DISEÑO DE UNA HERRAMIENTA WEB BASADA EN EL MARCO DE TRABAJO CSF NIST PARA LA EVALUACIÓN DE RIESGOS INFORMÁTICOS E IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA G0 S.A.S

JUAN GUILLERMO CAMPOS GARCIA
OSCAR MIGUEL MORENO MORALES

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2021

DISEÑO DE UNA HERRAMIENTA WEB BASADA EN EL MARCO DE TRABAJO CSF NIST PARA LA EVALUACIÓN DE RIESGOS INFORMÁTICOS E IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA G0 S.A.S

JUAN GUILLERMO CAMPOS GARCIA
OSCAR MIGUEL MORENO MORALES

Proyecto de grado para optar por el título de Especialista de Seguridad Informática

Asesor Temático
ALVARO ESCOBAR ESCOBAR
Director Especialización

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2021

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 28 de noviembre 2021

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág

LISTA DE ANEXOS

GLOSARIO

AMENAZA: es cualquier circunstancia o evento que pueda tener un impacto adverso en las operaciones y los activos de la organización, los individuos, otras organizaciones o la Nación a través de un sistema de información a través del acceso no autorizado, destrucción, divulgación o modificación de información y / o denegación de servicio.[1]

CATÁLOGO DE CONTROL: caja de herramientas que contiene una colección de salvaguardas, contramedidas, técnicas y procesos para responder a los riesgos de seguridad y privacidad.[2]

CONTROL: descripciones de las salvaguardas y capacidades de protección apropiadas para lograr los objetivos particulares de seguridad y privacidad de la organización y reflejar las necesidades de protección de las partes interesadas de la organización.[3]

CONTROLES DE SEGURIDAD: salvaguardas o contramedidas empleadas dentro de un sistema o una organización para proteger la confidencialidad, integridad y disponibilidad del sistema y su información y para administrar la seguridad de la información riesgo.[4]

CIBERSEGURIDAD: capacidad de proteger o defender el uso del ciberespacio de *cyber* ataques.[5]

EVALUACION DE RIESGOS: es el proceso de identificar, estimar y priorizar los riesgos de seguridad de la información.[6]

---

[1] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30: Guía para la realización Evaluaciones de riesgo [en línea]. Septiembre de 2012. 17 p. [Consultado: 29 de julio de 2021]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[2] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53 Revisión 5: Controles de seguridad y privacidad para organizaciones y sistemas de información [en línea]. Septiembre de 2020. 29 p. [Consultado: 29 de julio de 2021]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[3] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.35.

[4] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.28.

[5] LÓPEZ DUQUE, Carlos Mario. Diferencia entre seguridad informática y ciberseguridad. En: Colecciones Especialización en Seguridad Informática [en línea]. Universidad Piloto de Colombia, 2018, p.1.[Consultado: 29 de julio de 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8600/Diferencia%20entre%20seguridad%20informatica%20y%20ciberseguridad.pdf?sequence=1&isAllowed=y

[6] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.15.

MALWARE: software especialmente diseñado para dañar o infiltrarse en los sistemas, sin el consentimiento del usuario. Virus informáticos o software malicioso (troyanos, gusanos, *spyware*).[7]

REQUISITO: obligaciones de seguridad y privacidad de la información impuestas a las organizaciones. Expresión de las necesidades de protección de las partes interesadas para un sistema u organización en particular.[8]

RIESGO: es la medida en que una entidad está amenazada por una circunstancia o evento.[9]

RIESGOS INFORMÀTICOS: eventualidad que imposibilita el cumplimiento de un objetivo, es decir, todo aquel peligro o daño que puede afectar el funcionamiento directo o los resultados esperados de un sistema informático.[10]

RIESGO DE INFRAESTRUCTURA: ocurren cuando en las organizaciones no existe una estructura de información tecnológica efectiva (*hardware*, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.[11]

SEGURIDAD INFORMÁTICA: medidas y controles que garantizan la confidencialidad, integridad y disponibilidad de activos del sistema de información, incluido *hardware*, software, *firmware* e información que se procesa, almacena y comunica.[12]

VULNERABILIDAD: es una debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser aprovechada por una fuente de amenaza.[13]

---

[7] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Decálogo Ciberseguridad empresas: Una guía de aproximación para el empresario [en línea]. España.2017. 13 p. [Consultado: 29 de julio de 2021].
Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

[8] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.34.

