DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI PARA LA EMPRESA GOTALK SAS CON BASE A LA NORMA ISO 27001:2013

JULY ESTEFANIA VARGAS MACIAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MADRID, CUNDINAMARCA
2023

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI PARA LA EMPRESA GOTALK SAS CON BASE A LA NORMA ISO 27001:2013

JULY ESTEFANIA VARGAS MACIAS

Proyecto de Grado – Proyecto Aplicado

JOSE HERNANDO PEÑA HIDALGO
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MADRID, CUNDINAMARCA
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad y Fecha (11, septiembre, 2023)

DEDICATORIA

Por mi lado espiritual primero agradezco a Dios, por darme la sabiduría y la vida para cursar esta etapa académica permitiéndome crecer profesionalmente, de igual manera agradezco a mi familia por su apoyo incondicional, su acompañamiento indirecto durante esta etapa, brindando tranquilidad y paciencia para lograr con éxitos este reto académico.

AGRADECIMIENTOS

Doy mis agradecimientos primero a los tutores, directores, compañeros y personal académico y/o administrativo de la Universidad Nacional Abierta y a Distancia, por su acompañamiento, tutoría, retroalimentación y su educación el cual permite el cierre de esta etapa académica. También agradezco a la empresa GOTALK SAS, que me permitió y aprobó aplicar este proyecto para mi desarrollo profesional.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: es algo que una organización valora y por lo tanto debe proteger.

AMENAZA: a todo elemento o acción capaz de atentar contra la seguridad de la información.

ANÁLISIS DE RIESGO: un proceso que permite identificar las amenazas y vulnerabilidades de una organización con el objetivo de generar controles que minimicen los efectos de los riesgos.

ATAQUE INFORMÁTICO: Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red.

CONFIDENCIALIDAD: equivalente a la privacidad de la información, evitando que personas no autorizadas puedan acceder a la información

DATOS: representación de una variable cuantitativa o cualitativa.

DISPONIBILIDAD: la información y los recursos relacionados estén disponibles para el personal autorizado.

INCIDENTE DE SEGURIDAD: se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.

INFORMACIÓN: Como información denominamos al conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto.

INTEGRIDAD: guardar la totalidad de la información cuyo contenido debe permanecer inalterado a menos que sea modificado por personal autorizado.

MITIGAR: es el proceso de desarrollar opciones y acciones que al ser implementadas pueden mejorar las oportunidades y reducir el impacto negativo o la probabilidad de ocurrencias de un evento en particular.

PHISHING: es un tipo de ataque que proviene de estafadores que se hacen pasar por fuentes de confianza y pueden facilitar el acceso a todo tipo de datos confidenciales.

POLÍTICA DE SEGURIDAD: conjunto de reglas que definen lo que se desea proteger y que se espera de los usuarios del sistema.

RANSOMWARE: es una forma de malware que amenaza con destruir o retener los datos o archivos de la víctima a cambio de un pago monetario para el rescate y restauración de la información.

RIESGO: es cuando existe la posibilidad de que una amenaza se aproveche de las vulnerabilidades puede causar consecuencias e impactar a la organización.

SEGURIDAD DE LA INFORMACIÓN: es aquel conjunto de medidas y técnicas empleadas para controlar y salvaguardar todos los datos que se manejan dentro de una empresa o institución y asegurar que estos no salgan del sistema establecido por la empresa.

VULNERABILIDAD INFORMÁTICA: es una debilidad en el software o en el hardware que permite a un atacante comprometer la integridad, disponibilidad o confidencialidad del sistema o de los datos que procesa.

RESUMEN

Acorde a las necesidades y brechas que se presentan en temas de seguridad de la información en la empresa Gotalk SAS, y que en la actualidad en cuanto al avance la migración de información digital (alojadas y salvaguardas en nube), así mismo avanza las amenazas, vulnerabilidad y ataques cibernéticos, que hace necesario involucrar y conocer la norma ISO 27001:2013, que informa los requisitos de implementar el sistema de gestión de seguridad de la información con la finalidad de fortalecer el sistema de seguridad, lograr su certificación y así dar más valor a la organización.

Con el presente proyecto se busca diseñar el sistema de seguridad de la información teniendo en cuenta sus antecedentes, funcionamiento de la empresa y normatividad, el cual se hará mediante el modelo PHVA incluido en la norma ISO 27001:2013, siguiendo paso a paso lo establecido en el ciclo, con el fin de llevar a cabo el desarrollo de los objetivos propuestos, desde la creación de la políticas de seguridad de la información como la identificación de los activos con los que actualmente cuenta la empresa Gotalk SAS, llevando a cabo la presentación del diseño SGSI frente a la Gerencia para dar cumplimiento con la documentación requerida en la norma ISO 27001:2013.

INTRODUCCIÓN

Partiendo de la triada CIA (Confidencialidad, Integridad y Disponibilidad), conceptos básicos de la ciberseguridad, se hace necesario la protección de la información siendo uno de los activos más importantes de las empresas, regulados bajo normas y estándares como la ISO 27001:2013, que tienen como finalidad regular el debido manejo de la información entregada y administrada por personas naturales y jurídicas; y proteger el derecho a la confidencialidad y privacidad de la información garantizando el buen uso requerido por la empresa.

Conforme al avance al tecnológico, la administración y suministro de la información, ha cambiado de manera sustancial al formato digital mediante el repositorio de servidores en nube o local, registro de datos mediante aplicaciones y/o redes sociales corporativas, entre otras. Generando mayores beneficios a las organizaciones, permitiendo la facilidad en la consulta, resguardo y manejo, ahorrando en costos de espacio y almacenamiento físico.

Sin embargo, con estos beneficios acarrea la atención de los delincuentes cibernéticos e informáticos, buscando y detectando cualquier vulnerabilidad de seguridad, con el fin de apropiarse de la información para motivos económicos o delictivos.

Por consiguiente, se hace primordial y fundamental diseñar el Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa GOTALK SAS, que permita mitigar los riesgos y amenazas de seguridad de la información, basado en el ciclo de Deming (PHVA), que consiste en Planificar- Hacer- Verificar- Actuar.

1. DEFINICIÓN DEL PROBLEMA

Debido a la preocupación expresada por el Gerente de Gotalk SAS frente a los temas de seguridad de la información y quien, en su poco conocimiento respecto al tema, pero quien considera la importancia de cumplir y garantizar la seguridad de la información que se maneja en la empresa sugiere como iniciativa la revisión global del estatus actual de la empresa.

Esto conlleva a realizar la visita a la empresa Gotalk SAS; que, con base a la visita y a la información suministrada por parte de gerencia, se evidencia como la información que se maneja se encuentra en alto riesgo y exposición frente a las vulnerabilidades de seguridad y junto con ello la necesidad de diseñar el sistema de gestión de seguridad de la información.

También se evidencia que el personal administrativo y gerencia no cuenta con capacitación y concientización frente a la seguridad de la información, así como tampoco cuenta con políticas de seguridad establecidas.

Teniendo en cuenta el contexto y funcionamiento de la empresa, administrando y manipulando información sensible como lo son los datos personales de los Estudiantes y Profesores, dicha información se encuentra en línea alijada en servidores que es suministrado por los Estudiantes en el momento de registrarse a la plataforma y realizar sus cursos, de igual manera para los profesores de varios países latinoamericanos y otros continentes. Es importante resaltar el cumplimiento de la Ley 1581 de 2012 de acuerdo con el tratamiento de datos y teniendo como finalidad garantizar la protección de los datos personales.

1.1. ANTECEDENTES DEL PROBLEMA

A medida que la información cada vez más es migrada y administrada de manera digital, encuentran total dependencia del buen funcionamiento de software y servicio en nube que por lo tanto también se presta para la preocupación y crecimiento de ataques cibernéticos con un aprovecho económico. Gotalk SAS establecida en agosto de 2019 y legalmente constituida ante la Cámara de Comercio en marzo de 2020, prestando sus servicios en medio de la pandemia del COVID 19, donde para el año 2019, Colombia fue blanco de más de 40 billones de intentos de ciberataques, donde la mayoría de estos intentos son denominados exploits que son la llave para que los cibercriminales accedan a los sistemas, otro de los ciberataques es el DoublePulsar siendo un troyano empleado para afectar sistemas de institución financiera y vehículo para distribuir malware. También se encuentra los malware que ingresan por correo electrónico y los phishing siendo el ataque más frecuente. Esto es una advertencia para las empresas e instituciones gubernamentales apostar a la ciberseguridad como elemento complementario y necesidad critica para el proceso de transformación digital.[1]

Así como estudios por parte de Fortinet informa que los ataques más utilizados son Ransomware y Phishing generado mayor perdidas, también el informe de Tendencia del Cibercrímenes 2019-2020, el equipo de la Policía Nacional y empresas tecnológicas reportaron un total de 15.948 denuncias[2], esto conlleva a como las empresas con plataforma tecnológica que prestan el servicio de educación, a

[1] Semana. En solo tres meses Colombia sufren 42 billones de intentos de ataques cibernéticas. Colombia: Semana. 2019. p.1.

[2] CCIT. Informe de las Tendencias del Cibercrimen en Colombia 2019-2020. Bogotá: Copyright. 2019. p.1.

plantear las respectivas medidas de seguridad si las adoptadas son suficientes o presentan mayo riesgo, así como el involucrar la capacitación a los usuarios para adecuar la seguridad informática de la manera más pertinente.

1.2. FORMULACIÓN DEL PROBLEMA

De acuerdo con la información suministrada y la revisión de lo actualmente implementado por la empresa GOTALK SAS, no se ha presentado incidentes de seguridad, sin embargo, se evidencia que no cuenta con un SGSI lo que muestra que no se tiene implementada las políticas de seguridad para la protección de la información y tampoco hay concientización frente a la importancia de la protección de la información, lo cual hace que no exista un control sobre el manejo y tratamiento de esta.

Con base al funcionamiento de la empresa obliga a la manipulación de información sensible y confidencial de los estudiantes, docentes y personal administrativo, esta información se encuentra almacenada en las bases de datos de la plataforma, ambiente de desarrollo, gestor de correos, entre otros, donde se evidencia que no se cuenta con un control y proceso documentado para la asignación y configuración de roles de acceso y/o permisos a los diferentes sistemas de información de la empresa, demostrando así las vulnerabilidades y riesgos a los que se enfrenta GOTALK SAS y la no garantía en la protección de la información tratada.

De acuerdo con lo anterior, con el desarrollo del presente proyecto aplicado se busca dar respuesta al interrogante: ¿Cómo el diseño del sistema de gestión de la seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001:2013, ayuda a recibir los riesgos y amenazas de seguridad de la información en la empresa GOTALK SAS?

2. JUSTIFICACIÓN

Actualmente es fundamental y base el aprovechamiento, manejo y administración de la información y ser custodiado en materia de seguridad frente a los posibles ataques con propósitos delictivos con un beneficio propio y/o económico, con la finalidad de causar daño y afectar el buen nombre de las organizaciones.

Por lo anterior, se hace importante la protección del activo más importante (información) independiente del objetivo de la organización. Por lo tanto, con el diseño del SGSI ayuda a Gotalk SAS en primera instancia identificar el inventario de activos con los que cuenta actualmente y conocer los posibles riegos, estableciendo principios y controles para determinar una rápida y eficaz respuesta ante los incidentes de seguridad que se presentan. Tanto el personal administrativo como los estudiantes y profesores tendrán mayor tranquilidad y seguridad frente a la empresa ya que puede garantizar el buen tratamiento de los datos personales de información sensible, ya que con este diseño se implementa la política de seguridad de la información.

Al contar con un sistema de seguridad de la información con base a los estándares internacionales garantiza el buen manejo de los datos minimizando los riesgos, teniendo una mayor probabilidad de certificarse mostrando más valor como empresa frente a la seguridad.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar un SGSI basado en la norma ISO/IEC 27001:2013, para la gestión de la seguridad de la información en la organización GOTALK S.A.S.

3.2. OBJETIVOS ESPECÍFICOS

- Evaluar los activos de información de la organización GOTALK S.A.S mediante la aplicación de metodologías para la medición del riesgo que permita identificar el impacto de las amenazas.

- Proponer las salvaguardas para los activos de información basados en el anexo A de la norma ISO/IEC 27001:2013 para hacer frente a las amenazas identificadas.

- Establecer las políticas de seguridad a partir de buenas prácticas y estándares para la gestión segura de la información.

- Consolidar la documentación mínima requerida para el establecimiento de un SGSI de acuerdo con la norma ISO/IEC 27001:2013 para la gestión de la seguridad en la organización.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

Con base a los tres principios básicos de la seguridad de la información ya establecidos (Confidencialidad, Integridad y Disponibilidad), los cuales orientan a que la información no sea manipulada por usuarios o entidades no autorizadas garantizando la confidencialidad, teniendo en cuenta que los usuarios autorizados tengan el control para las modificaciones haciendo cumplimiento con el principio de integridad y que esté disponible la información a las usuarios o entidades autorizadas.

- **Confidencialidad**: la confidencialidad es aproximadamente equivalente a la privacidad. Las medidas emprendidas para garantizar la confidencialidad están diseñadas para evitar que la información confidencial llegue a las personas equivocadas, al tiempo que se garantiza que las personas adecuadas puedan obtenerla: el acceso debe estar restringido a aquellos autorizados para ver los datos en cuestión. También es común que los datos se clasifiquen de acuerdo con la cantidad y el tipo de daño que se podría hacer si cae en manos no deseadas. Se pueden implementar medidas más o menos estrictas de acuerdo con esas categorías.[3]

- **Integridad**: la integridad implica mantener la consistencia, precisión y confiabilidad de los datos durante todo su ciclo de vida. Los datos no deben modificarse en tránsito, y deben tomarse medidas para garantizar que personas no autorizadas no puedan alterar los datos (por ejemplo, en una violación de la confidencialidad). Estas medidas incluyen permisos de archivos y controles de acceso de usuarios.[4]

- **Disponibilidad**: la disponibilidad se garantiza mejor manteniendo rigurosamente todo el hardware, realizando reparaciones de hardware de inmediato cuando sea necesario y manteniendo un entorno de sistema operativo que funcione correctamente y libre de conflictos de software. También es importante mantenerse al día con todas las actualizaciones necesarias del sistema.[5]

Para el tratamiento de la información como activo valioso para las organización se encuentran parametrizados y establecidos políticas, procedimientos y normas con la finalidad de salvaguardar dicho activo, generando las buenas prácticas y beneficios a la organización como el buen en nombre y garantía de seguridad, también el implementar con suma importancia las charlas y/o capacitaciones para concientizar a todo el personal y cliente el manejo de la normatividad y la seguridad de la información.

Como lo es la norma ISO 27000 que se describe como el conjunto de estándares internacionales sobre la Seguridad de la Información. La familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información.

> Las normas que forman la serie ISO/IEC-27000 son un conjunto de estándares creados y gestionados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación y reconocimiento en todo el mundo.

[3] Ontek. ¿Qué es? Triada CID (confidencialidad, integridad y disponibilidad). p.1.

[4] Ibid. p.1.

[5] Ibid. p.1.

Hoy en día, la información es uno de los activos más importantes de una compañía, por lo que es necesario que esta se encuentre debidamente protegida. Las normas de la familia de ISO 27000 tratan la gestión de la seguridad de la información y pueden ser combinadas para proporcionar un marco reconocido a nivel mundial.[6]

FAMILIA ISO 27000[7]

- **ISO 27000**: facilita las bases y el lenguaje común para el resto de las normas de la serie.
- **ISO 27001**: especifica los requerimientos necesarios para implantar y gestionar un SGSI. Es la norma más importante de la familia y es certificable.
- **ISO 27002:** es soporte del proceso de gestión de riesgos de la norma ISO/IEC-27001, define un conjunto de buenas prácticas para la implantación del SGSI, a través de 93 controles, estructurados en 4 grandes dominios.
- **ISO 27003:** proporciona una guía para la implantación de forma correcta de un SGSI, centrándose en los aspectos importantes para realizar con éxito dicho proceso.
- **ISO 27004:** proporciona pautas orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI.
- **ISO 27005:** define cómo se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información, orientado en cómo establecer la metodología a emplear.
- **ISO 27006:** establece los requisitos que deben cumplir aquellas organizaciones que quieran ser acreditadas para certificar a otras en el cumplimiento de la ISO/IEC-27001.
- **ISO 27007:** es una guía que establece los procedimientos para realizar auditorías internas o externas con el objetivo de verificar y certificar implementaciones de la ISO/IEC-27001.

Tiene como propósito el sistema de gestión de seguridad de la información garantizar que los riesgos de seguridad acorde con los activos de información se minimicen mediante el diseño e implementación de controles y así contrarrestar los incidentes de seguridad.

