectos de acuerdo con la evaluación del riesgo y vulnerabilidades.
- Establecimiento de hoja de ruta. (Proyecto, presupuesto, tiempo).

Etapa 4. Presentación de resultados

- Presentar el Plan Estratégico de Seguridad Informática a la alta dirección de CIBJO SAS BIC.

[84] BACA URBINA. Gabriel. introducción a la seguridad informática. México: Patria, 2016. p. 9.

[85] Escrivá Gasco. Gema. Seguridad informática p. 22

10. CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10	MES 11	MES 12
Etapa 1. Análisis y evaluación del estado actual de la organización:												
Etapa 2. Análisis del Riesgo.												
2.1. Identificación de activos y valoración de estos.												
2.3**.** Evaluación del riesgo mediante metodología Magerit.												
2.4 Análisis de los controles ISO/IEC 27001:2013												
2.5 Revisión técnica de vulnerabilidades de sistemas (Ética al Hacking). Mediante herramientas opesource.												
Etapa 3. Plan director:												
3.1 Priorizar y proponer proyectos de acuerdo con la evaluación del riesgo y vulnerabilidades.												
3.2. Establecimiento de hoja de ruta. (Proyecto, presupuesto, tiempo).												
Etapa 4. Presentación de resultados												
4.1 Presentar el Plan Estratégico de Seguridad Informática a la alta												

dirección de CIBJO SAS BIC.												

11. RECURSOS NECESARIO

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Un especialista en seguridad informática. (Valor anual).	$48.000.000
Equipos y Software	Alquiler de un equipo de cómputo para cada recurso humano incluye office. (Anual)	$2.400.000
	Alquiler de computador para laboratorio y análisis de pruebas de intrusión y hacking. (cuatro meses)	$1.000.000
	Software Opensource	$0
Materiales y suministros	Papelería, medios magnéticos, otros	$500.000
Bibliografía	Bases de datos Biblioteca UNAD	0
Viajes y Salidas de Campo	Transporte publico	$3.000.000
TOTAL		$54.900.000

12. RESULTADOS O PRODUCTOS ESPERADOS

RESULTADO/PRODUCTO ESPERADO	INDICADOR	BENEFICIARIO
Mitigar brechas de seguridad de la empresa Joyce S.A.S BIC.	Mediante la aprobación y ejecución del Plan de Seguridad Informática: Seguimiento a la evolución de los controles propuestos.	Cibjo S.A.S BIC
Concientización a todos los miembros de la organización.	Capacitación en Ciberseguridad.	Cibjo S.A.S BIC
Proyecto ejecutado aplicando conocimientos adquiridos en la Especialización de Seguridad informática	Sustentación de proyecto.	Estudiante (Andrea Franco Cortés).

13. BIBLIOGRAFÍA

ÁLVAREZ MARAÑON, Gonzalo. Seguridad informática para empresas y particulares. [digital]. España: McGraw-Hill, 2004. 442p. [Consultado el 20 de agosto de 2021].

BACA URBINA. Gabriel. Introducción a la seguridad informática. [en línea]. Primera Edición. México: Patria, 2016. 361p. [Consultado el 05 de septiembre de 2021]. Disponible en: https://books.google.com.co/books?id=IhUhDgAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

ESCRIVÁ GASCO. Gema. Seguridad informática. Macmillan. p. 218p. [digital]. [Consultado el 18 de agosto de 2021]. ICONTEC. Norma Técnica Colombiana NTC-ISO 31000. Gestión del Riesgo Principios y Directrices. [Libro Digital] Bogotá. (22 de febrero de 2011). pp.3. [Consultado el 01 de abril de 2023].

EQUIPO DE POLICIA NACIONAL, ALIADOS ESTRATEGICOS, EQUIPO DE INVESTIGACIÓN. Tendencias Cibercrimen Colombia 2019 – 2020. [en línea]. Bogotá: (29 de octubre del 2019). P. 4 – 7. [Consultado el 15 de septiembre de 2021]. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/#:~:text=Actualmente%2C%20el%2045.5%25%20de%20las,sido%20denunciados%20ante%20la%20fiscal%C3%ADa.