[9] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.15.

[10] CORDA, María Cecilia; VIÑAS, Mariela; CORIA, Marcela Karina. Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. En: Palabra Clave (La Plata) [en línea]. Universidad Nacional de La Plata Argentina: e032, octubre, 2017, vol. 7, nro. 1, p. 1-18. [Consultado el 29 de Julio del 2021]. Disponible en http://polux.unipiloto.edu.co:8080/00004422.pdf. E-ISSN: 1853-9912.

[11] Ibid. p.9

[12] LÓPEZ DUQUE, Carlos Mario. Diferencia entre seguridad informática y ciberseguridad. En: Colecciones Especialización en Seguridad Informática [en línea]. Op.Cit., p.1.

[13] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.18.

RESUMEN

G0 S.A.S al ser parte del grupo de las pymes de Colombia, toma decisiones de acuerdo su operatividad, dejando en segundo plano el desarrollo de un análisis de riesgos para su infraestructura tecnológica. Entendiendo su situación, se desarrolla el siguiente trabajo como una opción que le permita tanto a G0 S.A.S como a las pequeñas empresas a acceder a estas mejoras de una forma fácil y sencilla.

Se escogió el marco de trabajo CSF NIST porque se adapta muy bien a este tipo de empresas ya que llega más al detalle en la identificación del riesgo, para luego ser evaluado de una forma óptima, contribuyendo al ciclo de vida del desarrollo de la organización.

Con los resultados obtenidos, se encontró que G0 S.A.S presenta falencias salvaguardado la confidencialidad, integridad y disponibilidad en los procedimientos que se efectúan en la empresa. Las oportunidades de mejora en los procesos de la organización, se dan para la segregación de roles y funciones, opciones de tratamiento de riesgos y algunos controles que, de alguna forma, se pueden mitigar para este tipo de riesgo.

Para lograr que G0 SAS tenga acceso a este tipo de conocimiento, se plantea el prototipo presentado en este documento, el cual le permitirá tener acceso de una forma rápida y oportuna habiendo evaluado previamente los riesgos. Adicional, se presenta un listado de controles sugeridos los cuales le permitirán entender a G0 S.A.S si son aplicados de manera oportuna librándolos de eventos de amenaza que pueda causar daños reputacionales o pérdidas monetarias que afecten a la organización.

INTRODUCCIÓN

Las tecnologías de la información, representan un nuevo factor productivo que transforma la operación comercial de las empresas, aportando un ilimitado número de herramientas tecnológicas que permiten la administración, tratamiento y gestión de la información obtenida. Además, los activos generadores de valor como la recepción y procesamiento de los datos, son factores totalmente necesarios para la implementación de la seguridad informática como medida de protección para las operaciones no autorizadas, que puedan ocasionar daños en la red informática.

Es importante considerar que, en el desarrollo y avance tecnológico, existe la necesidad que la información sea protegida en el momento que se utilicen todos los medios electrónicos para generar la operación de las empresas, como llamadas telefónicas móviles, almacenamiento de datos, mensajería instantánea, entre otros. Adicional, es preciso comprender, que cuando no se emplean los respectivos protocolos de seguridad y se presentan fallos en la tecnología, esta información se vuelve vulnerable, ocasionando pérdidas en la organización y quedando expuesta para ser utilizada de forma improductiva.

G0 S.A.S es una empresa dedicada a prestar servicios de desarrollo de software y consultoría informática. Su área de Tecnología es el *Core* de negocio, brindando productos y servicios en la construcción de software y redes de datos, lo cual involucra toda la operatividad del negocio, la cual recae en la infraestructura de red. Debido a lo anterior, es fundamental gestionar la información como un activo transcendental, para proteger la operación de la compañía ante las amenazas y los riesgos existentes asociados a la materialización de un ataque en las tecnologías de la información, gestionando una metodología que permita analizar las vulnerabilidades e identificar los riesgos a los que están expuestos.