¿Qué es SGSI?[8]

Toda la información almacenada y procesada por una organización está expuesta ante amenazas de ataque (por intereses comerciales, intelectuales y/o chantaje y extorsión), error (intencionado o por negligencia), ambientales (por ej. inundación o incendio), fallo en los sistemas (de almacenamiento de datos, informáticos, redes telemáticas), entre otras y también está sujeta a vulnerabilidades que representan puntos débiles inherentes a su propio uso en el ciclo de vida representado a continuación.

Permitir que una información precisa y completa esté disponible de manera oportuna para aquellos autorizados que tienen una necesidad es un catalizador para la eficiencia del negocio. Para poder interrelacionar y coordinar las actividades de protección para la seguridad de la información, cada organización necesita establecer su propia política y objetivos para la seguridad de la información dentro de la coherencia del marco de globales de la organización. Una vez fijados los objetivos en seguridad de la información necesitamos asegurar el modo de poder lograrlos eficazmente, en definitiva, un sistema de gestión de la seguridad de la información o SGSI en su forma abreviada.

[6] ALFONSO, Cesar. ISO 27000 y el conjunto de estándares de Seguridad de la. Global Suite Solutions. 2023. p.1.
7 Ibid. p.1.
[8] ISO 2700.SGSI. ISO 2700.ES. p.1.

Por tanto, un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales.

Figura 1. Beneficios de la implementación del SGSI.

Fuente: ISO 2700.SGSI. ISO 2700.ES. p.1.

IMPLANTACIÓN

"Las actividades propias para la implantación inicial de un SGSI y su posterior mantenimiento se deben considerar como un proyecto más que aborda la organización mediante la determinación de unas actividades críticas para el éxito del proyecto que llevan asociadas una planificación con los responsables principales, los recursos necesarios y los posibles riesgos asociados al proyecto".[9]

La siguiente información documentada mínima es requerida para un SGSI atendiendo a las cláusulas del estándar ISO/IEC 27001:2013:[10]

- Alcance SGSI: El alcance del SGSI aclara los límites del SGSI en función del contexto y/o importancia y ubicación de los activos críticos de información de la organización (por ejemplo, unidades, ubicaciones o departamentos) y los riesgos propios o externos asociados (p.ej. leyes y reglamentos, obligaciones contractuales, estrategias y políticas impuestas por organismos centrales).

[9] ISO 2700.SGSI. ISO 2700.ES. p.1.
[10] Ibid. p.1.

- Política del SGSI: Establece y confirma el compromiso de la alta dirección con los objetivos de seguridad de la información de la organización y la mejora continua del SGSI, entre otros posibles aspectos relevantes.

Evaluación de riesgos: Los auditores esperan un proceso estructurado y repetible, es decir, un procedimiento documentado de evaluación de riesgos que explique cómo se identifican, analizan (p. ej. con base a posibles consecuencias y probabilidades de ocurrencia), evalúan (p. ej. aplicando criterios específicos para la aceptación del riesgo) y priorizan los riesgos relacionados con los activos de información más relevantes del alcance (p.ej. en atención a niveles de riesgo definidos).

- Declaración de aplicabilidad: Conocida también como SoA (por sus siglas en inglés) establece los riesgos de información y los controles de seguridad que son relevantes y aplicables al SGSI de su organización, como resultado de la determinación de sus evaluaciones periódicas del riesgo o según lo exijan las leyes, reglamentos o buenas prácticas.

- Tratamiento de riesgos: Proporcionar informes relevantes, los planes de tratamiento de riesgos relacionados con aquellas situaciones no deseadas/inaceptables por la dirección, entradas en su registro de riesgos, métricas, etc. son formas de convencer a los auditores de que el proceso funciona correctamente.

- Objetivos y planes: El requisito de ISO de "retener información documentada sobre los objetivos de seguridad de la información" puede adoptar distintas formas. Un enfoque habitual es comenzar con los compromisos declarados en la política del SGSI ("marco para los objetivos") derivando de ellos el riesgo de la información y los objetivos de seguridad de forma más precisa.
- Competencias: "Retener información documentada como evidencia de la competencia" es muy variable según el tamaño de la organización y el número de personas implicadas en el alcance del SGSI. Confiar en los registros de recursos humanos que documenten la experiencia relevante, habilidades, calificaciones, cursos de capacitación (entre otros) es habitual.

- Planificación y control operacional y métricas: Mantener "información documentada en la medida necesaria para tener la confianza de que los procesos se han llevado a cabo según lo previsto" implica, en términos generales, disponer de información de gestión relacionada con el SGSI. Aunque los detalles varían según la organización, debería ser claramente evidente a partir de la documentación de que el SGSI está en funcionamiento con el nivel de eficacia requerido y con acciones de corrección y/o de mejora según sea oportuno.

- Auditorías internas y revisión por la dirección: Los informes de auditoría interna del SGSI son la evidencia más directa que documenta los principales hallazgos, conclusiones y recomendaciones de la auditoría con la posibilidad de comunicar no conformidades y acciones correctivas, mejoras.

- No conformidades y acciones correctivas: Las no conformidades son requisitos del SGSI parcial o totalmente insatisfechos. El origen de los requisitos es obviamente el estándar ISO/IEC 27001 pero también surgen de las necesidades aplicadas por la propia organización (estrategias, políticas, procedimientos, pautas) o por partes externas a ella (leyes, regulaciones y contratos) en relación con las actividades del alcance del SGSI.

Figura 2. Integración del sistema de gestión.

Fuente: ISO 2700.SGSI. ISO 2700.ES. p.1.

Un SGSI es, en primera instancia, un sistema de gestión, es decir, una herramienta de la que dispone la gerencia para dirigir y controlar un determinado ámbito, en este caso, la seguridad de la información.

Además de ISO 27001, la gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales: se gestiona la calidad según ISO 9001, el impacto medioambiental según ISO 14001 o la prevención de riesgos laborales según ISO 45001 (OHSAS 18001)

“Las facilidades para la integración de las normas ISO son evidentes gracias a la estructura común para la equivalencia en los requisitos similares aplicables a todos los sistemas de gestión en base al Anexo SL, es decir, estructura de publicación en 10 cláusulas principales que desarrolla los elementos comunes en las mismas ubicaciones de norma y requisitos (liderazgo, política, objetivos, recursos, revisión por la dirección, auditorías internas, mejora continua)”.[11]

[11] ISO 2700.SGSI. ISO 2700.ES. p.1

4.2. MARCO CONCEPTUAL

Es importante dar claridad a diferentes conceptos que se levaran acabo para el diseño del SGSI de la empresa GOTALK SAS, como lo son:

- **Vulnerabilidad informática: "**es una debilidad en el software o en el hardware que permite a un atacante comprometer la integridad, disponibilidad o confidencialidad del sistema o de los datos que procesa".[12]

- **Seguridad de la información: "**es aquel conjunto de medidas y técnicas empleadas para controlar y salvaguardar todos los datos que se manejan dentro de una empresa o institución y asegurar que estos no salgan del sistema establecido por la empresa. Es, además, una pieza clave para que las compañías puedan actualmente llevar a cabo sus operaciones, ya que los datos manejados son esenciales para la actividad que desarrollan".[13]

- **Amenaza:** "a todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales".[14]

- **Análisis de riesgo:** "un proceso que permite identificar las amenazas y vulnerabilidades de una organización con el objetivo de generar controles que minimicen los efectos de los riesgos, el cual implica determinar que o cuales activos proteger, de que o de quien hay que protegerlos y cómo hacerlo".[15]

- **Ataque informático:** "Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red".[16]

- **Información:** "Como información denominamos al conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto".[17]

[12] CARISIO, Emanuel. Vulnerabilidad Informática ¿Cómo protegerse? Barcelona: Media PRO. p.1.
[13] Ayudaley. Seguridad de la información: Aspectos para tener en cuenta. Blog Ayudaley protección datos. 2020. p.1.
[14] Departamento de seguridad informática. Amenazas a la seguridad de la información. Argentina: Universidad Nacional de Lujan. p.1.
[15] MOJICA, Manuel y ALVAREZ, Yenny. El análisis de riesgo en la seguridad de la información. Dep. Legal. 2009. p.33.
[16] ECURED. Ataque informático. Ecured.co. p.1
[17] Significados. Significación de la información. Signficados.com. p.1.

- **Incidente de seguridad:** “se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad”.[18]

4.3. MARCO CONTEXTUAL

El proyecto se realizará para la empresa GOTALK SAS.

GOTALK SAS

Es una empresa establecida en agosto del 2019 con premisa de facilitar el acceso al inglés de forma virtual y personalizada a profesionales de habla hispana. Esta se encuentra registrada en la Cámara de Comercio de Bogotá desde el 16 de marzo de 2020 y como una LLC en Delaware Estados Unidos desde septiembre del mismo año; por lo cual se considera una empresa Colombo Americana con la capacidad de recibir pagos tanto en dólares como en pesos colombianos.

Son una plataforma Online Americana, que han reunido amor e interés por los idiomas, formando así una comunidad ansiosa por compartir saberes, crecimiento personal y profesional. Entendiendo que la metodología más acertada y la cual los representa es la personalizada, además añadiendo Clubes Conversacionales grupales.

***Nota**: Inicialmente se llamó GoTalk101 sin embargo este nombre se cambió buscando que la marca tuviera una mayor recordación, por ende, pasó a ser **Bookii** a partir de junio de 2020.*

OBJETIVOS:

- A corto plazo (diciembre 2021): A finales del presente año se espera tener registrados aproximadamente 150 estudiantes principalmente colombianos y chilenos, para ello desde diciembre del 2019 se ha desarrollado una plataforma tecnológica llamada “academy.bookii.co” en la cual los estudiantes pueden agendar clases personalizadas en sus horarios preferidos, tener acceso a material específico, asistir a clubes conversacionales, clases y Webinar grupales.

- Con esta plataforma se pasó de tener 15 usuarios activos a finales del 2019 a un aproximado de 75 a principios del 2021. Además, se espera lanzar a finales del 2012 el servicio de cursos personalizados de español para angloparlantes.

- A mediano plazo (2022- 2023): se busca consolidar el modelo para empresas (B2B) en el cual se pueda llegar a aquellas compañías interesadas en proveer mayor preparación a sus empleados en el idioma inglés tales como compañías de software, hotelería y

[18] MINTIC. Guía para la Gestión y Clasificación de Incidentes de seguridad de la información. Colombia: MINTIC. 2016. p.1.

turismo, consulting entre otras. Con ello se espera alcanzar un mínimo de 500 usuarios a finales del 2022 o mediados del 2023. Para ello se deben aumentar los recursos destinados a almacenamiento de datos y rendimiento de nuestra plataforma, además realizar algunos arreglos para mejorar la imagen y eficiencia de la plataforma, de igual forma se está analizando la viabilidad de una aplicación móvil.

- A largo Plazo: En los próximos se espera tener un posicionamiento sólido como una de las mejores plataformas para el aprendizaje de inglés y español, tomando como principal objetivo el mercado americano.

MISIÓN

Aumentar el nivel de inglés de personas no angloparlantes a lo largo del mundo a través de una metodología innovadora que combina cursos personalizados con espacios grupales online que permitan crear una comunidad internacional con estudiantes y profesores de diferentes países. Siempre comprometidos con la calidad académica y facilidad de uso de las herramientas tecnológicas que permitan a nuestros estudiantes alcanzar sus metas laborales y personales

VISIÓN

Consolidar a Bookii como una de las mejores plataformas para el aprendizaje de inglés y español en el continente americano, esto gracias a su enfoque de alta calidad, su continuo avance tecnológico y alto compromiso con el verdadero aprendizaje de cada estudiante que utilice Bookii.

CALIDAD

Bookii se caracteriza por la calidad de su servicio, la preparación y experiencia de sus profesores, así como su enfoque en un excelente servicio al cliente que haga un seguimiento continuo de la experiencia de cada uno de los estudiantes.

RESPONSABILIDAD

Su compromiso con la sociedad es aportar para conseguir una Colombia y América Latina bilingüe con cursos de altísima calidad. Contando tanto con servicios gratuitos como pagos

CLIENTES

En un principio la mayoría de los clientes estaban en la ciudad de Bogotá, con el lanzamiento de la plataforma web en marzo del 2020 se tuvo un mayor alcance con personas de otras ciudades del país; en agosto del 2020 se hizo una expansión al mercado chileno se tuvo grandes resultados. Actualmente se tienen 80 estudiantes con un plan de pago activo, 65% de ellos en Colombia y 35% en Chile. Además de ello se cuenta con usuarios que asisten a muchos de los conversatorios gratuitos, con lo cual se busca llegar a más personas y a otros países.

PROVEEDORES

El 100% de los profesores son freelance en su mayoría son certificados C1 acorde al marco común europeo, se cuenta con profesores en Filipinas, Sudáfrica, Estados Unidos, Argentina y Colombia.

Bookii utiliza servicios de terceros como Heroku y Atlas MongoDb como hosting de nuestra plataforma web, Twilio como servicio de mensajería móvil entre otros.

SERVICIOS

Bookii ofrece diferentes tipos de cursos de inglés personalizados.

- Cursos estructurados por niveles (11 niveles) acorde al marco común europeo del A1 al B2.

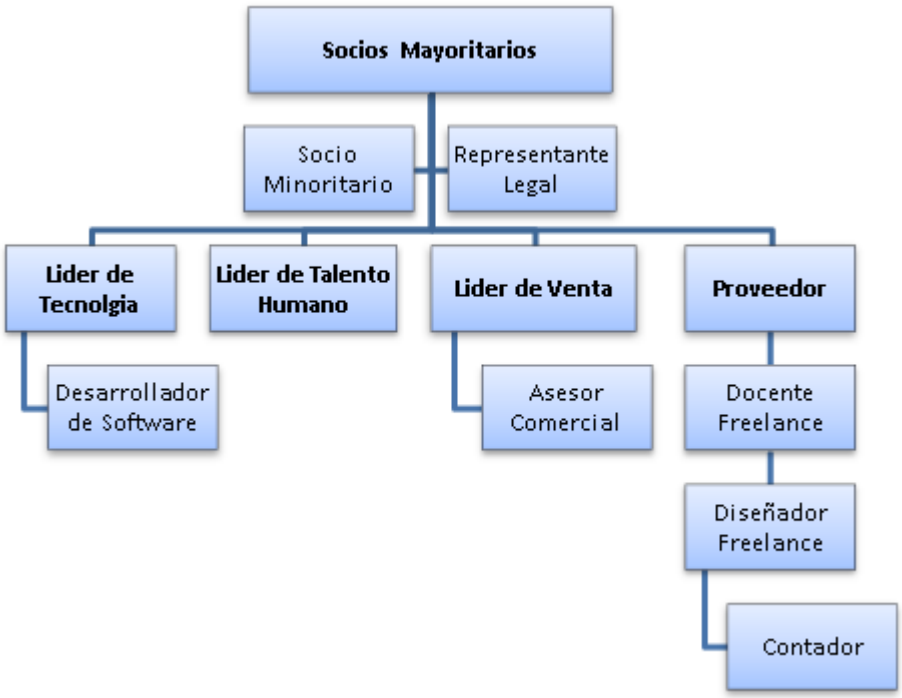
- Cursos de inglés de Negocios para personas nivel intermedio

- Preparaciones para exámenes como IELTS, TOEFL o TOEIC.
    - Cursos Free Talk (conversacionales)
    - Cursos para niños de 5 a 14 años
    - Cursos para adultos de (15 a 70 años)
    - Se ofrece una clase de prueba gratuita con duración de 1 hora conocimiento de la plataforma e interacción con el profesor

Figura 3. Logo Empresa GOTALK SAS

Fuente: Logo Empresa Bookii (GoTalk SAS)

Figura 4. Organigrama de la empresa Gotalk SAS



Fuente: elaboración propia

4.4. ANTECEDENTES O ESTADO ACTUAL

Como inicio al enfoque del proyecto, se hace a partir de la identificación de los activos y el análisis de riesgos. Tal como lo establece la norma ISO 27001:2013 que es fundamental para cada organización interesa en certificarse y fortalecer la gestión de la seguridad información, implementado el sistema de gestión de seguridad de la información para la gestión de riesgos y protección de la información.

Como lo indica la norma en Colombia “Para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con frecuencia, el resultado de un proceso constituye directamente la entrada del proceso siguiente”[19], se denota la importancia que tiene la gestión en los procesos de la empresa GOTALK SAS.

Por lo tanto, como requisito general de acuerdo con la norma NTC-ISO/IEC 27001:2013, “La organización debe establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta.”[20] Con los antecedentes de otras organizaciones se confirma a necesidad de diseñar un sistema de gestión de seguridad de la información.