GÓMEZ VIEITES. Álvaro. Gestión de incidentes de seguridad informática. [digital]. Madrid: RA-MA, 2015. 124p. [Consultado el 19 de septiembre de 2021].

URIBE RAYAS, Edgar Felipe. Proceso para la Definición de Servicios Iniciales en un equipo de Respuesta ante Incidencias de Seguridad informática (CSIRT). Zacatecas: 2014. p.2. [en línea]. [Consultado el 01 de septiembre de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/39405/deurregof.pdf?sequence=1

DECLARACIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

Los autores de la presente propuesta manifestamos que conocemos el contenido del Acuerdo 06 de 2008, Estatuto de Propiedad Intelectual de la UNAD, Artículo 39 referente a la cesión voluntaria y libre de los derechos de propiedad intelectual de los productos generados a partir de la presente propuesta. Asimismo, conocemos el contenido del Artículo 40 del mismo Acuerdo, relacionado con la autorización de uso del trabajo para fines de consulta y mención en los catálogos bibliográficos de la UNAD.

INSTRUCCIONES DE DILIGENCIAMIENTO	
IMPORTANTE: Este formato debe ser diligenciado en procesador de texto o esfero negro con letra legible. Este formato debe ser diligenciado por el estudiante que presenta la propuesta de proyecto aplicado, en las modalidades Proyecto de Desarrollo Tecnológico, Proyecto de Desarrollo Social y Diagnósticos. No aplica para opción de Proyecto de Emprendimiento Empresarial. La extensión máxima de la propuesta debe ser de 10 páginas. El número máximo de estudiantes a presentar la propuesta son 3 estudiantes. Los estudiantes que presentan la propuesta de Proyecto Aplicado son responsables de la información aquí consignada en cuanto a su carácter inédito, autenticidad y el respeto de la propiedad intelectual.	
1	Responda en forma clara los datos de la información general de la propuesta de trabajo de grado aplicado (se excluye proyecto emprendimiento empresarial) Tenga en cuenta que el título de la propuesta debe ser corto, claro, conciso e indicar la naturaleza del proyecto y el área de aplicación.
2	Responda en forma clara y completa la información sobre los datos específicos del proyecto.