Este proyecto de investigación presenta el Marco de Trabajo NIST CSF, como una metodología fundamental para la evaluación de riesgos en la infraestructura tecnológica de G0 S.A.S, identificando las amenazas, vulnerabilidades, y la generación de controles, que permitan el tratamiento de los riesgos con el fin de mitigarlos, de tal forma que reduzca la probabilidad de un ataque o pérdida de información confidencial en la empresa.

En este contexto la aplicación del estándar NIST, genera una propuesta de seguridad y privacidad informática en la infraestructura tecnológica de la empresa, elevando el grado de confiabilidad con los clientes y brindando directrices que conduzcan a la aplicación de la guía implementando seguridad informática, en el manejo de la información que actualmente administra y en los futuros proyectos de crecimiento y posicionamiento tecnológicos de G0 S.A.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

El nuevo mundo digitalizado genera un significativo número de medios de comunicación y negociación, o herramientas electrónicas que permiten la interacción y comercialización de productos y servicios ofertados por las empresas, produciendo el registro de millones de datos de los usuarios que acceden a determinados canales electrónicos:

> Sistemas de información modernos pueden incluir una variedad de plataformas informáticas (por ejemplo, sistemas de control industrial, sistemas informáticos de propósito general, sistemas ciber físicos, supercomputadoras, sistemas de armas, sistemas de comunicaciones, sistemas de control ambiental, dispositivos médicos, dispositivos integrados, sensores y dispositivos móviles como teléfonos inteligentes y tabletas). Todas estas plataformas comparten una base común: computadoras con *hardware*, software y *firmware* complejos que brindan una capacidad que respalda la misión esencial y las funciones comerciales de las organizaciones.[14]

Esta funcionalidad representa la operación comercial de las empresas, la cual cumplen con el objetivo de generar la estabilidad, sostenimiento y proyección económica, por lo tanto, estos activos deben ser protegidos con la implementación de marcos de seguridad, que garanticen la confiabilidad de los sistemas de información, y adicionalmente políticas de seguridad informática respaldadas por los Gobiernos.

En Colombia existe una falencia de seguridad en el eslabón más importante de la cadena productiva, siendo necesario la implementación de marcos de seguridad que permitan al sector empresarial realizar análisis de riesgos y generar controles de seguridad, evitando el crecimiento acelerado de la delincuencia cibernética.

"La pérdida de datos en las organizaciones, los robos de identidad, y la sofisticación del *malware* han hecho que las empresas replanteen todos sus esquemas de trabajo. Deben continuar fortaleciendo su nivel de madurez en los modelos de ciberseguridad, convirtiendo al 2021 en un año muy activo para el área TI"[15].

---

[14] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.28.

[15] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Ciberseguridad en entornos cotidianos, estudio del cibercrimen 2020. [sitio web]. Bogotá: Wework. Diciembre 2020. [Consultado: 31 de julio de 2021]. Disponible en: https://www.ccit.org.co/estudios/ciberseguridad-en-entornos-cotidianos-estudio-del-cibercrimen-2020/

“Los ciberdelitos presentados durante el 2020 llegaron a más de 45000 casos, un incremento del 89% frente al año anterior, convirtiéndose en el año de mayor ascenso en cifras e impacto en Colombia. Durante el período denominado COVID (marzo-diciembre 2020), se presentó un incremento del 101%, con más de 37000 reportes, en el número de noticias criminales instauradas ante la Fiscalía-General de la Nación”[16].

Para mitigar, controlar y reducir estos ciberdelitos, es necesario generar medidas de seguridad informática que prevengan los riesgos, permitiendo a las empresas ser competitivas y confiables, evitando que se conviertan en posibles blancos de ataques.

“Las organizaciones deben ejercitar debida diligencia en la gestión de riesgos de privacidad y seguridad de la información. Esto se logra, en parte, mediante el establecimiento de un programa integral de gestión de riesgos que utiliza la flexibilidad inherente a las publicaciones del NIST para categorizar sistemas, seleccionar e implementar controles de seguridad y privacidad que satisfagan la misión y las necesidades comerciales”[17].