[19] ICONTEC. Norma Técnica NTC-ISO/IEC Colombiana 27001. Colombia: ICONTEC. 2006. p.I.
[20] Ibid. p.4.

4.5. MARCO LEGAL

Para el desarrollo de este proyecto se basa en la norma de Colombia NTC-ISO/IEC COLOMBIANA 27001:2013. Norma dirigida para ser aplicada por cualquier tipo de organización, especificando los requisitos necesarios para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un sistema de gestión de seguridad de la información SGSI.

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

> El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente. Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se difunda de acuerdo con las necesidades de la organización.[21]

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma.[22]

- **Liderazgo**
  - Liderazgo y compromiso
  - Política
  - Roles, responsabilidades y autoridades en la organización
- **Planificación**
  - Acciones para tratar riesgos y oportunidades
  - Objetivos de seguridad de la información y planes para lograrlos

[21] ICONTEC. Norma Técnica NTC ISO IEC COLOMBIANA 27001. Colombia: ICONTEC. 2013. p. i.
[22] Ibid. p. 2.

- **Soporte**

  - Recursos
  - Competencias
  - Toma de conciencia
  - Conciencia
  - Información documentada

- **Operación**

  - Planificación y control operacional
  - Valoración de riesgos de la seguridad de la información
  - Tratamiento de riesgos de la seguridad de la información
- **Evaluación del desempeño**

  - Seguimiento, medición, análisis y evaluación
  - Auditoría interna
  - Revisión por la dirección

- **Mejora**

  - No conformidades y acciones correctivas
  - Mejora continua

LEY 1581 DE 2012

"Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".[23]

LEY 1273 DE 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."[24]

Cuenta con dos capítulos: Capitulo 1: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y Capítulo 2: De los atentados informáticos y otras infracciones.

[23] Función pública. Ley 1581 de 2012. Colombia: Gov.co. 2012. p. 1.
[24] MinTIC. Ley 1273 de 2009. Colombia: Congreso de Colombia. 2009. p. 5.

5. DISEÑO METODOLÓGICO

Para dar cumplimiento a cada uno de los objetivos propuestos del proyecto se hace mediante el ciclo Deming incluido en la norma ISO 27001:2013, que consiste en Planificar-Hacer-Verificar-Actuar (PHVA).

El modelo PHVA se describe de la siguiente manera:

- **Planificar**: se establecen los objetivos y los procesos necesarios para conseguir resultados según las necesidades de los clientes y la política de seguridad de la organización.
- **Hacer**: se implantan los procesos.
- **Verificar**: se revisan y se evalúan tanto lo servicios como los procesos comprándolos con las políticas, los objetivos y los requisitos de información sobre los resultados.
- **Actuar**: comienzan a emprender acciones para mejorar el rendimiento del Sistema de Gestión Ambiental de forma continua.

Paso a paso del modelo PHVA[25]

Planificar

Se debe realizar una planificación de la implantación y la prestación de la gestión de servicios. El alcance puede venir definido dentro de parte del plan de gestión de servicios. La gestión de servicios tiene que estar planificada. Incluye lo siguiente:

- El alcance de la gestión de los servicios de la empresa.
- Los requisitos y los objetivos que tiene que cumplir la gestión de servicios.
- Los procesos que se deben realizar.
- La infraestructura de las funciones y las responsabilidades de gestión, incluyendo al responsable del proceso y la gestión de proveedores externos a la organización.
- La interfaz entre todos los procesos de gestión de servicios y el modo en el que se tiene que coordinar las actividades llevadas a cabo por la empresa.
- Enfocar lo que se tiene que hacer para poder identificar, evaluar y gestionar los problemas y los riesgos de llevar a cabo los objetivos que se han definido.
- El intercambio de información con proyectos que ya estén creados o en proceso.
- Los recursos, las instalaciones y el presupuesto necesario para conseguir todos los objetivos que han sido definidos.
- Es la herramienta más adecuada para dar soporte a todos los procesos del Sistema de Gestión de Seguridad de la Información.

Tiene que existir una gestión clara por parte de la dirección y las responsabilidades tienen que estar documentadas, revisadas, autorizadas, comunicadas e implementadas.

[25]ISOTOOLS. ISO 27001: Ciclo de Deming. Blog PHG-SSI. 2015. p.1.

En cualquier plan específico de un proceso que se elabore debe ser compatible con el plan de gestión de servicios de la empresa.

Un plan de gestión de servicios tiene que incluir:

- Implementación de gestión de servicios.
- Facilitar los procesos de gestión de servicios.
- Los cambios en los procesos de gestión de servicios.
- Las mejoras en los procesos de gestión de servicios.
- Nuevos servicios.

Hacer

Implantar los objetivos y planificar la gestión de servicios, incluyendo

- La asignación de fondos y presupuestos
- Asignación de funciones y responsabilidades
- Documentación y mantenimiento de políticas, procedimientos y definiciones para cada proceso
- Identificar y gestionar los riesgos para el servicio
- Gestionar equipos
- Servicio de atención al cliente y operaciones.
- Informe de progreso y coordinación de procesos de gestión de servicios

Verificar

Se tiene que supervisar y verificar todos los objetivos y el plan de gestión de servicios establecido por la organización, para comprobar que se cumplen.

La empresa tiene que realizar una planificación para poder implementar la supervisión y la verificación de los procesos de gestión de servicios y los servicios asociados.

La norma ISO 27001:2013 nos dice que los resultados de la verificación deben ofrecer información sobre el programa de mejora del servicio. Entre todos los elementos que se tienen que supervisar, evaluar y analizar se encuentran:

- Los logros respecto de los objetivos del servicio definido.
- La satisfacción de los clientes.
- La utilización de recursos.
- Las tendencias.
- Las no conformidades.
- Todos los resultados de los análisis que pueden generar una mejora.

Actuar

El objetivo que persigue esta fase es mejorar la eficacia de las prestaciones y la gestión de los servicios.

Se debe realizar una política, que sea pública, para mejorar el servicio. Cualquier falta de conformidad con la norma ISO 27001:2013 tiene que ser remediada. Todas las funciones y las responsabilidades que sean necesarias para realizar las actividades de mejora del servicio se tienen que definir de forma clara.

Todas las mejoras de los servicios que propone la organización deben pasar por ser revisadas, registradas, priorizadas y autorizadas. Se puede utilizar un plan de mejora del servicio para poder controlar la actividad.

La empresa tiene que disponer de un proceso que identifique, evalúe y gestione todas las actividades de mejora.

Se tienen que incluir las mejoras del proceso individual para que la persona responsable del proceso pueda implantar los recursos necesarios y las mejoras de toda la empresa.

La empresa puede realizar una serie de actividades con las que recopilar datos para llevar a cabo evaluaciones comparativas de la capacidad de la empresa; identificar, planificar e implementar las mejoras necesarias; consultar a las partes interesadas; generar objetivos para conseguir mejorar la calidad de la seguridad de la información y disminuir los costes. Se tienen que considerar las aportaciones que se realizan referentemente a las mejoras que se realizan en el Sistema de Gestión de Seguridad de la Información ISO 27001:2013. Se debe revisar la política de seguridad y los procedimientos siempre que sea necesario.

Las mejoras que se realizan en el servicio de más importancia se tienen que gestionar como un proyecto.

6. DESARROLLO DE LOS OBJETIVOS

6.1. EVALUACIÓN ACTIVOS DE INFORMACIÓN

Para minimizar los riesgos que presenta la empresa Gotalk SAS, es necesario como primera instancia identificar los activos con los que actualmente cuenta la empresa y ser cobijados por el sistema de gestión de la seguridad de la información.

Se entiende como activo de información todo elemento que guarda o trata información para la empresa Gotalk SAS.

Para la identificación de los activos de información se hace mediante la metodología Magerit la cual determina los siguientes pasos para el análisis de riesgos:

1. Determinación y valoración de los activos relevantes, para el caso de la empresa Gotalk SAS, asignando el tipo y valor.
2. Determinación y valoración de amenazas, catalogando los niveles de peligros y afectación para los activos.
3. Determinación de salvaguardas dispuestos y eficaces para el riesgo.
4. Evaluar el impacto del daño producido por la materialización de la amenaza sobre el activo.
5. Evaluar el riesgo del impacto con la ocurrencia de la amenaza.[26]

Dando continuidad a la implementación de la metodología se realizó reuniones vía zoom con el Representante Legal para el levantamiento del inventario de activos ayudando a la identificación de estos y esto conlleva a la clasificación del tipo de activo de acuerdo con la metodología, lo identificado fue un total de 58 activos de información, de los cuales 5 de tipo activo, 1 de tipo dato, 11 de tipo servicios, 22 de tipo hardware, 3 de tipo comunicaciones, 3 de tipo auxiliares, 3 de tipo instalaciones y 8 de tipo personal.

Siguiendo la metodología se aplica lo guiado en el Libro I y II de MAGERIT para la evaluación de los riesgos, identificando las posibles amenazas que puede presentar los activos de información de la empresa teniendo en cuenta las dimensiones de valoración (D, I, D) y los criterios de valoración.

[26]Magerit. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información-Libro I-Método. 2012.p.22

Tabla 1

Categoría activos de información Magerit

Activos Esenciales	
Nombre Categoría	**ID**
Informacion	Info
Servicio	Service
Activos Relevantes	
Nombre Categoría	**ID**
Datos/informacion	[D]
Claves criptográficas	[K]
Servicios	[S]
Software	[SW]
Hardware	[HW]
Redes de comunicación	[COM]
Soporte de informacion	[MEDIA]

Fuente: elaboración propia

Nota. Esta tabla muestra las categorías de los activos de información y su respectivo ID de acuerdo con lo relacionado en Magerit, con el fin de facilitar la creación y planeación del inventario de activos de informacion.

En las siguientes imágenes se relaciona en detalle el inventario de activos de información. Sin embargo, en el Anexo A Matriz Evaluación del Riesgo se muestra con más información y características, en las hojas “AVC”, “VC” y “APT”.

Figura 5 Activos de información del tipo Activo

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
1	Hojas de vida Docentes y Administrativos	Andrea Peña	ACTIVO
2	Facturas	Nicolas Laverde	ACTIVO
3	Base de datos Estudiantes	Andrea Peña	ACTIVO
4	Base de datos Docentes	Andrea Peña	ACTIVO
5	Base de datos Administrativos	Andrea Peña	ACTIVO

Fuente: elaboración propia

En la figura N.5 se muestra 5 activos de información del tipo “Activo”.

Figura 6 Activos de información del tipo Datos

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
6	Copias de seguridad	Santiago Hernandez	DATOS

Fuente: elaboración propia

Para la figura No. 6 se tiene” se tiene 1 activo de información del tipo “Datos”.

Figura 7 Activos de información del tipo Servicios

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
7	Servidor de dominio	Daniel Herrera	SERVICIOS
8	Servidor en nube HEROKU	Tomas Hernandez	SERVICIOS
9	Servidor en nube Atlas Mongo DB	Tomas Hernandez	SERVICIOS
10	Gsuite Google	Daniel Herrera	SERVICIOS
11	Facebook Business	Santiago Hernandez	SERVICIOS
12	Tik Tok	Sara Lugo	SERVICIOS
13	Instagram	Sara Lugo	SERVICIOS
14	Twitter	Sara Lugo	SERVICIOS
15	YouTube	Sara Lugo	SERVICIOS
16	Facebook	Sara Lugo	SERVICIOS
17	Pagina Web	Daniel Herrera	SERVICIOS

Fuente: elaboración propia

Para la figura No. 7 está clasificado como tipo “Servicios” 11 activos de información.

Figura 8 Activos de información del tipo Hardware

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Tipo de Acti
18	Equipo computo Talento Humano	Andrea Peña	HARDWARE
19	Equipo computo Tecnologia	Santiago Hernandez	HARDWARE
20	Equipo computo Tecnologia	Daniel Herrera	HARDWARE
21	Equipo computo Tecnologia	Tomas Hernandez	HARDWARE
22	Equipo computo Tecnologia	Santiago Hernandez	HARDWARE
23	Equipo computo Gerencia	Nicolas Laverde	HARDWARE
24	Equipo computo Gerencia	Nicolas Laverde	HARDWARE
25	Equipo computo Ventas	Sara Lugo	HARDWARE
26	Equipo computo Ventas	Camila Taborda	HARDWARE
27	Equipo computo Ventas	Andres Peñaranda	HARDWARE
28	Equipo computo Ventas	Andres Peñaranda	HARDWARE
29	Equipo computo Sala de Juntas	Nicolas Laverde	HARDWARE
30	Equipo computo Sala de Juntas	Nicolas Laverde	HARDWARE
31	Router Cisco	Santiago Hernandez	HARDWARE
32	Switch Cisco	Santiago Hernandez	HARDWARE
33	Telefono movil Tecnologia	Santiago Hernandez	HARDWARE
34	Telefono movil Tecnologia	Daniel Herrera	HARDWARE
35	Telefono movil Tecnologia	Tomas Hernandez	HARDWARE
36	Telefono movil Tecnologia	Nicolas Laverde	HARDWARE
37	Telefono movil Gerencia	Nicolas Laverde	HARDWARE
38	Telefono movil Gerencia	Nicolas Laverde	HARDWARE
39	Telefono movil Gerencia	Nicolas Laverde	HARDWARE

Fuente: elaboración propia

De acuerdo con la figura No.8 se tiene 22 activos del tipo “Hardware”.

Figura 9 Activos de información del tipo Comunicaciones

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
40	Telefonia movil	Santiago Hernandez	COMUNICACIONE
41	Internet	Santiago Hernandez	COMUNICACIONE
42	Red local	Santiago Hernandez	COMUNICACIONE

Fuente: elaboración propia

En la figura No.9 hay 3 se tiene 3 activos de información del tipo “Redes de comunicaciones”.

Figura 10 Activos de información del tipo Equipos auxiliares

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
43	Rack de datos	Santiago Hernandez	AUXILIAR
44	Fuentes de alimentacion	Santiago Hernandez	AUXILIAR
45	Cableado	Santiago Hernandez	AUXILIAR

Fuente: elaboración propia

En la figura No.10 del tipo “Equipos auxiliares” se tiene 3 activos de información.

Figura 11 Activos de información del tipo Instalaciones

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
46	Oficina DTI	Santiago Hernandez	INSTALACIONES
47	Oficina DTH	Andrea Peña	INSTALACIONES
48	Oficina DV	Andres Peñaranda	INSTALACIONES
49	Sala de Juntas	Nicolas Laverde	INSTALACIONES
50	Oficina Gerencia	Nicolas Laverde	INSTALACIONES

Fuente: elaboración propia

Para la figura No.11 del tipo “Instalaciones” se tiene 5 activos de información.

Figura 12 Activos de información del tipo Personal

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
51	Nicolas Laverde	Nicolas Laverde	PERSONAL
52	Santiago Hernandez	Santiago Hernandez	PERSONAL
53	Andres Peñaranda	Andres Peñaranda	PERSONAL
54	Andrea Peña	Andrea Peña	PERSONAL
55	Sara Lugo	Sara Lugo	PERSONAL
56	Camila Taborda	Camila Taborda	PERSONAL
57	Daniel Herrera	Daniel Herrera	PERSONAL
58	Tomas Hernandez	Tomas Hernandez	PERSONAL

Fuente: elaboración propia

En la figura No.12 se tiene 8 usuarios del tipo “Personal”.

VALORACIÓN DE LOS ACTIVOS

Dando continuidad con la metodología Magerit de su libro II v.3, en el apartado No. 3. Dimensiones de valoración, informa que son características que hacen valioso un activo, estas dimensiones son utilizadas para valorar las consecuencias de la materialización de una amenaza.

Dimensiones:

- “[D] Disponibilidad: es una característica que afecta a todo tipo de activos. Tiene un gran valor ya que las consecuencias serían graves, si una amenaza afecta la disponibilidad del activo”.
- “[I] Integridad: los datos reciben una alta valoración desde la integridad cuando su alteración voluntaria o intencionada, causan graves daños a la organización”.
- “[C] Confidencialidad: los datos reciben una alta valoración desde la confidencialidad cuando su revelación causaría graves daños a la organización, y viceversa, los datos carecen de valor cuando su conocimiento por cualquiera no supone preocupación alguna”.[27]

Luego de la definición de las dimensiones para los activos se procede con la valoración, siendo esta la determinación del costo en el que se supone podría recuperarse luego de que por un incidente destroce el activo.

En el Libro I v.3 de Magerit establece dichas acciones para ser consideradas:[28]

- Coste de reposición: adquisición e instalación
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo
- Lucro cesante: pérdida de ingresos
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- Sanciones por incumplimiento de la ley u obligaciones contractuales
- Daño a otros activos, propios o ajenos
- Daño a personas
- Daños medioambientales

Por lo tanto, se establece el criterio de valoración de los activos para Gotalk SAS.