3	El resumen debe tener un máximo de 200 palabras y contener la información necesaria y precisa de la pertinencia y calidad del proyecto, debe contener una síntesis del problema, el marco teórico, objetivos, la metodología a utilizar y resultados esperados.
4	El planteamiento del problema debe describir el problema que se espera resolver con el desarrollo del proyecto, si se tienen datos reales es importantes analizarlos, debe formularse claramente la pregunta concreta que motivan la propuesta y que se quiere responder, en el contexto del problema a cuya solución o entendimiento se contribuirá con la ejecución del proyecto. Se recomienda, además, hacer una descripción precisa y completa de la naturaleza y magnitud del problema que se espera resolver con el desarrollo del proyecto, aportando indicadores cuantificables de la situación actual y futura.
5	Debe presentarse la justificación desde la relevancia y pertinencia del proyecto aplicado en función de la necesidad o naturaleza del problema. Es importante mencionar las razones del por qué se pretende realizar el proyecto aplicado. En general, se deben exponer las razones de pertinencia en lo académico o disciplinario, en lo social y en lo personal.
6	El Objetivo General Deben estar relacionados de manera consistente con descripción del problema. Se recomienda formular un solo objetivo general, coherente con el problema planteado, y los objetivos específicos necesarios para lograr el objetivo general.
7	Los Objetivos Específicos deben estar relacionados de manera consistente con descripción de la idea de negocio. Deben ser coherentes con el producto o servicio que fundamenta el proyecto de emprendimiento (¿Qué? ¿Cómo? ¿Para qué? ¿Quién? ¿Por qué? de la idea de negocio) y los necesarios para lograr el objetivo general. Estos últimos deben ser alcanzables con la metodología propuesta.
8	Marco Conceptual y Teórico debe realizarse una revisión del conjunto de conocimientos, técnicas y metodologías existentes para desarrollar el proyecto, se presenta donde se ubica el problema y de qué forma la propuesta contribuirá a la solución o al desarrollo del sector de aplicación interesado.
9	La Metodología debe contener información detallada de: • ¿Cómo planea desarrollar el proyecto de aplicación? • ¿Cuáles técnicas y herramientas de análisis emplearán? Además, se deben describir los métodos de recolección de datos, controles a introducir, métodos de estadística, tipo de análisis, etc. Para la propuesta del proyecto de desarrollo tecnológico, debe contemplar las demás fases propias de este tipo de proyecto: ➢ La creación del nuevo producto o proceso. ➢ Las pruebas experimentales y ensayos necesarios para su concreción. La elaboración de prototipos previos al inicio de la explotación industrial y comercial.
10	El cronograma de actividades es relación de actividades a realizar en función del tiempo (meses), en el periodo de ejecución del proyecto.
11	En los recursos necesarios Se deben relacionar de manera detallada los recursos académicos, administrativos, técnicos, entre otros. De igual forma, el estudiante deberá establecer cómo serán adquiridos (propios, UNAD, empresa).
12	Resultados o productos esperados, estos deben ser coherentes con los objetivos específicos y con la metodología planteada. Los resultados/productos son hechos concretos, tangibles, medibles, verificables y pueden ser expresados por medio de indicadores de tipo cuantitativo y cualitativo. Enumere los resultados verificables que se alcanzarán durante el desarrollo del proyecto.
13	En la Bibliografía debe incluir las fuentes de información básicas utilizadas para construir la propuesta.

Anexo G. Autorización de la Empresa

Bogotá DC, 2023
03-04-23/TIC
TIC

Señor
LUIS VARTO
Jefe TIC
Dirección: Av. Calle 68 N.
Bogotá, Colombia

Referencia:

1. Autorización para Propuesta Plan de Seguridad informática para la Empresa.

Respectado Ingeniero,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia “UNAD”. Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a Cibjo S.A.S BIC, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: Plan de Seguridad Informática para Empresa Colombiana de Ingeniería Civil CIBJO SAS BIC, el cual se encuentra avalado por parte la Institución de educación superior “UNAD”.

El proyecto en su objetivo general describe lo siguiente: “Proponer un Plan de Seguridad Informática para la Empresa CIBJO SAS BIC, mediante la aplicación de controles y buenas prácticas de seguridad que permita reducir los riesgos y llevarlos a un nivel aceptable.”; al mismo tiempo será apoyado por los objetivos específicos:

- Analizar la situación actual de la empresa CIBJO SAS BIC para establecer el nivel de madurez deseado.
- Elaborar inventario de activos y evaluar el riesgo para su tratamiento y minimizar la exposición de este.
- Proponer Plan Estratégico de Seguridad Informática, mediante controles y proyectos alineados a la organización.
- Justificar el plan propuesto a la Alta Dirección de la organización para aprobación y ejecución.

Para obtener como resultado un impacto positivo en la gestión de la seguridad de la organización.

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por CIBJO S.A.S BIC.

- La empresa CIBJO S.A.S BIC deberá establecer qué tipo de información es privada y cuál es pública para delimitar el acceso de pruebas en la ejecución del proyecto.

- La solicitud de información al igual que ejecución de pruebas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.

- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.

- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia “UNAD”. El documento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrera profesional.

Firman en Bogotá D.C., a los (20) días del mes de (abril) de 2023

Cordialmente,

Andrea Franco Cortés.	**Luis Varto**
Estudiante UNAD	**Jefe TIC**
C.C. 52.906.406 de Bogotá	C.C. 71.586.911 de Bogotá