Teniendo en cuenta lo anteriormente expuesto, es de carácter prioritario que la empresa G0 S.A.S, realice una evaluación de riesgos y establezca la implementación de controles de seguridad y privacidad, según el marco de trabajo NIST CFS, debido a que actualmente no cuenta con ningún sistema o aplicativo de seguridad de la información a nivel de activos para la gestión de riesgos, lo cual la hace vulnerable ante diversos riesgos informáticos, incidentes de fugas de información y la administración inadecuado de la misma, afectando la funcionalidad de la empresa.

1.2 FORMULACION DEL PROBLEMA

¿Qué controles de seguridad y privacidad debe implementar la empresa G0 SAS, para mitigar los riesgos y proteger los datos informáticos registrados en su infraestructura tecnológica?

[16] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. [sitio web]. Op.Cit.,
[17] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.8.

2. JUSTIFICACIÓN

El nuevo modelo de los negocios se establece bajo la estrategia informática, la cual por medio del internet incursiona en los mercados, enlazando los diferentes medios electrónicos con el cliente, y las empresas, estableciendo significativas oportunidades comerciales y de crecimiento económico organizacional, empleando los datos e información registrados en las estructuras tecnológicas empresariales.

> Del mismo modo que ha evolucionado la tecnología que utilizamos para desarrollar el trabajo en la empresa, lo ha hecho la ciberdelincuencia y los peligros a los que nos exponemos. Los ataques e intrusiones no se limitan ya a «curiosos» o a personas que buscaban superar retos personales introduciéndose en sistemas «ajenos», sino que ahora tienen una motivación principalmente económica, con grupos y mafias altamente organizadas y especializadas de ciberdelincuentes, con medios tecnológicos muy avanzados, que buscan el provecho económico. Los ciberdelincuentes atacan sistemas informáticos, extorsionan, realizan delitos de fraude y falsificación, etc. con el fin de obtener información valiosa de la que sacar partido económico. Aunque también tienen como objetivo tomar el control de otros sistemas para utilizarlos en ataques más sofisticados, (software *malware*).[18]

Este significativo avance tecnológico-empresarial, también presenta un alto nivel de vulnerabilidad, el cual radica en el riesgo informático que afrontan las empresas al manejar la información o los datos:

> El riesgo de ataques cibernéticos en infraestructura crítica y fraude o robo de datos ha sido siempre una prioridad para los líderes empresariales a nivel mundial. Según el Informe de Riesgos Globales 2020 del Foro Económico Mundial, el riesgo de ciberataques a la infraestructura crítica y el fraude o robo de datos se clasificaron entre los 10 principales riesgos con mayor probabilidad de ocurrir, mientras que la reciente Perspectiva de Riesgos del COVID-19 del Foro Económico Mundial identificó los ciberataques como la tercera mayor preocupación debido a nuestra actual y sostenida transición hacia los patrones de trabajo digital. Los datos disponibles respaldan estas preocupaciones; se estima que los daños por delitos cibernéticos alcanzarán los US$6 billones para 2021, lo que equivale al producto interno bruto (PIB) de la tercera economía más grande del mundo.[19]

---

[18] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Decálogo Ciberseguridad empresas: Una guía de aproximación para el empresario [en línea]. España.2017. 13 p. [Consultado: 31 de julio de 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

[19] BANCO INTERAMERICANO DE DESARROLLO. Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe [en línea]. Universidad de Oxford. 2020. 28-29 p. [Consultado: 31 de julio de 2021]. Disponible en: https://observatoriociberseguridad.org/#/home

En Colombia en el año 2020, según la Cámara Colombiana de Informática y Telecomunicaciones, se encontraron 3 delitos, que demuestran el alto crecimiento de la ciberdelincuencia, en plena etapa de expansión digital:

"El delito que mayores denuncias presentó fue la suplantación de sitios web para capturar datos personales con un crecimiento del 303% comparado con el 2019. Este delito tiene una relación directa con modalidades conocidas, tales como el phishing, *spoofing* y *pharming* que sufrieron las empresas. Adicionalmente, hubo 5.440 casos denunciados donde este tipo de ataques fue utilizado por los cibercriminales para capturar datos personales"[20].