[27]Magerit. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información-Libro II-Catalogo de elementos. 2012.p.15
[28]Magerit. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información-Libro I-Catalogo de elementos. 2012.p.25

Tabla 2

Criterios de valoración de activos de la empresa Gotalk SAS

Valoracion Cualitativa	Escala de Valoracion	Escala Cuantitativa Millones
21 a 25	MA: Critico	200
16 a 20	A: Importante	100 a 200
10 a 15	M: Apreciable	50 a 100
5 a 9	B: Bajo	10 a 50
1 a 4	MB: Despreciable	0 a 10

Fuente: elaboración propia

Nota. En la tabla anterior muestra cómo se definió los criterios de valoración de los activos de informacion de la empresa Gotalk SAS con una valoración cualitativa de 1 a 25, escala de valoración de despreciable a critico y una escala cuantitativa en millones.

Luego de la definición de los criterios de valoración para los activos de información, se establece la valoración de los activos de información para la empresa Gotalk SAS, representada en el **Anexo A** **Matriz Evaluación del Riesgo**, en la hoja “VC”.

También se tuvo en cuenta para la valoración de los activos, las posibles amenazas a las que están expuestos los activos de información basados en el catálogo de amenazas del libro II Magerit v3.0 y de las dimensiones (C, I, D) que pueden ser afectadas por el tipo de amenaza.

Figura 13 Valoración Activos de la empresa Gotalk SAS

	Nombre	Riesgo	CONFIDENCIALIDAI	INTEGRIDAD	DISPONIBILIDAD	VALOR
1	Hojas de vida Docentes y Administrativos	IMPORTANTE	20	9	20	16
2	Facturas	IMPORTANTE	9	20	20	16
3	Base de datos Estudiantes	CRITICO	25	25	25	25
4	Base de datos Docentes	CRITICO	25	25	25	25
5	Base de datos Administrativos	CRITICO	25	25	25	25

Fuente: elaboración propia

En la figura No.13 se evidencia que dos de los activos esta con una valoración cualitativa “Importante” y cuantitativa “16” y los tres siguiente como “critico” en su valoración cualitativa y “25” cuantitativa.

Figura 14 Valoración Datos de la empresa Gotalk SAS

	Nombre	Riesgo	CONFIDENCIALIDAI	INTEGRIDAD	DISPONIBILIDAD	VALOR
6	Copias de seguridad	CRITICO	25	25	25	25

Fuente: elaboración propia

De acuerdo con la figura No.14 el activo copias de seguridad quedo con riesgo critico en una valoración cualitativa y 25 cuantitativa

Figura 15 Valoración servicios de la empresa Gotalk SAS

	Nombre	Riesgo	CONFIDENCIALIDAI	INTEGRIDAD	DISPONIBILIDAD	VALOR
7	Servidor de dominio	IMPORTANTE	20	20	20	20
8	Servidor en nube HEROKU	CRITICO	25	25	25	25
9	Servidor en nube Atlas Mongo DB	CRITICO	25	25	25	25
10	Gsuite Google	IMPORTANTE	20	20	20	20
11	Facebook Business	IMPORTANTE	20	20	20	20
12	Tik Tok	APRECIABLE	15	15	15	15
13	Instagram	APRECIABLE	15	15	15	15
14	Twitter	APRECIABLE	15	15	15	15
15	YouTube	APRECIABLE	15	15	15	15
16	Facebook	APRECIABLE	15	15	15	15
17	Pagina Web	IMPORTANTE	20	20	20	20

Fuente: elaboración propia

Para la figura No.15 hay 5 activos en riesgo apreciable con un valor de 15 correspondientes a las redes sociales, también se encuentra dos activos en riesgo importante con un valor de 20 correspondiente a la página web y servidor de dominio y por último el servidor en nube HEROKU y Atlas Mongo en riesgo crítico con una valoración de 25

Figura 16 Valoración Hardware de la empresa Gotalk SAS

	Nombre	Riesgo	CONFIDENCIALIDAI	INTEGRIDAD	DISPONIBILIDAD	VALOR
18	Equipo computo Talento Humano	IMPORTANTE	20	9	20	16
19	Equipo computo Tecnologia	IMPORTANTE	20	9	20	16
20	Equipo computo Tecnologia	IMPORTANTE	20	9	20	16
21	Equipo computo Tecnologia	IMPORTANTE	20	9	20	16
22	Equipo computo Tecnologia	IMPORTANTE	20	9	20	16
23	Equipo computo Gerencia	IMPORTANTE	20	9	20	16
24	Equipo computo Gerencia	IMPORTANTE	20	9	20	16
25	Equipo computo Ventas	IMPORTANTE	20	9	20	16
26	Equipo computo Ventas	IMPORTANTE	20	9	20	16
27	Equipo computo Ventas	IMPORTANTE	20	9	20	16
28	Equipo computo Ventas	IMPORTANTE	20	9	20	16
29	Equipo computo Sala de Juntas	IMPORTANTE	20	9	20	16
30	Equipo computo Sala de Juntas	IMPORTANTE	20	9	20	16
31	Router Cisco	IMPORTANTE	20	9	20	16
32	Switch Cisco	IMPORTANTE	20	9	20	16
33	Telefono movil Tecnologia	APRECIABLE	9	9	15	11
34	Telefono movil Tecnologia	APRECIABLE	9	9	15	11
35	Telefono movil Tecnologia	APRECIABLE	9	9	15	11
36	Telefono movil Tecnologia	APRECIABLE	9	9	15	11
37	Telefono movil Gerencia	APRECIABLE	9	9	15	11
38	Telefono movil Gerencia	APRECIABLE	9	9	15	11
39	Telefono movil Gerencia	APRECIABLE	9	9	15	11

Fuente: elaboración propia

En la figura No.16 se evidencia que en la mayoría de los activos están calificados como riesgo importante con una valoración cuantitativa de 16 y los demás en apreciable con una valoración de 11.

Figura 17 Valoración Comunicaciones de la empresa Gotalk SAS

	Nombre	Riesgo	CONFIDENCIALIDAI	INTEGRIDAD	DISPONIBILIDAD	VALOR
40	Telefonia movil	IMPORTANTE	20	20	9	16
41	Internet	IMPORTANTE	20	20	9	16
42	Red local	IMPORTANTE	20	20	9	16

Fuente propia

En la figura No.17 muestra como para la telefonía móvil, internet y red local están evaluados como riesgo importante con un valor de 16.

Figura 18 Valoración Equipos auxiliares de la empresa Gotalk SAS

	Nombre	Riesgo	CONFIDENCIALIDAI	INTEGRIDAD	DISPONIBILIDAD	VALOR
43	Rack de datos	APRECIABLE	15	15	15	15
44	Fuentes de alimentacion	APRECIABLE	15	15	15	15
45	Cableado	APRECIABLE	15	15	15	15

Fuente: elaboración propia

Para los equipos auxiliares como se muestra en la figura No.18 están valorados en riesgos apreciable con una valoración cuantitativa de 15.

Figura 19 Valoración Instalaciones de la empresa Gotalk SAS

	Nombre	Riesgo	CONFIDENCIALIDAI	INTEGRIDAD	DISPONIBILIDAD	VALOR
46	Oficina DTI	IMPORTANTE	20	20	20	20
47	Oficina DTH	IMPORTANTE	20	20	20	20
48	Oficina DV	IMPORTANTE	20	20	20	20
49	Sala de Juntas	IMPORTANTE	20	20	20	20
50	Oficina Gerencia	IMPORTANTE	20	20	20	20

Fuente: elaboración propia

En la figura No.19 todas las instalaciones están con una valoración de 20 y como riesgo importante.

Figura 20 Valoración Personal de la empresa Gotalk SAS

	Nombre	Riesgo	CONFIDENCIALIDAI	INTEGRIDAD	DISPONIBILIDAD	VALOR
51	Nicolas Laverde	IMPORTANTE	20	20	20	20
52	Santiago Hernandez	IMPORTANTE	20	20	20	20
53	Andres Peñaranda	IMPORTANTE	20	20	20	20
54	Andrea Peña	IMPORTANTE	20	20	20	20
55	Sara Lugo	IMPORTANTE	20	20	20	20
56	Camila Taborda	IMPORTANTE	20	20	20	20
57	Daniel Herrera	IMPORTANTE	20	20	20	20
58	Tomas Hernandez	IMPORTANTE	20	20	20	20

Fuente: elaboración propia

De acuerdo con la figura No.20 para los 8 usuarios clasificados como personal se tiene como valoración 20 y en un riesgo importante como valoración cualitativa.

Mediante la metodología MAGERIT se realizó la evaluación de riesgo de acuerdo con la identificación de los activos de información y las posibles amenazas que se pueden llegar a presentar en términos de seguridad en la empresa, con la finalidad de identificar el costo de estos activos en caso de que materialice el riesgo.

Por último, se puede consultar en el Anexo A de este documento donde se relaciona la evaluación de riesgo en detalle:

- Personal y dependencia de la empresa Gotalk SAS, en la hoja “PYD”
- Los activos de información y valoración cualitativa, en la hoja “AVC”
- **V**aloración cuantitativa de los activos de información, en la hoja “VC”
- Amenazas y vulnerabilidades, en la hoja “APT”

- Resumen ejecutivo, en la hoja “RE”.

6.2. SALVAGUARDAS PARA LOS ACTIVOS DE INFORMACIÓN

Es importante comunicar a la empresa GOTALK SAS el nivel de riesgo al que actualmente se enfrentan y como se puede mitigar mediante la aplicación de salvaguardas haciendo frente a cada una de las amenazas identificadas basado en el Anexo A de la norma ISO/IEC 27001:2013.

El Anexo A es un documento normativo compuesto de 114 controles de seguridad que están dirigidos a mejorar la seguridad de la información de la empresa.[29]

Es fundamental y obligatorio la aplicación de estos controles para la implementación del SGSI aclarando que dependiendo de cada caso existirán controles que no se pueden aplicar.

Estos controles abarcan todos los ámbitos no solamente de ciberseguridad, a continuación, se relacionan las 14 sesiones del Anexo A:[30]

- **A.5: Políticas de Seguridad de la Información:** hace referencia a los controles sobre cómo escribir y revisar políticas de seguridad.
- **A.6: Organización de la Seguridad de la información:** los controles se encargan de establecer responsables. Al mismo tiempo también se centra en dispositivos móviles y situaciones como la de teletrabajo.
- **A.7: Seguridad de los Recursos Humanos:** controles para las situaciones previas y posteriores referentes a la contratación y finalización de contrato de personal.
- **A.8: Gestión de Recursos:** establecidos para realizar inventario, clasificación de información y manejo de los medios de almacenamiento.
- **A.9: Control de Acceso:** control del acceso tanto a la información como a aplicaciones u otro medio que contenga información.
- **A.10: Criptografía:** controles para gestionar encriptación de información.
- **A.11: Seguridad física y ambiental:** controles para garantizar factores externos, seguridad de equipo y medios que puedan comprometer la seguridad.
- **A.12: Seguridad Operacional:** controles relacionados con gestión de la protección de malware o vulnerabilidades.
- **A.13: Seguridad de las comunicaciones:** Control sobre la seguridad de las redes, transmisión de información, mensajería.
- **A.14: Adquisición, desarrollo y mantenimiento de Sistemas:** controles que establecen los requisitos de seguridad en desarrollo y soporte.
- **A.15: Relaciones con los proveedores:** incluye lo necesario a la hora de realizar contratos y seguimiento a proveedores.
- **A.16: Gestión de Incidentes en Seguridad de la Información:** sirven para reportar eventos las debilidades, así como procedimientos de respuesta.
- **A.17: Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio:** referidos a la planificación de continuidad de negocio.

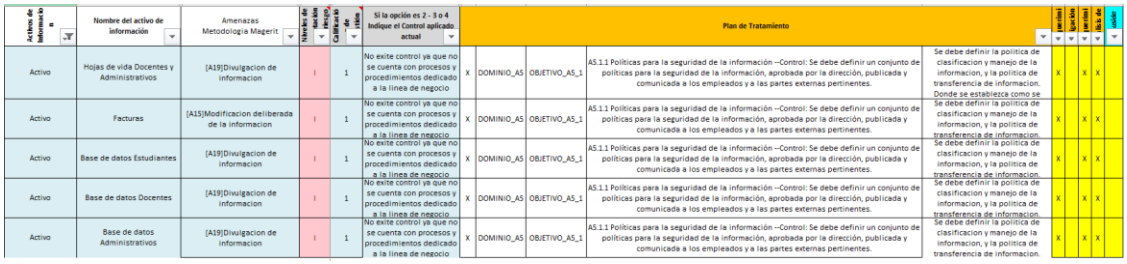
29 ISOTools Excellence. Anexo A en ISO 27001, objetivos de control y controles de referencia. Blog. 2020.p1.
30 Ibid.p1.

- **A.18: Cumplimiento:** control relacionado a la hora de identificar regulaciones relacionadas con seguridad de la información y hacer que se cumplan.

Para la propuesta de las salvaguardas se tuvo en cuenta la evaluación de riesgo que se hizo a cada una de las amenazas identificadas con un total de 120 amenazas basadas en el Libro II Magerit v3, y la identificación de controles existentes, que para el caso de la empresa GOTALK SAS, actualmente no cuentan con este tipo de controles aplicados.
En el Anexo B Tratamiento del riesgo, se puede visualizar en detalle el nivel de aceptación del riesgo, el plan de acción que se va a hacer con cada amenaza y la relación de los controles a aplicar a partir de la norma ISO 27001:2013.

A continuación, se presenta las siguientes imágenes con algunos de los detalles del anexo.

Figura 21 Salvaguardas Tipo Activo de la empresa Gotalk SAS

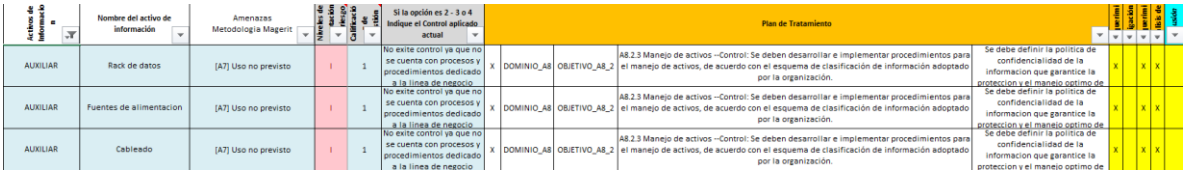


Activos de información	Nombre del activo de información	Amenazas Metodología Magerit	Niveles de aceptación del riesgo	Calificación de riesgo	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Plan de Tratamiento					
Activo	Hojas de vida Docentes y Administrativos	[A19]Divulgacion de informacion	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A5	OBJETIVO_A5_1	A5.1.1 Políticas para la seguridad de la información --Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Se debe definir la política de clasificacion y manejo de la informacion, y la política de transferencia de informacion.	X X X
Activo	Facturas	[A15]Modificacion deliberada de la informacion	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A5	OBJETIVO_A5_1	A5.1.1 Políticas para la seguridad de la información --Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Donde se establezca como se Se debe definir la política de clasificacion y manejo de la informacion, y la política de transferencia de informacion.	X X X
Activo	Base de datos Estudiantes	[A19]Divulgacion de informacion	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A5	OBJETIVO_A5_1	A5.1.1 Políticas para la seguridad de la información --Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Se debe definir la política de clasificacion y manejo de la informacion, y la política de transferencia de informacion.	X X X
Activo	Base de datos Docentes	[A19]Divulgacion de informacion	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A5	OBJETIVO_A5_1	A5.1.1 Políticas para la seguridad de la información --Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Se debe definir la política de clasificacion y manejo de la informacion, y la política de transferencia de informacion.	X X X
Activo	Base de datos Administrativos	[A19]Divulgacion de informacion	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A5	OBJETIVO_A5_1	A5.1.1 Políticas para la seguridad de la información --Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Se debe definir la política de clasificacion y manejo de la informacion, y la política de transferencia de informacion.	X X X

Fuente: elaboración propia

En la figura No.21 se relaciona el plan de tratamiento bajo el dominio A_5 Política para la seguridad de la información y el control A.5.1.1 Política para la seguridad de la información como salvaguardas de los cinco activos de información que están clasificados como Activo (Hojas de vida Docentes y Administrativos, Facturas, Base de datos Estudiantes, Base de datos Docentes, Base de datos Administrativos)

Figura 22 Salvaguardas Tipo Auxiliares de la empresa Gotalk SAS

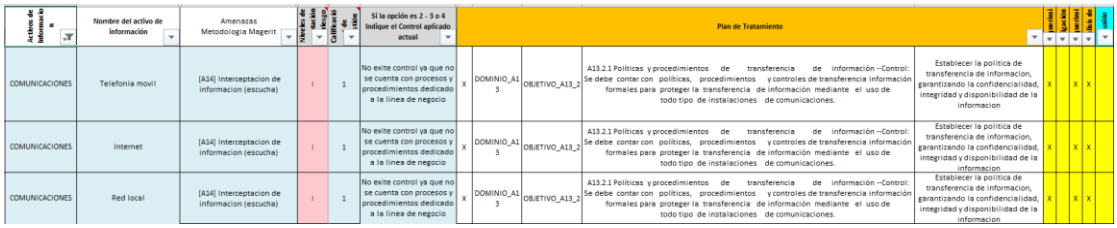


Activos de información	Nombre del activo de información	Amenazas Metodología Magerit	Niveles de aceptación del riesgo	Calificación de riesgo	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Plan de Tratamiento				
AUXILIAR	Rack de datos	[A7] Uso no previsto	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.3 Manejo de activos --Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Se debe definir la política de confidencialidad de la informacion que garantice la proteccion y el manejo optimo de	X X X
AUXILIAR	Fuentes de alimentacion	[A7] Uso no previsto	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.3 Manejo de activos --Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Se debe definir la política de confidencialidad de la informacion que garantice la proteccion y el manejo optimo de	X X X
AUXILIAR	Cableado	[A7] Uso no previsto	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.3 Manejo de activos --Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Se debe definir la política de confidencialidad de la informacion que garantice la proteccion y el manejo optimo de	X X X

Fuente: elaboración propia

Para la figura No.22 se evidencia que para los activos tipo auxiliares se trata como salvaguarda el dominio A_8 Gestión de los activos y como control el A.8.2.3 Manejo de activos para la definición de procesos y políticas que garanticen la protección y manejo de los activos de información.