"El segundo delito con mayor número de denuncias, con 9.487 casos registrados fue la violación de datos personales. Este presentó un crecimiento del 174% como consecuencia de la filtración y robo de datos, lo que generó un doble impacto que compromete aspectos operativos, así como legales y de cumplimiento por la pérdida de información sensible"[21].

"Seguido, se encuentra el hurto por medios informáticos con un 37% de crecimiento, registró más de 16.000 casos denunciados. Pese a tener la mayor frecuencia estadística, la modalidad más común sigue siendo el apoderamiento de credenciales para el acceso a servicios de banca online, con los cuales los cibercriminales, consiguen suplantar al titular del producto bancario y apoderarse del dinero generalmente dispuesto en cuentas bancarias"[22].

Todos los delitos cibernéticos ocurridos, muestran la alta viabilidad a la cual se encuentran expuestas todas las empresas diariamente al gestionar la operación informática y en mayor probabilidad las que no implementan marcos de seguridad. En este caso, la empresa G0 SAS no cuenta con un sistema de gestión de riesgo, lo que la deja vulnerable a cualquier ciberataque y por ende a un riesgo reputacional que le puede causar pérdidas económicas irrecuperables.

En las propuestas actuales y proyecciones en informática y de Inteligencia Artificial, es necesario la ciberseguridad convirtiéndose en una prioridad como empresa que se encuentra inmersa en un entorno tecnológico que presenta constantes cambios. Esta vulnerabilidad de riesgo conduce a establecer un análisis integral del entorno interno y externo que valide los aspectos técnicos, físicos, organizativos y legales. Esta afinidad que debe tener las empresas, al querer validar los sistemas de la información como un activo indispensable en cualquier proceso que lleve una empresa: desde marketing hasta logística, evoca la necesidad de que una empresa

[20] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. [sitio web]. Op.Cit.,
[21] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. [sitio web]. Op.Cit.,
[22] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. [sitio web]. Op.Cit.,

de tecnología como G0 SAS, cumpla los indicadores de seguridad mínimos que el entorno le exige y la necesidad que la supervivencia le obliga.

En esta área de la seguridad informática ante el crecimiento del cibercrimen y el alto nivel productivo que generan las TIC, para las organizaciones, se establecen metodologías o marcos de seguridad y gobernanza con estándares internacionales, desarrollados e implementados para reducir el riesgo informático en las infraestructuras tecnológicas:

> SP 800:30 (Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información), Es un estándar desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), fue formulado para la evaluación de riesgos de seguridad de la información especialmente a los sistemas de TI (Tecnología de la Información), proporciona un guía para la seguridad de las infraestructuras de la misma desde una perspectiva técnica. Por otro lado, esta guía provee fundamentos para la administración de riesgos, así como la evaluación y mitigación de los riesgos identificados dentro del sistema de TI con el objetivo de apoyar a las organizaciones con todo lo relacionado a Tecnología.[23]

> La Publicación Especial NIST 800-53, Revisión 5, responde a esta necesidad al embarcarse en un enfoque proactivo y sistémico para desarrollar y poner a disposición de una amplia base de organizaciones del sector público y privado un conjunto integral de medidas de protección de seguridad y privacidad para todos los tipos de computación. plataformas, incluidos los sistemas informáticos de propósito general, los sistemas ciberfísicos, los sistemas en la nube, los sistemas móviles, los sistemas de control industrial y los dispositivos de Internet de las cosas (IoT). Las medidas de protección incluyen controles de seguridad y privacidad para proteger las operaciones y los activos críticos y esenciales de las organizaciones y la privacidad de las personas.[24]

La presente propuesta busca establecer con la aplicación del marco de trabajo CSF NIST, los parámetros y las prácticas adecuadas de seguridad informática, para proteger los activos que conforman la estructura tecnológica de la empresa G0 SAS, reduciendo la vulnerabilidad y posicionándola como una organización reconocida por el manejo de altos niveles de seguridad informática, custodiando la reputación e integridad de los clientes y actualizando y adaptándose a los nuevos y exigentes modelos de negociación enmarcados en la funcionalidad y competitividad digital de sostenimiento y posicionamiento a nivel empresarial.