Figura 23 Salvaguardas Tipo Comunicaciones de la empresa Gotalk SAS



Archivo de Información	Nombre del activo de información	Amenazas Metodología Magerit	Nivel de Valoración	Riesgo	Calificación del riesgo	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Plan de Tratamiento					Confidencialidad	Integridad	Disponibilidad de la información	Estado
COMUNICACIONES	Telefonia movil	[A14] Interceptacion de informacion (escucha)	I		1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	x	DOMINIO_A13	OBJETIVO_A13_2	A13.2.1 Políticas y procedimientos de transferencia de información --Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Establecer la política de transferencia de informacion, garantizando la confidencialidad, integridad y disponibilidad de la informacion	X	X	X	
COMUNICACIONES	Internet	[A14] Interceptacion de informacion (escucha)	I		1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	x	DOMINIO_A13	OBJETIVO_A13_2	A13.2.1 Políticas y procedimientos de transferencia de información --Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Establecer la política de transferencia de informacion, garantizando la confidencialidad, integridad y disponibilidad de la informacion	X	X	X	
COMUNICACIONES	Red local	[A14] Interceptacion de informacion (escucha)	I		1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	x	DOMINIO_A13	OBJETIVO_A13_2	A13.2.1 Políticas y procedimientos de transferencia de información --Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Establecer la política de transferencia de informacion, garantizando la confidencialidad, integridad y disponibilidad de la informacion	X	X	X	

Fuente: elaboración propia

En la anterior figura No. 23 se tiene como plan de tratamiento el dominio A_13 Seguridad de las comunicaciones y el control A.13.2.1 Políticas y procedimientos de transferencia de información, con la finalidad de establecer la política de transferencia de información a los tres activos clasificados como Comunicaciones (telefonía móvil, Internet, red local).

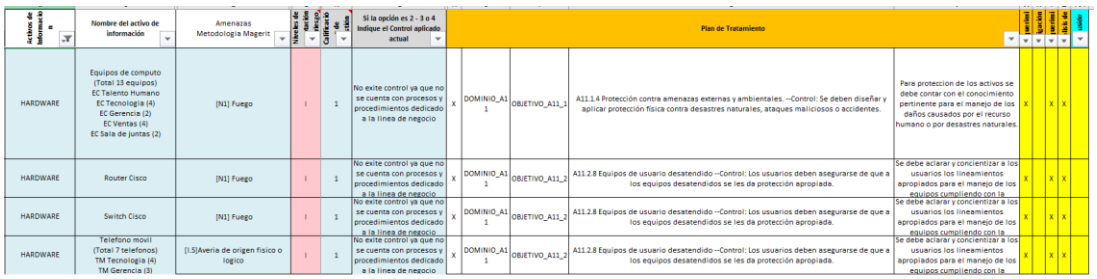
Figura 24 Salvaguardas Tipo Datos de la empresa Gotalk SAS

Archivo de Información	Nombre del activo de información	Amenazas Metodología Magerit	Nivel de Valoración	Riesgo	Calificación del riesgo	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Plan de Tratamiento					Confidencialidad	Integridad	Disponibilidad de la información	Estado
DATOS	Copias de seguridad	[E2]Errores del administrador	I		1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	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.	Se debe definir la política de copia de respaldo, para contar con un estandar relacionando, la periodicidad, los responzables,	X	X	X	

Fuente: elaboración propia

De acuerdo con la figura No.24 se visualiza que para el activo copias de seguridad se define el plan de tratamiento con el dominio A_12 Seguridad de las operaciones y el control A.12.3.1 Respaldo de información, para definir la copia de seguridad relacionando la periodicidad, responsable y ubicación de copias.

Figura 25 Salvaguardas Tipo Hardware de la empresa Gotalk SAS



Archivo de Información	Nombre del activo de información	Amenazas Metodología Magerit	Nivel de Valoración	Riesgo	Calificación del riesgo	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Plan de Tratamiento					Confidencialidad	Integridad	Disponibilidad de la información	Estado
HARDWARE	Equipos de computo (Total 13 equipos) EC Talento Humano EC Tecnologia (4) EC Gerencia (2) EC Ventas (4) EC Sala de juntas (2)	[N1] Fuego	I		1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	x	DOMINIO_A11	OBJETIVO_A11_1	A11.1.4 Protección contra amenazas externas y ambientales. --Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Para proteccion de los activos se debe contar con el conocimiento pertinente para el manejo de los daños causados por el recurso humano o por desastres naturales.	X	X	X	
HARDWARE	Router Cisco	[N1] Fuego	I		1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	x	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendido --Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la	X	X	X	
HARDWARE	Switch Cisco	[N1] Fuego	I		1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	x	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendido --Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la	X	X	X	
HARDWARE	Telefono movil (Total 7 telefonos) TM Tecnologia (4) TM Gerencia (3)	[I.5]Averia de origen fisico o logico	I		1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	x	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendido --Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la	X	X	X	

Fuente: elaboración propia

En la figura No.25 se relaciona los activos tipo hardware con el dominio A_11 Seguridad física y del entorno con los controles A.11.1.4 Protección contra amenazas externas y ambientales y A.11.2.8 Equipos de usuarios desatendido como salvaguardas para la aclaración y concientización de los usuarios para el adecuado manejo de los equipos cumpliendo con la confidencialidad, integridad y disponibilidad de la información.

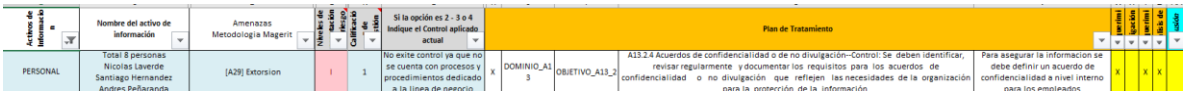
Figura 26 Salvaguardas Tipo Instalaciones de la empresa Gotalk SAS

Archivo de Información	Nombre del activo de información	Amenazas Metodología Magerit	Nivel de Valoración	Riesgo	Calificación del riesgo	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Plan de Tratamiento					Confidencialidad	Integridad	Disponibilidad de la información	Estado
INSTALACIONES	Oficinas (Total 5 oficinas) DTI DTH	[N1]Fuego	I		1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	x	DOMINIO_A11	OBJETIVO_A11_2	A11.2.8 Equipos de usuario desatendido --Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Se debe aclarar y concientizar a los usuarios los lineamientos apropiados para el manejo de los equipos cumpliendo con la	X	X	X	

Fuente: elaboración propia

En la figura No.26 las instalaciones de la empresa se tienen como plan de tratamiento el dominio A_11 Seguridad física y el entorno con el control A.11.2.8 Equipos de usuarios desatendido.

Figura 27 Salvaguardas Tipo Personal de la empresa Gotalk SAS

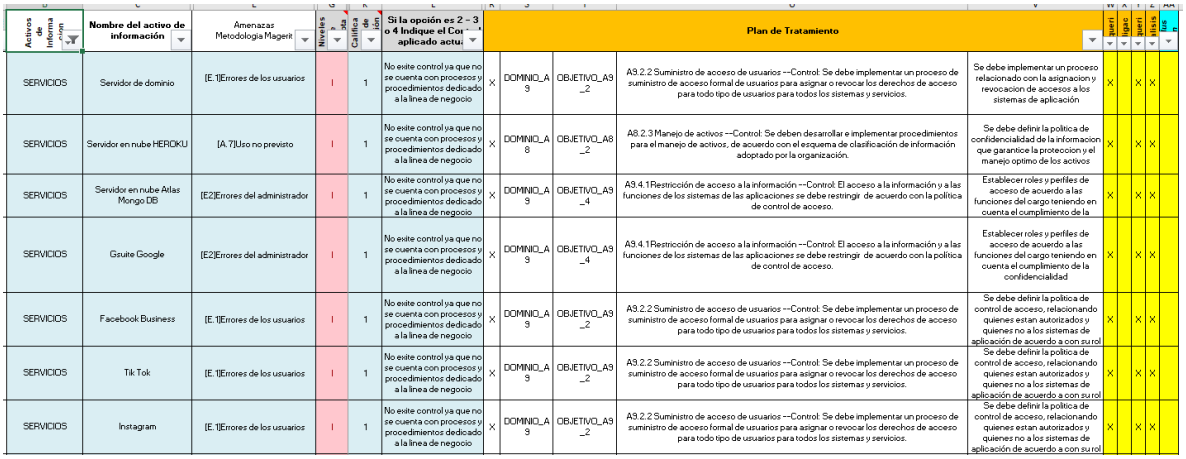


Activos de Información con	Nombre del activo de información	Amenazas Metodología Magerit	Nivel de valoración riesgo	Calificación de riesgo	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual		Plan de Tratamiento				
PERSONAL	Total 8 personas Nicolas Laverde Santiago Hernandez Andres Peñaranda	[A29] Extorsion	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A13	OBJETIVO_A13_2	A13.2.4 Acuerdos de confidencialidad o de no divulgación--Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información	Para asegurar la información se debe definir un acuerdo de confidencialidad a nivel interno para los empleados	X X X X

Fuente: elaboración propia

Para la figura No.27 se tiene ocho usuarios clasificados como tipo de activo personal con un plan de tratamiento basado en el dominio A_13 Seguridad de las comunicaciones y el control A.13.2.4 Acuerdos de confidencialidad o de no divulgación.

Figura 28 Salvaguardas Tipo Servicios de la empresa Gotalk SAS



Activos de Información con	Nombre del activo de información	Amenazas Metodología Magerit	Nivel de valoración riesgo	Calificación de riesgo	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual		Plan de Tratamiento				
SERVICIOS	Servidor de dominio	[E.1]Errores de los usuarios	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A9	OBJETIVO_A9_2	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.	Se debe implementar un proceso relacionado con la asignacion y revocacion de accesos a los sistemas de aplicación	X X X
SERVICIOS	Servidor en nube HEROKU	[A.7]Uso no previsto	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.3 Manejo de activos --Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Se debe definir la politica de confidencialidad de la informacion que garantice la proteccion y el manejo optimo de los activos	X X X
SERVICIOS	Servidor en nube Atlas Mongo DB	[E2]Errores del administrador	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la politica de control de acceso.	Establecer roles y perfiles de acceso de acuerdo a las funciones del cargo teniendo en cuenta el cumplimiento de la	X X X
SERVICIOS	Gsuite Google	[E2]Errores del administrador	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la politica de control de acceso.	Establecer roles y perfiles de acceso de acuerdo a las funciones del cargo teniendo en cuenta el cumplimiento de la confidencialidad	X X X
SERVICIOS	Facebook Business	[E.1]Errores de los usuarios	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A9	OBJETIVO_A9_2	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.	Se debe definir la politica de control de acceso, relacionando quienes estan autorizados y quienes no a los sistemas de aplicación de acuerdo a con su rol	X X X
SERVICIOS	Tik Tok	[E.1]Errores de los usuarios	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A9	OBJETIVO_A9_2	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.	Se debe definir la politica de control de acceso, relacionando quienes estan autorizados y quienes no a los sistemas de aplicación de acuerdo a con su rol	X X X
SERVICIOS	Instagram	[E.1]Errores de los usuarios	I	1	No exite control ya que no se cuenta con procesos y procedimientos dedicado a la linea de negocio	X	DOMINIO_A9	OBJETIVO_A9_2	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.	Se debe definir la politica de control de acceso, relacionando quienes estan autorizados y quienes no a los sistemas de aplicación de acuerdo a con su rol	X X X

Fuente: elaboración propia

De acuerdo con la figura No.28 se tiene diferentes dominios y controles para el plan de tratamiento como A_9 Control de acceso con el control A.9.2.2 Suministro de acceso de usuarios y A.9.4.1 Restricciones de acceso a la información, dominio A_8 Gestión de activos y el control A.8.2.3 Manejo de activos y el dominio A_12 Seguridad de las operaciones con el control A.12.1.3 Gestión de capacidad de los activos de información tipo servicios, con la finalidad de definir la política de control de accesos, procedimientos para la asignación y revocación de accesos, y seguimiento y revisión de la capacidad operacional.

Tabla 3

Resumen de salvaguardas a aplicar a las amenazas identificadas

Salvaguardas por Dominio	Total Vulnerabilidades a aplicar
Dominio_A5 Políticas de seguridad de la información	13
Dominio_A7 Seguridad de los recursos humanos	1
Dominio_A8 Gestión de activos	21
Dominio_A9 Control de acceso	19
Dominio_A11 Seguridad física y del entorno	54
Dominio_A12 Seguridad de las operaciones	8
Dominio_A13 Seguridad de las comunicaciones	4
Total: 120 salvaguardas	

Fuente: elaboración propia

Nota. En esta table se puede identificar el resumen de las salvaguardas identificadas para aplicar en las amenazas identificadas en la empresa Gotalk SAS.

Es así como se logra establecer las salvaguardas mediante los controles del Anexo A de la norma ISO 27001:2013, con el fin de hacer frente a las amenazas identificadas a los activos de información de la empresa.

6.3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Posterior a la identificación de los activos de información con su respectiva evaluación de riesgos y definición de las salvaguardas con base al Anexo A de la norma ISO 27001:2013, se establecen las políticas de seguridad de la información teniendo en cuenta las buenas prácticas y estándares dando cumplimiento a la norma ISO 27001:2013 para la gestión segura de la información.

Se hace necesario la definición de estas políticas de seguridad para la empresa Gotalk SAS debido a que no cuenta con procesos y guías para el manejo adecuado de los activos de información y las buenas prácticas en términos de seguridad que debe contemplar y cumplir para garantizar la mitigación de riesgos y la protección de la información.

Las políticas de seguridad se generan a partir de los controles relacionados en el Anexo A de la norma ISO 27001:2013 como referente para llevar a cabo las buenas prácticas de la norma y siendo una guía verdaderamente practica para el departamento de TI ya que permite ser el punto de referencia, de lo que se debe cumplir de acuerdo con los activos de información que tiene la empresa y tener en detalle de lo que haría falta por implementar o reforzar, siendo estas publicadas y divulgadas para cada uno de los empleados, proveedores y accionistas de la empresa.

Es importante resaltar que las políticas de seguridad son con lineamientos generales siendo como guía para la implementación de procedimientos y/o lineamientos específicos de acuerdo con los procesos.

Las políticas están definidas en dos documentos:

- **SegInf P1.0** Política De Seguridad De La Información-Todos Los Empleados: esta política relaciona una descripción general del cumplimiento de las políticas y lineamientos de seguridad para toda la empresa.
- **SegInf P2.0** Política De Seguridad De La Información Empleados Con Funciones Y Responsabilidades Técnicas. En esta política se establece en detalle los lineamientos que se deben seguir de acuerdo con los controles del Anexo A de la norma ISO 27001:2013, con el cumplimiento de: clasificación y manejo de activos, gestión de activos y gestión de la configuración, controles de acceso, uso de cifrado, seguridad de las operaciones, seguridad de la red, seguridad de la eliminación y reutilización de activos, incidentes de seguridad, capacitación de concientización de seguridad y cumplimiento.

- Para mayor detalle y lectura completa de las políticas se encuentran en el Anexo C: SegInf P1.0 Política De Seguridad De La Información -Todos Los Empleados y el Anexo D: SegInf P2.0 Política De Seguridad De La Información Empleados Con Funciones Y Responsabilidades Técnicas.

Estas políticas establecen la siguiente declaración y propósito: “

El propósito de esta política es establecer los principios y requisitos para la protección de los sistemas de tecnología de la información de GOTALK SAS y la información que contienen. Los principios y requisitos de esta política están definidos por el departamento de Seguridad para proteger a GOTALK SAS, empleados y estudiantes del daño causado por el mal uso de los activos de GOTALK SAS y nuestros datos. El mal uso de estos activos incluye tanto acciones deliberadas como involuntarias.”

A su vez como definición y alcance establece lo siguiente: “Esta política incluye todos los sistemas de tecnología de la información de GOTALK SAS y la información que contienen.”

6.3.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN- TODOS LOS EMPLEADOS

Declaraciones

1. **Uso Aceptable**

    - Activos: los activos proporcionados por GOTALK SAS deben usarse únicamente con fines laborales y comerciales.
    - Redes sociales: las cuentas de redes sociales de GOTALK SAS están destinadas a ser utilizadas únicamente con fines laborales y comerciales.
    - Software: debe utilizarse únicamente con fines autorizados y previstos, no debe copiarse, distribuirse, instalarse ni eliminarse sin la debida autorización. Solo el

software aprobado y autorizado por GOTALK SAS se instalará en los activos corporativos.

- Datos: se utilizarán con fines autorizados y previstos, no debe copiarse, distribuirse, editarse, agregarse ni eliminarse sin la autorización correspondiente.
- Internet y correo electrónico: los controles de seguridad establecidos por GOTALK SAS no se cambiarán ni eludirán:

    - ✓ Para reducir el riesgo de un ataque de phishing, cada empleado debe interactuar de manera segura con todas las formas de tecnología y tener cuidado al hacer clic en enlaces o descargar archivos adjuntos. Nunca ingrese la contraseña de sus credenciales de dominio en sitios web de terceros.
    - ✓ Los correos electrónicos de GOTALK SAS no deben reenviarse a cuentas personales.
    - ✓ Los empleados no pueden establecer reglas de enrutamiento para reenviar automáticamente cuentas de correo electrónico externas a una cuenta de Gmail de GOTALK SAS, incluidas las cuentas de correo electrónico de los estudiantes, ni configurar Gmail para ingerir cuentas de correo electrónico externas.

- Traiga su propio dispositivo: los empleados que utilicen dispositivos personales (portátiles y/o móviles) y software relacionado para acceder a la red y a los datos de GOTALK SAS deben con los estándares de contraseña y manejar los datos confidenciales de manera adecuada.
- Copia de seguridad de datos: los empleados utilizarán Drive (Google) para fines de copia de seguridad de datos. No se permite un dispositivo de almacenamiento o una cuenta personales en la nube para realizar copias de seguridad de datos corporativos o de estudiantes. Los empleados con un requisito para usar medios extraíbles pueden solicitar una excepción y espera de aprobación.
- Reporte de eventos/incidentes de Seguridad: cada empleado tiene la responsabilidad de reportar cualquier incidente confirmado o la sospecha de un problema de seguridad al departamento de seguridad e infraestructura tan pronto como se dé cuenta del problema.
- Trabajo remoto: Los empleados tomarán medidas de manera proactiva para asegurar y proteger sus redes domésticas mientras realizan sus funciones laborales de GOTALK SAS.
- Los empleados se conectarán de forma segura mediante VPN mientras realizan sus funciones laborales de GOTALK SAS desde cualquier ubicación pública.
- Los dispositivos de GOTALK SAS no deberán acompañar a los empleados que viajen por motivos personales.
- Cuando los activos de trabajo de GOTALK SAS acompaña a un empleado que viaja fuera de la ciudad designado y con fines comerciales, los empleados primero deben solicitar la aprobación por escrito de su jefe inmediato.

2. **Gestión De Contraseñas De Usuario**

- Las contraseñas deben ser complejas. Las contraseñas deben tener un mínimo de ocho (8) caracteres de longitud y debe incluir caracteres especiales, mayúsculas, minúsculas y numero.
- Las contraseñas deben cambiarse cada 90 días.
- Las contraseñas no deben contener información personal o de trabajo como el nombre de usuario ni ninguna parte del nombre completo del usuario.
- Las contraseñas no se pueden reutilizar con más frecuencia que cada 5 actualizaciones de contraseña.
- Las contraseñas no deben anotarse ni almacenarse electrónicamente en un archivo.
- Las contraseñas solo pueden almacenarse en aplicaciones de administrador de contraseñas autorizadas por GOTALK SAS
- Las contraseñas son únicas e intransferibles, son confidenciales y no deben compartirse con otros.

3. Capacitación De Concientización Sobre Seguridad

La capacitación sobre seguridad tiene como propósito ayudar a los empleados a reconocer y evaluar las diversas amenazas que enfrentamos a diario. Para el éxito de las operaciones comerciales de la empresa requiere que cada usuario sea competente en la gestión del riesgo de la información que maneja.

- Todos los empleados deberán completar la capacitación de concientización sobre seguridad en las fechas acordadas.
- La capacitación en concientización sobre seguridad comenzará tan pronto como sea posible después de que los empleados se unan a la empresa como parte del proceso de inducción. Las actividades de concientización y la capacitación continuarán de manera continua/escalonada a partir de entonces para mantener un nivel razonablemente constante de concientización.
- GOTALK SAS tiene como deber proporcionar a los empleados información sobre la ubicación de los materiales de capacitación de concientización sobre seguridad, las políticas de seguridad y otros documentos relacionados en temas de seguridad.

6.3.2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EMPLEADOS CON FUNCIONES Y RESPONSABILIDADES TÉCNICAS.

Declaraciones

1. Clasificación y Manejo de Datos y Activos

Refleja el nivel de impacto para GOTALK SAS si se compromete la confidencialidad, la integridad o la disponibilidad de los datos. El propietario de los datos es responsable de determinar la etiqueta de clasificación para cada dato.

Manejo de datos: para proteger la información restringida y confidencial, implemente los siguientes controles:

- Definir una Política de control de acceso y restringir el acceso a las personas que lo necesiten.
- Cifrar datos en tránsito a través de cualquier red.
- Enviar o recibir información Restringida y Confidencial en Mensajes Instantáneos (IM) o Chat, los mensajes están prohibidos ya que, por naturaleza, estos métodos de comunicación electrónica no son seguros y están sujetos a interceptación y lectura o copia en tránsito hacia el destino.
- La información restringida y la información confidencial no se pueden almacenar en almacenamiento expandible para ningún propósito. El almacenamiento ampliable es una forma de almacenamiento informático diseñado para insertarse y extraerse de un sistema. Cualquier requisito comercial para usar almacenamiento expandible, como dispositivos relacionados con medios extraíbles, debe aprobarse a través de una solicitud de excepción y, si se aprueba, se utilizará encriptación.
- La copia de seguridad de la Información Restringida y Confidencial debe estar encriptada.
- Eliminar de forma segura los sistemas y medios que contengan información restringida o confidencial.

2. Gestión De Activos Y Gestión De La Configuración

Gestión de activos

Se debe mantener una base de datos de administración de activos para identificar todo el inventario de dispositivos administrados por GOTALK SAS.

Luego de la adquisición de todo hardware de usuario final e infraestructura de GOTALK SAS se debe registrar en la base de datos de gestión de activos, con una información mínima de registro: número de serie, número de orden de compra, número de factura, fecha de adquisición, propiedad, estado, ubicación, número de modelo, ID de etiqueta de activo.

Gestión de la configuración

Se debe mantener una base de datos de gestión de configuración para identificar todos los activos de hardware conectados a la red corporativa de GOTALK SAS y todos los activos de software instalados que utilizan los empleados de la empresa.

Los campos detectables y no detectables se registrarán para los activos identificados dentro de la base de datos de gestión de configuración. Los siguientes campos no detectables se agregarán manualmente:

- El propietario y los usuarios del activo, incluidos el propietario de la información, el propietario de la aplicación, el propietario de la plataforma, el propietario de los datos, el custodio de los datos, el administrador de los datos y los usuarios de los datos.
- Un contacto de emergencia, al que se debe contactar para fines de respuesta rápida.
- La ubicación de la infraestructura de alojamiento y almacenamiento de datos.

3. Control de acceso

Procedimiento de control de acceso

Documentar un procedimiento de control de acceso para cada aplicación o sistema que describa cómo administrar los riesgos de la administración de cuentas de usuario, la aplicación y el control del acceso, la separación de funciones y el acceso remoto. Tener en cuenta: los requisitos de seguridad del sistema o aplicación comercial; el tipo de datos contenidos en el sistema o en la aplicación; cualquier obligación legal o contractual con respecto a la limitación del acceso a datos o servicios; gestión de derechos de acceso y segregación de roles de control de acceso; requisitos para la autorización formal de las solicitudes de acceso y revisión periódica de los derechos de acceso; eliminación de los derechos de acceso; roles con acceso privilegiado; mantener un registro de auditoría de todos los eventos significativos relacionados con los derechos de acceso y la gestión de identidades y la fuerza de la autenticación, ya sea autenticación de un solo factor (SFA) o multifactor Autenticación (MFA).

Gestión de acceso de usuarios

El acceso a sistemas, aplicaciones o información ya sea que se concedida o se revoque, es un proceso de dos pasos:

- Se asigna una "ID de usuario" a un usuario, se habilita y finalmente se inhabilita o revoca.
- Los derechos de acceso se asignan o se revocan a partir de ese ID de usuario.

Identidades de usuario

- Asignar identificaciones únicas a una sola persona para garantizar la responsabilidad individual.
- Deshabilitar o eliminar las identificaciones de usuario dentro de las 24 horas posteriores a la recepción de la notificación de terminación del contrato del empleado.
- No reemitir credenciales previamente asignadas a otros usuarios.
- Descartar ID de usuario que ya no sean en uso.

Identidades de aplicaciones o sistemas

- Requerir el cambio de contraseña cada 90 días
- Asignar las cuentas de servicio, por defecto, al titular de la aplicación o del sistema, o en su defecto a una persona autorizada. El propietario de la cuenta de servicio es responsable de su uso.
- Las cuentas de servicio pueden transferirse a un nuevo propietario cuando finaliza el contrato.
- Deshabilitar o eliminar las cuentas de servicio que ya no se necesitan.
- Requerir un mínimo de 8 caracteres de longitud y permitir que el propietario seleccione contraseñas de longitud significativamente mayor. Acepte todos los caracteres de impresión ASCII.

Aprovisionamiento de acceso

- Asignar derechos de acceso en función de las necesidades corporativas.
- Implementar un proceso de autorización para aplicaciones y sistemas según lo requieran los datos o activos clasificación
- Realizar los trámites de autorización previos a la habilitación de los derechos de acceso.

Administrar los derechos de acceso privilegiado

Se debe tener mucho cuidado respecto a la asignación de acceso privilegiado y con la menor cantidad de privilegios necesarios. Mitigar el uso inapropiado de los derechos de acceso privilegiado, para evitar violaciones o fallas de datos.

- Asignar derechos de acceso privilegiado a los usuarios según la necesidad del rol.
- Mantener un proceso de autorización y registro para la asignación de accesos privilegiados. Completar los trámites de autorización antes de habilitar los derechos de acceso.
- Desarrollar e implementar procedimientos para evitar el uso no autorizado de ID de usuarios administrativos genéricos.
- Identificar y rastrear los derechos de acceso privilegiado asociados con cada sistema o dispositivo.
- Mantener la confidencialidad de la información de autenticación personal para las identificaciones de usuarios administrativos genéricos.

Revocación de derechos de acceso

- Eliminar los derechos de acceso cuando ya no exista una necesidad corporativa para que el empleado no tenga acceso.
- Bloquear o eliminar el acceso dentro de las 24 horas posteriores a la recepción de la notificación de terminación del contrato de un empleado.

Control de acceso a aplicaciones y sistemas

Procedimientos de inicio de sesión seguro

Utilice procedimientos de inicio de sesión seguros para controlar el acceso a aplicaciones y sistemas:

- Implementar mecanismos multifactoriales para cualquier autenticación sobre redes públicas.
- Implementar mecanismos multifactoriales para cualquier autenticación de usuarios con derechos de acceso privilegiado.
- Proteger el sistema de autenticación contra intentos de inicio de sesión de fuerza bruta, por ejemplo, con bloqueo procedimientos después de 5 intentos fallidos de inicio de sesión dentro de un cierto intervalo de tiempo.
- Registrar los intentos de inicio de sesión exitosos y fallidos.
- Registrar un evento de seguridad si se detecta un intento o una violación exitosa de los controles de inicio de sesión.
- No transmitir credenciales en texto claro por ninguna red.
- Terminar las sesiones inactivas después de 30 minutos o más de inactividad.

Gestión de contraseñas

La contraseña para todos los sistemas y aplicaciones de GOTALK SAS, en todos los entornos, debe tener las siguientes características:

- Genere o permita que el usuario cree una contraseña o frase de contraseña segura.
- Proporcionar un medio para que el usuario cambie o regenere la contraseña.
- Requerir el cambio de contraseña cuando exista evidencia o sospecha de compromiso.
- Requerir el cambio de contraseña cada 90 días.
- Evitar el uso de contraseñas triviales o fáciles de adivinar o comprometidas, es decir, evitar el uso de la ID de usuario como contraseña, números consecutivos, etc.
- Considere proporcionar una opción para mostrar la contraseña a medida que se escribe, en lugar de una serie de puntos o asteriscos.
- No permita que el usuario almacene una "pista" de contraseña que podría usarse para recuperar una contraseña olvidada. No pida al usuario que utilice información específica al crear una contraseña (“cómo se llama su primera mascota”).

4. **Uso de cifrado**

El cifrado se utiliza para proteger los datos en tránsito en redes públicas y privadas, así como los datos almacenados en aplicaciones o sistemas. El uso adecuado del cifrado en la red mitiga amenazas como el espionaje caídas, fugas de información y ataques.

El cifrado de los datos almacenados ("en reposo") protege contra el acceso no autorizado en caso de una violación del sistema, así como el acceso por parte de usuarios no autorizados y/o administradores deshonestos. El cifrado de discos y otros medios de almacenamiento protege la información cuando los dispositivos o medios se pierden o son robados.

El departamento de TI es el área autorizado y responsable de definir y establecer los algoritmos de cifrado y las respectivas herramientas. Por lo tanto, tener en cuenta:

- Determinar qué datos se deben cifrar teniendo en cuenta la aplicación y la ubicación de almacenamiento de los datos.
- En un entorno virtualizado o en la nube, cuando se requiera el cifrado de datos a través de la red, cifre los datos cuando se transmitan entre aplicaciones que residan en sistemas operativos separados o contenedores virtuales, y cuando se transmitan a través de redes virtualizadas.
- Utilice solo algoritmos de cifrado aprobados y longitudes de clave mínimas.

5. Seguridad de las Operaciones

Procedimientos operativos documentados

Crear y mantener procedimientos operativos documentados y tenerlos a disposición de todos los usuarios relevantes.
Esto proporciona a todos los usuarios una referencia de los procedimientos acordados, lo que permite una gestión coherente de la seguridad de la aplicación o el sistema. Podrían incluir: instalación y configuración de aplicaciones y sistemas; procedimientos de arranque y cierre; procedimientos de mantenimiento
y respaldo; procedimientos de manejo de información tanto en actividades manuales como automatizadas; determinación y manejo de problemas; registro y monitoreo centralizados; comunicación con contactos de soporte y escalamiento y manejo de incidentes de seguridad.

Separación de entornos

Separar los entornos de producción y de prueba para reducir los riesgos de acceso no autorizado o cambios en el entorno de producción.

- Definir y documentar procedimientos para la transferencia de software de no producción a producción.
- Operar software de producción y no producción en dominios de seguridad segregados (como sistemas separados, controles de acceso separados).
- Probar los cambios en las aplicaciones en un entorno que no sea de producción antes de aplicar los cambios en los sistemas de producción.
- Sólo en circunstancias excepcionales realizar pruebas en los sistemas de producción.
- No copie datos de producción en un entorno que no sea de producción a menos que el equivalente de producción se proporcionan controles.

Gestión de cambios

Es importante controlar los cambios operativos para reducir el riesgo de impacto adverso en la confidencialidad, integridad o disponibilidad de la información y el entorno operativo. Evaluar, documentar y gestionar los cambios operativos que podrían alterar la eficacia de los controles de seguridad de los activos. Pueden incluir las siguientes características: documentación del cambio, incluido cualquier impacto potencial en los controles de seguridad.