---

[23] TEJENA MACÍA, Mayra A. Análisis de riesgos en seguridad de la información. En: Polo del Conocimiento [en línea]. Abril 2018, vol.3, nro.4, p.233-244. [Consultado: 31 de julio de 2021]. DOI 1023857/pc. v3i4.809. Disponible en: http://polodelconocimiento.com/ojs/index.php/es. E-ISSN:2550-682X.

[24] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.11.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un prototipo de herramienta web basada en el marco de trabajo NIST, para la evaluación de los riesgos informáticos y la generación de controles de seguridad en la empresa G0 S.A.S.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar la evaluación de los riesgos informáticos según el marco de trabajo CSF NIST SP800-30, en la infraestructura tecnológica de G0 S.A.S.

- Proponer los controles a implementar con base en el análisis de riesgos de acuerdo con el marco de trabajo CSF NIST SP800-53, que permitan mejorar confidencialidad, integridad y disponibilidad de la información en la infraestructura tecnológica de G0 S.A.S.

- Definir la estructura del prototipo contemplando la interfaz gráfica, las posibles opciones de interacción y los posibles resultados a obtener.

- Presentar el diseño de un prototipo web que integre el marco de trabajo CSF NIST, para la seguridad informática de la infraestructura tecnológica de G0 S.A.S.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Marco del NIST CSF. “El Instituto Nacional de Estándares y Tecnología (NIST) ha confeccionado marco de trabajo para proporcionar orientación a las organizaciones dentro del sector de las infraestructuras críticas para reducir el riesgo asociado con la ciberseguridad. El marco se llama *NIST Cyber Security Framework for Critical Infrastructure* (NIST CSF).”[25]

“Actualmente cuenta con dos versiones, una lanzada en el 2014 y otra más reciente lanzada en el 2017. La implementación del NIST CSF necesita alinearse y complementarse con otros marcos existentes. El NIST afirma que el CSF no es un marco de madurez. Por lo tanto, es necesario adoptar un modelo de madurez existente o crear uno para tener una forma común de medir el progreso de la implementación del CSF.”[26]

“De acuerdo con el NIST: El marco de trabajo es una guía voluntaria, basada en estándares, directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen mejor y reduzcan el riesgo de ciberseguridad. Además, se diseñó para fomentar las comunicaciones de gestión del riesgo y la seguridad cibernética entre los interesados internos y externos de la organización.”[27]

“Es importante tener presente que el marco de trabajo no es un documento estático, sino que cada organización puede determinar con base en sus necesidades las actividades que considera prioritarias, permitiendo de esa forma un despliegue personalizado y paulatino. El CSF referencia a los siguientes estándares, directrices y mejores prácticas.”[28]

- COBIT 5
- *Council on CyberSecurity* (CCS)
- *Critical Security Controls* (CSC)
- ANSI/ISA-62443-2-1 (99.02.01)-2009
- ANSI/ISA-62443-3-3 (99.03.03)-2013

---

[25] XIII Seminario Iberoamericano de Seguridad en las Tecnologías de la Información) [en línea]. En:(17: 19-23, marzo 2018: La Habana, Cuba). Implementación del Marco de Trabajo para la Ciberseguridad NIST CSF desde la Perspectiva de Cobit 5. La Habana: GAE, 2018. 13 P. [Consultado: 2 de agosto de 2021]. Disponible en: https://scholar.google.com/scholar?hl=es&as_sdt=0%2C5&q=Implementaci%C3%B3n+del+Marco+de+Trabajo+para+la+Ciberseguridad+NIST+CSF+desde+la+Perspectiva+de+Cobit+5&btnG=

[26] Ibid.,

[27] Ibid.,

[28] Ibid.,

- ISO/IEC 27001:2013
- NIST SP 800-53 Rev. 5

4.1.1 Partes Principales del Marco NIST CSF. El marco se define en las siguientes partes: Núcleo del marco, Niveles de implementación, y Perfiles del marco, en donde a continuación se describe cada una de ellas.