Protección de malware

- Implementar medidas técnicas adecuadas a la plataforma para evitar la ejecución y propagación de código malicioso (malware).
- El software antimalware es obligatorio para detectar y bloquear intentos de ejecución de malware en tiempo real, buscar actualizaciones de firmas al menos diariamente y escanear periódicamente en buscade códigos maliciosos almacenados en el activo.
- Registro y monitoreo centralizados de cualquier alerta de la solución antimalware.

Copias de seguridad

- Implementar un procedimiento de respaldo.
- Asegúrese de que los medios de copia de seguridad estén protegidos contra el acceso no autorizado.
- Mantener un inventario de los medios de respaldo.

Gestión de Vulnerabilidades Técnicas

- Mantener en todo momento una configuración segura de las aplicaciones y sistemas.
- Deshabilitar o limitar el acceso a funciones de la aplicación o componentes del sistema que no se utilizan.

Escaneo de vulnerabilidades

Resuelva las vulnerabilidades de seguridad de manera oportuna para limitar la exposición de la aplicación o el sistema.

- Se requiere un análisis de vulnerabilidades para aplicaciones y bases de datos antes de la activación del servicio.
- Se requiere un análisis de vulnerabilidad periódico para todas las aplicaciones y sistemas.

6. Seguridad de la red

Las redes seguras protegen la información en los sistemas y aplicaciones. Teniendo en cuenta los siguientes objetivos:

- El acceso a las redes de GOTALK SAS solo está disponible para las partes autorizadas.
- Las redes están diseñadas para ser resistentes cuando se enfrentan a amenazas externas de intrusión y ruptura.

Gestión de red

- Permitir que solo los sistemas autorizados se conecten a las redes operadas por GOTALK SAS.
- Proporcionar controles técnicos para evitar conexiones de red no autorizadas a sistemas, aplicaciones y dispositivos de red.
- Proporcionar controles técnicos para detectar y prevenir intrusiones, y para defenderse contra la denegación de servicio y ataques.
- Bloquear el acceso a Internet a hosts maliciosos conocidos y bloquear el acceso a Internet a contenido inapropiado.

7. Seguridad de eliminación y reutilización de activos.

Para desechar de forma segura los sistemas o medios, o para preparar estos activos de forma segura para su reutilización asegurarse de que los datos del activo sean irrecuperables.

- Antes de la reutilización interna, se debe hacer que los datos del activo sean ilegibles.
- Antes de la reutilización externa, hacer que los datos del activo sean irrecuperables.
- Destruir físicamente los medios electrónicos de los bienes que no vayan a ser reutilizados.

8. Incidentes de seguridad

El equipo de respuesta a incidentes de GOTALK SAS es el único equipo de respuesta a incidentes de seguridad autorizado para incidentes relacionados con los entornos informáticos de GOTALK SAS. Esto incluye todos los sistemas y activos de TI de propiedad y administración de GOTALK SAS.
En la medida de lo posible, además de informar un incidente sospechoso de inmediato al Equipo de Respuesta a Incidentes de GOTALK SAS, no tome medidas para recopilar evidencia, almacenar evidencia o información sobre el incidente, realizar análisis forenses, restaurar datos o alterar el Activo de TI afectado, a menos que se le indique.

9. Capacitación de concientización sobre seguridad

El propósito de la capacitación de concientización sobre seguridad es ayudar a los asociados a reconocer y evaluar las diversas amenazas que enfrentamos a diario.

- Hay que asegurar que todos los empleados de GOTALK SAS estén conscientes de los riesgos de seguridad asociados con sus actividades y de las políticas, estándares y procedimientos aplicables relacionados con la seguridad de los sistemas de GOTALK SAS.
- Garantizar que los empleados de GOTALK SAS estén capacitados para llevar a cabo las funciones asignadas relacionadas con la seguridad de la información.
- Proporcionar y garantizar la finalización de la formación en materia de seguridad centrada en el reconocimiento y la notificación de posibles indicadores de amenazas.

10. Cumplimiento

Cumplimiento de requisitos legales y contractuales

- Todos los requisitos legales, estatutarios, reglamentarios y contractuales aplicables relacionados con la información la seguridad y la tecnología de la información deben identificarse, documentarse, mantenerse actualizadas y cumplirse.
- Los datos deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legales, reglamentarios, contractuales y comerciales.
- Los datos personales/la información de identificación personal debe protegerse según lo exigen la legislación y la regulación pertinentes.

Consideraciones de auditoría del sistema de información

- Se deben implementar procedimientos de auditoría para ayudar a garantizar que las actividades que involucran revisiones o auditorías se planifiquen cuidadosamente para minimizar el riesgo de interrupciones en los procesos comerciales.
- Se deben implementar controles de acceso para ayudar a prevenir el acceso no autorizado y/o el abuso de la auditoría.
- Los sistemas de información de GOTALK SAS deben estar habilitados para generar registros de auditoría que contengan detalles para ayudar a establecer qué tipo de evento ocurrió, cuándo y dónde ocurrió el evento, la fuente y el resultado del evento y la identidad de cualquier individuo o sujeto asociado con el evento.

Por lo tanto, se debe hacer cumplimiento de las políticas y lineamientos de seguridad, sin alguna excepción, con el fin de garantizar las buenas prácticas para la protección de los activos de información.

6.4. DOCUMENTACIÓN MÍNIMA PARA ESTABLECER UN SGSI

La norma 27001 establece cuales son todos los requisitos necesarios para el SGSI de una empresa. Promoviendo eficacia de la información sensible y destaca todas las vulnerabilidades aseguradas que se encuentran protegidas contra las amenazas.[31]

Es importante conocer que como parte de la implementación de un SGSI basada en la norma ISO 27001:2013, se requiere que se produzcan una serie de documentos. La norma ISO 27001:2013 establece los siguientes documentos obligatorios:

- Alcance
- Política de seguridad de la información
- Proceso de evaluación de riesgos para la seguridad de la información
- Proceso de tratamiento de riesgos de seguridad de la información
- Declaración de aplicabilidad
- Los objetivos de seguridad de la información
- Evidencia de la competencia
- Los resultados de las evaluaciones de riesgos realizadas
- Los resultados el tratamiento de la información de riesgos de seguridad
- La evidencia de la de la motorización de la información de desempeño de seguridad y los resultados de medición
- Programa de auditoría interna y los resultados de la auditoría
- Procedimiento de auditoría interna
- La evidencia de todos los resultados de las revisiones por la dirección
- La evidencia de la naturaleza de las no conformidades y de cualquier acción tomada posteriormente, y los resultados de cualquier acción correctiva

Para la empresa Gotalk SAS y con base a los objetivos del diseño SGSI se reúne y produce los siguientes documentos:

- Alcance
- Política de seguridad de la información
- Proceso de evaluación de riesgos para la seguridad de la información
- Proceso de tratamiento de riesgos de seguridad de la información
- Declaración de aplicabilidad
- Los objetivos de seguridad de la información

A continuación, se presenta el documento del diseño del SGSI para la empresa Gotalk SAS, con la relación de los documentos mínimos requeridos por la norma ISO 27001:2013.

31 ISOTools Excellence. Documentación requerida por la ISO 27001. Blog. 2016. p1.

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI PARA LA EMPRESA GOTALK SA

1. ALCANCE

El sistema de gestión de seguridad de la información de la empresa Gotalk SAS se aplica a todos los activos de información, sin excepción y de igual manera a todos los empleados, proveedores y accionistas de la empresa. El cumplimiento es obligatorio y responsabilidad de cada una de las unidades de la empresa.

2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Tiene como propósito establecer los principios y requisitos para la protección de los sistemas de tecnología de la información de GOTALK SAS y la información que contienen. Los principios y requisitos de esta política están definidos por el departamento de Seguridad para proteger a GOTALK SAS, empleados y estudiantes del daño causado por el mal uso de los activos de GOTALK SAS y nuestros datos. El mal uso de estos activos incluye tanto acciones deliberadas como involuntarias.

Para mayor detalle de las políticas de seguridad de la información, se puede dirigir al apartado 6.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN y al Anexo C y Anexo D del presente documento.

3. PROCESO DE EVALUACIÓN DE RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN

En este proceso se hace uso de la metodología MAGERIT basado en el Libro I y II, para la identificación de los activos de información con su respectivo tipo y valoración del activo, identificación de las amenazas y su valoración de impacto para establecer el nivel de daño que puede llegar a causar si se materializa el riesgo en los activos identificados.

En el apartado 6.1 EVALUACIÓN ACTIVOS DE INFORMACIÓN se relaciona en detalle como se hizo uso de la metodología para la evaluación de riesgo y en el Anexo A de este documento se encuentra en detalle la evaluación de riesgos para los activos de información de la empresa.

4. PROCESO DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Se continua con la metodología MAGERIT para el tratamiento de riesgos teniendo en cuenta las salvaguardas y controles del Anexo A de la norma ISO 27001:2013, con la finalidad de mitigar cada uno de los riesgos identificados.

Para mayor detalle del tratamiento de riesgos podemos encontrar en el apartado 6.2 SALVAGUARDAS PARA LOS ACTIVOS DE INFORMACIÓN como se aplicó el Anexo A de la norma ISO 27001:2013 y en el Anexo B de este documento se puede evidenciar cada una de las salvaguardas que se deberían aplicar para los riesgos identificados.

5. DECLARACIÓN DE APLICABILIDAD

Luego de identificar los riesgos de seguridad y establecer las medidas para la mitigación de estos, es necesario e indispensable establecer la declaración de aplicabilidad con los controles de seguridad para reforzar los procesos para la protección de la información.

Esta declaración de aplicabilidad se definió basado en el Anexo A de la norma ISO 27001:2013, donde se relaciona 14 dominios y 114 controles.

Para la empresa se definió que se debe aplicar los 114 controles debido a los riesgos identificados y a la falta de contar con políticas y procedimientos de seguridad, también para la gestión de contratación, seguridad física y lógica, relación con proveedores, ambiente de desarrollo de la página web y plataforma de los cursos, cumplimiento de las políticas y procedimientos.

En el Anexo G del documento se relaciona la declaración de aplicabilidad de la empresa.

6. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Proteger los activos de información garantizando que solo el personal autorizado pueda acceder y tratar la información de los sistemas, definiendo las categorías de los usuarios, roles y permisos.

- Utilizar métodos de autenticación para evitar la suplantación de identidad, desde la implantación común de las credenciales de acceso y la certificación digital para la mejora de la seguridad y también los niveles de permisos y autorización.

- Definir los niveles de autorización para el acceso y manejo de los activos de información garantizando que se cuente con revisiones periódicas para que el acceso y tratamiento sea de usuarios autorizados y activos teniendo en cuenta la revocación de autorización.

- Proteger la integridad, confidencialidad y disponibilidad de la información mediante procesos autorizados que garanticen el cumplimiento de estos pilares, evitando la modificación y/o alteraciones, divulgación y acceso no autorizado de la información.

- Establecer seguimientos y alertas que puedan vigilar las actividades de seguridad y el registro de posibles incidentes o eventos sospechosos que coloque en riesgo la integridad de la información.

En este apartado se logra relacionar la documentación mínima que requiere la empresa para establecer un SGSI de acuerdo con la norma ISO 27001:2013.

7. CONCLUSIONES

- Tras el desarrollo de los objetivos presentados anteriormente demuestra que mediante la metodología MAGERIT se logró evaluar los activos de información de la empresa Gotalk SAS con el fin de seguir actualizando el inventario de activos de información e identificando las amenazas y vulnerabilidades que se pueden presentar como riesgo para dichos activos.

- Finalmente, al identificar el impacto de las amenazas para los activos de información se define el plan de tratamiento con las salvaguardas para los activos basados en el anexo A de la norma ISO 27001:2013 invitando a la empresa con la aplicación de estos tratamientos para mitigar los riesgos y a su vez con la constante actualización de la identificación de riesgos y el plan de tratamiento.

- Tal y como hemos podido comprobar la empresa frente a la falta de concientización, conocimiento e importancia a la seguridad de la información, sus activos se encuentran en un riesgo con impacto crítico y de atención inmediata lo cual conlleva a la definición de las políticas de seguridad con el fin de orientar y guiar las buenas prácticas y estándares para la gestión segura de la información dando cumplimiento a la norma ISO 27001:2013.

- Gracias a todo lo anterior, podemos fijar los documentos mínimos para que la empresa Gotalk SAS defina el SGSI basado en los requerimientos de la norma ISO 27001:2013 incitando a la empresa que implemente el SGSI garantizando que produzca los documentos obligatorios establecidos en la norma.

8. RECOMENDACIONES

- Implementar los controles y salvaguardas definidos con base al Anexo A de la norma ISO 27001:2013.

- La divulgación de las políticas de seguridad a los empleados y proveedores de la organización y así el cumplimiento de estas.

- Promover la concientización frente a los temas de seguridad y enseñar el valor y la importancia de proteger y salvaguardar los activos de información de la empresa.

- Implementar auditorías internas que velen por el cumplimiento de las políticas y controles de seguridad.

- Continuar con la documentación requerida que falta por crear para dar cumplimiento a la norma ISO 27001:2013 y así conseguir la implementación de la SGSI.

- Contratación de auditores externos que aseguren el cumplimiento legal de la norma ISO 27001:2013

- Importante que el personal especialista en seguridad de la información este en constante actualización frente al campo de seguridad con la finalidad de garantizar y vigilar la protección de los activos de información.

9. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de diseñar el sistema de gestión de seguridad de la información, puedan acceder al documento.

BIBLIOGRAFÍA

AMENAZAS A la seguridad de la información [Anónimo] [Sitio WEB]. Argentina: Universidad Nacional de Lujan. [Consultado: 30, enero, 2022]. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Blog Concepto. Dato [Sitio WEB]. [Consultado: 26, febrero, 2023]. Disponible en: https://concepto.de/dato/

CCIT. Informe de las Tendencias del Cibercrimen en Colombia 2019-2020 [Sitio WEB]. Bogotá: Copyright. [Consultado: 21, enero, 2022]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Cárdenas, Fabian. ¿Qué es la gestión de activos de información? [Sitio WEB]. Blog Novasec. [Consultado: 26, febrero, 2023]. Disponible en: https://www.novasec.co/blog/67-gestion-de-activos-de-información

CARISIO, Emanuel. Vulnerabilidad Informática ¿Cómo protegerse? [Sitio WEB]. Barcelona: Media PRO [Consultado: 30, enero, 2022]. Disponible en: https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/

ECURED. Ataque informático [Sitio WEB]. Ecured.co. [Consultado: 30, enero, 2022]. Disponibles en: https://www.ecured.cu/Ataque_inform%C3%A1tico

EN SOLO tres meses Colombia sufren 42 billones de intentos de ataques cibernéticas [Anónimo] [Sitio WEB]. Colombia: Semana. [Consultado: 21, enero, 2022]. Disponible en: https://www.semana.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556/

ESCUELA EUROPEA DE EXCELENCIA. Mitigación de riesgos: proceso de 3 pasos para hacer frente al riesgo [Sitio WEB]. 2021 [Consultado: 26, febrero, 2023]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2021/06/mitigacion-de-riesgos-proceso-de-3-pasos-para-hacer-frente-al-riesgo/

FUNCIÓN PÚBLICA. Ley 1581 de 2012 [Sitio WEB]. Colombia: Gov.co. [Consultado: 30, enero, 2022]. Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

FUNCIÓN PÚBLICA. Ley 1712 de 2014 [Sitio WEB] Colombia: Consejo de la Republica. [Consultado: 8, febrero, 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

IBM. Política y objetivos de seguridad [Sitio WEB]. Blog IBM. 2021 [Consultado: 26, febrero, 2023]. Disponible en: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

IBM. ¿Qué es el ransomware? [Sitio WEB]. [Consultado: 26, febrero, 2023]. Disponible en: https://www.ibm.com/co-es/topics/ransomware

ICONTEC. Norma Técnica NTC ISO IEC COLOMBIANA 27001 [Sitio WEB]. Colombia: ICONTEC. [Consultado: 30, enero, 2022]. Disponible en: file:///C:/Users/JULY%20VARGAS/Downloads/NORMA_TECNICA_NTC_ISO_IEC_COLOMBIANA_270.pdf

ICONTEC. Norma Técnica NTC-ISO/IEC Colombiana 27001 [Sitio WEB]. Colombia: ICONTEC. [Consultado: 30, enero,2022]. Disponible en: https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf

INTEDYA. ISO 27000 y el conjunto de estándares de seguridad de la información [Sitio WEB]. Internacional Dynamic Advisors. [Consultado: 22, enero, 2022]. Disponible en: https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-información.html#:~:text=ISO%2027000%20es%20un%20conjunto,la%20Seguridad%20de%20la%20Informaci%C3%B3n.