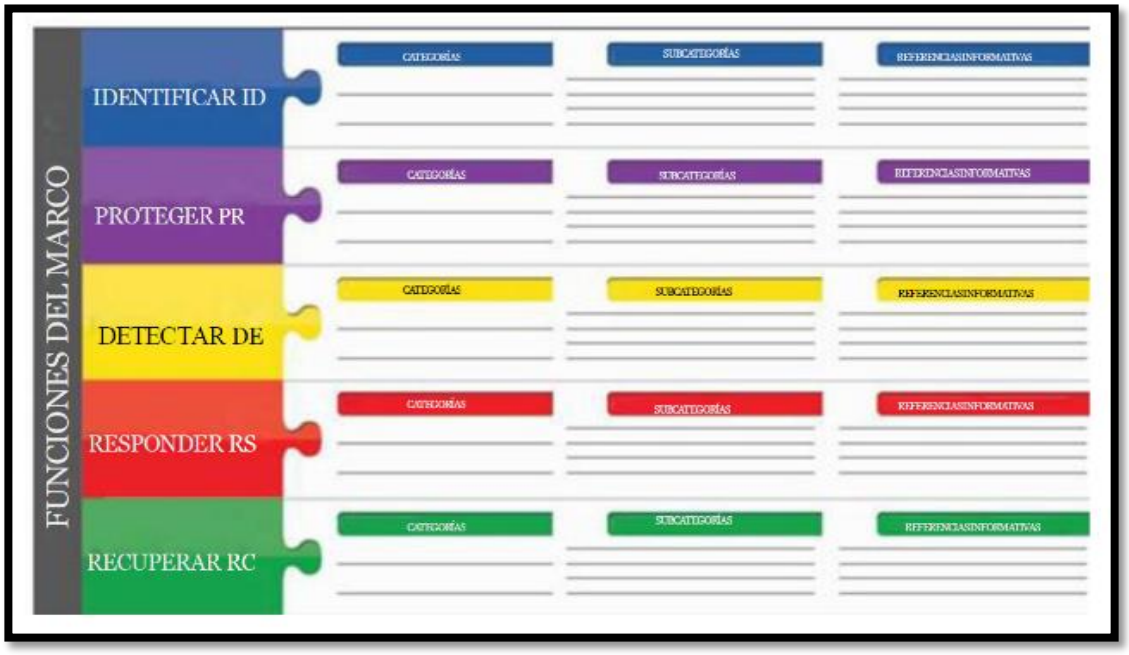
4.1.1.1 Núcleo del marco – marco básico (*framework core*). "El Núcleo del Marco proporciona un conjunto de actividades para lograr resultados específicos de seguridad cibernética y hace referencia a ejemplos de orientación en cómo lograr dichos resultados. El Núcleo no es una lista de verificación de las acciones a realizar. Este presenta los resultados clave de seguridad cibernética identificados por las partes interesadas como útiles para gestionar el riesgo de seguridad cibernética."[29]

"El Núcleo consta de cuatro elementos: Funciones, Categorías, Subcategorías y Referencias Informativas, las cuales conforman su estructura", en la figura 1, se muestra las funciones del marco.[30]

[29] XIII Seminario Iberoamericano de Seguridad en las Tecnologías de la Información) [en línea]. En:(17: 19-23, marzo 2018: La Habana, Cuba). Implementación del Marco de Trabajo para la Ciberseguridad NIST CSF desde la Perspectiva de Cobit 5. La Habana: GAE, 2018. 13 P. [Consultado: 2 de agosto de 2021]. Disponible en: https://scholar.google.com/scholar?hl=es&as_sdt=0%2C5&q=Implementaci%C3%B3n+del+Marco+de+Trabajo+para+la+Ciberseguridad+NIST+CSF+desde+la+Perspectiva+de+Cobit+5&btnG=

[30] Ibid.,

Figura 1. Estructura del núcleo del marco.



Fuente: https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf. p.6.