ISOTools Excellence. Anexo A en ISO 27001, objetivos de control y controles de referencia [Sitio WEB]. Blog pmg-ssi. 2020 [Consultado: 7, abril, 2023]. Disponible en: https://www.pmg-ssi.com/2020/03/anexo-a-en-iso-27001-objetivos-de-control-y-controles-de-referencia/

ISOTools Excellence. Documentación requerida por la ISO 27001 [Sitio WEB]. Blog pmg-ssi. 2020 [Consultado: 7, abril, 2023]. Disponible en: https://www.pmg-ssi.com/2016/05/documentacion-requerida-por-la-iso-27001/

ISO 2700.SGSI [Sitio WEB]. ISO 2700.ES. [Consultado: 22, enero, 2022]. Disponible en: https://www.iso27000.es/sgsi.html

ISOTOOLS. ISO 27001: Ciclo de Deming [Sitio WEB]. Blog PHG-SSI. [Consultado: 30, enero, 2022]. Disponible en: https://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/#:~:text=La%20norma%20ISO%2027001%20incluye,describir%20de%20la%20siguiente%20forma%3A&text=Hacer%3A%20se%20implantan%20los%20procesos.

MAGERIT. Metodología de análisis y gestión de riesgos de los sistemas de información Libro I Método [Sitio WEB]. España. 2012 [Consultado: 7, abril, 2023]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

MAGERIT. Metodología de análisis y gestión de riesgos de los sistemas de información Libro II Catalogo de Elementos [Sitio WEB]. España. 2012 [Consultado: 7, abril, 2023]. Disponible en: https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file

MINTIC. Guía para la Gestión y Clasificación de Incidentes de seguridad de la información [Sitio WEB]. Colombia: MINTIC. [Consultado: 30, enero, 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MINTIC. Ley 1273 de 2009 [Sitio WEB]. Colombia: Congreso de Colombia. [Consultado: 30, enero, 2022]. Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

MOJICA, Manuel y ALVAREZ, Yenny. El análisis de riesgo en la seguridad de la información [Sitio WEB]. Dep. Legal. [Consultado: 30, enero, 2022]. Disponible en: file:///C:/Users/JULY%20VARGAS/Downloads/Dialnet-ElAnalisisDeRiesgoEnLaSeguridadDeLaInformacionNota-6505355%20(1).pdf

¿QUE ES? Triada CID (confidencialidad, integridad y disponibilidad) [Anónimo]. [Sitio WEB]. [Consultado: 21, enero, 2022]. Disponible en: https://www.ontek.net/que-es-triada-cid/

SEGURIDAD DE la información: Aspectos para tener en cuenta [Anónimo] [Sitio WEB]. Blog Ayudaley protección datos. [Consultado: 30, enero, 2022]. Disponible en: https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/

SIGNIFICACION DE la información [Anónimo] [Sitio WEB]. Signficados.com. [Consultado: 30, enero, 2022]. Disponible en: https://www.significados.com/informacion/

ANEXOS

Anexo A. Matriz Evaluación de Riesgo
Link: Anexo A Matriz Evaluación del Riesgo.xlsx

Anexo B. Tratamiento del riesgo
Link: Anexo B Tratamiento del riesgo.xlsx

Anexo C. SegInf P1.0
Link: Anexo C SegInf P1.0.docx

Anexo D SegInf P2.0
Link: Anexo D SegInf P2.0.docx

Anexo E Autorización Empresa
Link: Autorización Empresa.pdf

Anexo F Acuerdo de confidencialidad
Link: Acuerdo de confidencialidad.pdf

Anexo G Declaración de Aplicabilidad
Link: Anexo G Declaración de Aplicabilidad Gotalk SAS.xlsx

RESUMEN ANALITICO EDUCATIVO
RAE

Título del texto	Diseño De Un Sistema De Gestión De Seguridad De La Información SGSI Para La Empresa Gotalk SAS Con Base A La Norma ISO 27001:2013
Nombres y Apellidos del Autor	July Estefania Vargas Macias
Año de la publicación	2024

Resumen del texto:
Debido al crecimiento y la migración de informacion digital de la empresa Gotalk SAS, así como el aumento de amenazas, vulnerabilidades y ataques cibernéticos, se hace necesario conocer e implementar la norma ISO 27001:2013. Esta norma establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), con el objetivo de fortalecer la seguridad, lograr la certificación y aumentar el valor de la organización.
El presente proyecto busca diseñar un SGSI considerando los antecedentes, el funcionamiento de la empresa y la normativa vigente. Para ello, se empleará el modelo PHVA (Planificar, Hacer, Verificar, Actuar) incluido en la norma ISO 27001:2013, siguiendo cada paso del ciclo. Los objetivos incluyen la creación de políticas de seguridad de la información y la identificación de los activos actuales de Gotalk SAS. Finalmente, se presentará el diseño del SGSI a la Gerencia para asegurar el cumplimiento de la documentación requerida por la norma ISO 27001:2013.

Palabras Claves	informacion, riesgo, vulnerabilidad, amenaza, controles y mitigar.

Definición de la problemática: Debido a la preocupación expresada por el Gerente de Gotalk SAS frente a los temas de seguridad de la información y quien, en su poco conocimiento respecto al tema, pero quien considera la importancia de cumplir y garantizar la seguridad de la información que se maneja en la empresa sugiere como iniciativa la revisión global del estatus actual de la empresa.
Esto conlleva a realizar la visita a la empresa Gotalk SAS; que, con base a la visita y a la información suministrada por parte de gerencia, se evidencia como la información que se maneja se encuentra en alto riesgo y exposición frente a las vulnerabilidades de seguridad y junto con ello la necesidad de diseñar el sistema de gestión de seguridad de la información. También se evidencia que el personal administrativo y gerencia no cuenta con capacitación y concientización frente a la seguridad de la información, así como tampoco cuenta con políticas de seguridad establecidas.
Teniendo en cuenta el contexto y funcionamiento de la empresa, administrando y manipulando información sensible como lo son los datos personales de los Estudiantes y Profesores, dicha información se encuentra en línea alijada en servidores que es suministrado por los Estudiantes en el momento de registrarse a la plataforma y realizar sus cursos, de igual manera para los profesores de varios países latinoamericanos y otros continentes. Es importante resaltar el cumplimiento de la Ley 1581 de 2012 de acuerdo con el tratamiento de datos y teniendo como finalidad garantizar la protección de los datos personales.

Objetivos:

- **General**: Diseñar un SGSI basado en la norma ISO/IEC 27001:2013, para la gestión de la seguridad de la información en la organización GOTALK S.A.S.

- **Específicos**:
  - Evaluar los activos de información de la organización GOTALK S.A.S mediante la aplicación de metodologías para la medición del riesgo que permita identificar el impacto de las amenazas.
  - Proponer las salvaguardas para los activos de información basados en el anexo A de la norma ISO/IEC 27001:2013 para hacer frente a las amenazas identificadas.
  - Establecer las políticas de seguridad a partir de buenas prácticas y estándares para la gestión segura de la información.
  - Consolidar la documentación mínima requerida para el establecimiento de un SGSI de acuerdo con la norma ISO/IEC 27001:2013 para la gestión de la seguridad en la organización.

Metodología: La metodología utilizada es MAGERIT, que permite evaluar riesgos y amenazas a los activos de información, identificar su impacto y proponer salvaguardas y controles para mitigar los riesgos identificados.
Se aplica el ciclo de Deming (PHVA): Planificar, Hacer, Verificar, Actuar.

- Planificar: se establecen los objetivos y los procesos necesarios para conseguir resultados según las necesidades de los clientes y la política de seguridad de la organización.
- Hacer: se implantan los procesos.
- Verificar: se revisan y se evalúan tanto lo servicios como los procesos comprándolos con las políticas, los objetivos y los requisitos de información sobre los resultados.
- Actuar: comienzan a emprender acciones para mejorar el rendimiento del Sistema de Gestión Ambiental de forma continua.

Resultados:

- Evaluación de Activos: Identificación y valoración cualitativa y cuantitativa de los activos de información de GOTALK SAS.
- Amenazas y Vulnerabilidades: Identificación de 120 amenazas basadas en el catálogo de amenazas de MAGERIT v3.0.
- Salvaguardas: Propuesta de controles y salvaguardas basadas en el Anexo A de la norma ISO 27001:2013.
- Políticas de Seguridad: Definición de políticas generales y específicas para la seguridad de la información.
- Documentación: Elaboración de los documentos mínimos requeridos por la norma ISO 27001:2013.

Conclusiones:

- El desarrollo de los objetivos establecidos demostró que, mediante la metodología MAGERIT, se logró evaluar los activos de información de Gotalk SAS. Esto permitió actualizar el inventario de activos e identificar las amenazas y vulnerabilidades que representan riesgos para dichos activos.
- Finalmente, al identificar el impacto de las amenazas para los activos de información, se definió un plan de tratamiento con salvaguardas basadas en el anexo A de la norma ISO 27001:2013. Se invita a la empresa a aplicar estos tratamientos para mitigar los riesgos y a actualizar constantemente la identificación de riesgos y el plan de tratamiento.
- La falta de concientización y conocimiento sobre la seguridad de la información en la

empresa ha puesto a sus activos en un riesgo crítico que requiere atención inmediata. Esto ha llevado a la definición de políticas de seguridad para orientar y guiar las buenas prácticas y estándares para la gestión segura de la información, cumpliendo con la norma ISO 27001:2013.

- Gracias a todo lo anterior, se pueden establecer los documentos mínimos necesarios para que Gotalk SAS defina su SGSI basado en los requerimientos de la norma ISO 27001:2013. Se incita a la empresa a implementar el SGSI y garantizar la producción de los documentos obligatorios establecidos por la norma.

Recomendaciones:

- Implementar los controles y salvaguardas propuestos.
- Divulgar las políticas de seguridad a empleados y proveedores.
- Promover la concientización sobre la seguridad de la información.
- Realizar auditorías internas para asegurar el cumplimiento de las políticas.
- Contratar auditores externos para verificar el cumplimiento legal de la norma ISO 27001:2013.
- Mantener al personal de seguridad de la información actualizado sobre las mejores prácticas y nuevas amenazas.

Bibliografía citada por el autor:

- AMENAZAS A la seguridad de la información [Anónimo] [Sitio WEB]. Argentina: Universidad Nacional de Lujan. [Consultado: 30, enero, 2022]. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12
- Blog Concepto. Dato [Sitio WEB]. [Consultado: 26, febrero, 2023]. Disponible en: https://concepto.de/dato/
- CCIT. Informe de las Tendencias del Cibercrimen en Colombia 2019-2020 [Sitio WEB]. Bogotá: Copyright. [Consultado: 21, enero, 2022]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf
- Cárdenas, Fabian. ¿Qué es la gestión de activos de información? [Sitio WEB]. Blog Novasec. [Consultado: 26, febrero, 2023]. Disponible en: https://www.novasec.co/blog/67-gestion-de-activos-de-información
- CARISIO, Emanuel. Vulnerabilidad Informática ¿Cómo protegerse? [Sitio WEB]. Barcelona: Media PRO [Consultado: 30, enero, 2022]. Disponible en: https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/
- ECURED. Ataque informático [Sitio WEB]. Ecured.co. [Consultado: 30, enero, 2022]. Disponibles en: https://www.ecured.cu/Ataque_inform%C3%A1tico
- EN SOLO tres meses Colombia sufren 42 billones de intentos de ataques cibernéticas [Anónimo] [Sitio WEB]. Colombia: Semana. [Consultado: 21, enero, 2022]. Disponible en: https://www.semana.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556/
- ESCUELA EUROPEA DE EXCELENCIA. Mitigación de riesgos: proceso de 3 pasos para hacer frente al riesgo [Sitio WEB]. 2021 [Consultado: 26, febrero, 2023]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2021/06/mitigacion-de-riesgos-proceso-de-3-pasos-para-hacer-frente-al-riesgo/
- FUNCIÓN PÚBLICA. Ley 1581 de 2012 [Sitio WEB]. Colombia: Gov.co. [Consultado: 30, enero, 2022]. Disponible en:

https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf
- FUNCIÓN PÚBLICA. Ley 1712 de 2014 [Sitio WEB] Colombia: Consejo de la Republica. [Consultado: 8, febrero, 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882
- IBM. Política y objetivos de seguridad [Sitio WEB]. Blog IBM. 2021 [Consultado: 26, febrero, 2023]. Disponible en: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives
- IBM. ¿Qué es el ransomware? [Sitio WEB]. [Consultado: 26, febrero, 2023]. Disponible en: https://www.ibm.com/co-es/topics/ransomware
- ICONTEC. Norma Técnica NTC ISO IEC COLOMBIANA 27001 [Sitio WEB]. Colombia: ICONTEC. [Consultado: 30, enero, 2022]. Disponible en: file:///C:/Users/JULY%20VARGAS/Downloads/NORMA_TECNICA_NTC_ISO_IEC_COLOMBIANA_270.pdf
- ICONTEC. Norma Técnica NTC-ISO/IEC Colombiana 27001 [Sitio WEB]. Colombia: ICONTEC. [Consultado: 30, enero,2022]. Disponible en: https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf
- INTEDYA. ISO 27000 y el conjunto de estándares de seguridad de la información [Sitio WEB]. Internacional Dynamic Advisors. [Consultado: 22, enero, 2022]. Disponible en: https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-información.html#:~:text=ISO%2027000%20es%20un%20conjunto,la%20Seguridad%20de%20la%20Informaci%C3%B3n.
- ISOTools Excellence. Anexo A en ISO 27001, objetivos de control y controles de referencia [Sitio WEB]. Blog pmg-ssi. 2020 [Consultado: 7, abril, 2023]. Disponible en: https://www.pmg-ssi.com/2020/03/anexo-a-en-iso-27001-objetivos-de-control-y-controles-de-referencia/
- ISOTools Excellence. Documentación requerida por la ISO 27001 [Sitio WEB]. Blog pmg-ssi. 2020 [Consultado: 7, abril, 2023]. Disponible en: https://www.pmg-ssi.com/2016/05/documentacion-requerida-por-la-iso-27001/
- ISO 2700.SGSI [Sitio WEB]. ISO 2700.ES. [Consultado: 22, enero, 2022]. Disponible en: https://www.iso27000.es/sgsi.html
- ISOTOOLS. ISO 27001: Ciclo de Deming [Sitio WEB]. Blog PHG-SSI. [Consultado: 30, enero, 2022]. Disponible en: https://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/#:~:text=La%20norma%20ISO%2027001%20incluye,describir%20de%20la%20siguiente%20forma%3A&text=Hacer%3A%20se%20implantan%20los%20procesos.
- MAGERIT. Metodología de análisis y gestión de riesgos de los sistemas de información Libro I Método [Sitio WEB]. España. 2012 [Consultado: 7, abril, 2023]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html
- MAGERIT. Metodología de análisis y gestión de riesgos de los sistemas de información Libro II Catalogo de Elementos [Sitio WEB]. España. 2012 [Consultado: 7, abril, 2023]. Disponible en: https://pilar.ccn-

cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file

- MINTIC. Guía para la Gestión y Clasificación de Incidentes de seguridad de la información [Sitio WEB]. Colombia: MINTIC. [Consultado: 30, enero, 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
- MINTIC. Ley 1273 de 2009 [Sitio WEB]. Colombia: Congreso de Colombia. [Consultado: 30, enero, 2022]. Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf
- MOJICA, Manuel y ALVAREZ, Yenny. El análisis de riesgo en la seguridad de la información [Sitio WEB]. Dep. Legal. [Consultado: 30, enero, 2022]. Disponible en: file:///C:/Users/JULY%20VARGAS/Downloads/Dialnet-ElAnalisisDeRiesgoEnLaSeguridadDeLaInformacionNota-6505355%20(1).pdf
- ¿QUE ES? Triada CID (confidencialidad, integridad y disponibilidad) [Anónimo]. [Sitio WEB]. [Consultado: 21, enero, 2022]. Disponible en: https://www.ontek.net/que-es-triada-cid/
- Seguridad de la información: Aspectos para tener en cuenta [Anónimo] [Sitio WEB]. Blog Ayudaley protección datos. [Consultado: 30, enero, 2022]. Disponible en: https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/
- Significación de la información [Anónimo] [Sitio WEB]. Signficados.com. [Consultado: 30, enero, 2022]. Disponible en: https://www.significados.com/informacion/

Nombre y apellidos de quien elaboró este RAE	July Estefania Vargas Macias
Fecha en que se elaboró este RAE	16 de mayo de 2024