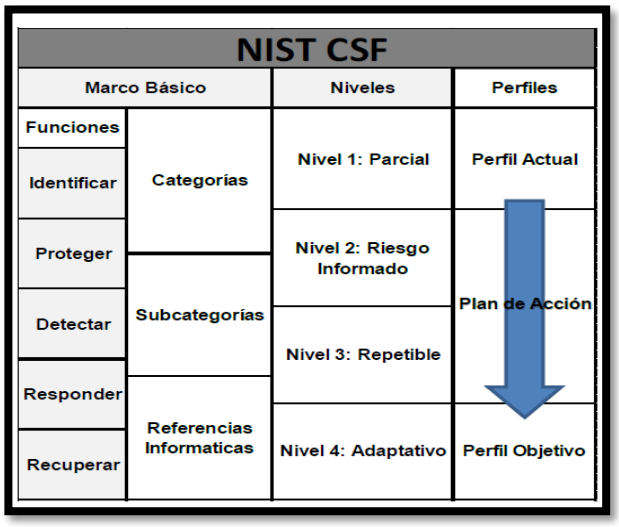
4.1.1.2 Niveles de implementación del marco (*Framework Implementation Tiers)*. "Los Niveles de Implementación del Marco ("Niveles") proporcionan un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo. Las definiciones de Nivel comprenden: Nivel 1: Parcial, Nivel 2: Riesgo informado, Nivel 3: Repetible y el Nivel 4: Adaptable, relacionados con el Proceso de gestión de riesgos, el Programa integrado de gestión de riesgos y la Participación externa."[31]

4.1.1.3 Perfiles del marco. "Es la alineación de las Funciones, Categorías y Subcategorías con los requisitos empresariales, la tolerancia al riesgo y los recursos de la organización. Un Perfil permite a las organizaciones establecer una hoja de ruta para reducir el riesgo de seguridad cibernética que está bien alineada con los objetivos organizacionales y sectoriales, considera los requisitos legales o reglamentarios y las mejores prácticas de la industria, y refleja las prioridades de gestión de riesgos."[32]

[31] INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. Op.Cit., p.15-18.
[32] INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. Op.Cit., p.18.

En la figura 2 se presenta la integración del núcleo o marco básico, los niveles y los perfiles para generar la arquitectura NIST CSF.

Figura 2. Niveles de implementación del NIST CFS.



Fuente: XIII Seminario Iberoamericano de Seguridad en las Tecnologías de la Información. Implementación del Marco de Trabajo para la Ciberseguridad NIST CSF desde la Perspectiva de Cobit 5. 2018. p.7.

4.2 NORMATIVIDAD

4.2.1 Marco NIST SP 800-30 para la Evaluación de Riesgos. "Proporciona orientación a las organizaciones sobre la identificación de factores de riesgo específicos para monitorear de manera continua, de modo que las organizaciones pueden determinar si los riesgos han aumentado a niveles inaceptables (es decir, superando la tolerancia al riesgo de la organización) y se deben tomar diferentes cursos de acción."[33]

"Los procesos de gestión de riesgos incluyen: Encuadrar el riesgo, Evaluar el riesgo, Respondedor al riesgo y Seguimiento del riesgo."[34]

[33] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.11.
[34] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.13.

4.2.1.1 Propósito del componente de evaluación de riesgos. “El propósito del componente de evaluación de riesgos es identificar en las organizaciones las amenazas, las vulnerabilidades internas y externas, el daño (es decir, el impacto adverso) que puede ocurrir dado el potencial de amenazas que explotan vulnerabilidades; y la probabilidad de que ocurra un daño. El resultado final es una determinación del riesgo (es decir, típicamente una función del grado de daño y la probabilidad de que ocurra).”[35]

4.2.1.2 Metodología de evaluación de riesgos. “Las metodologías de evaluación de riesgos son definidas por las organizaciones y son un componente de la estrategia de gestión de riesgos desarrollada durante la etapa de encuadre de riesgos del proceso de gestión de riesgos.”[36]

La metodología Incluye:

- Un proceso de evaluación de riesgos.
- Una explícita modelo de riesgo.
- Un enfoque de evaluación cuantitativo, cualitativo o semicualitativo.
- Un enfoque de análisis orientado amenazas, activos / impacto u orientado a vulnerabilidad).”[37]

4.2.1.3 Proceso para la evaluación del riesgo. “El proceso se centra en el componente de evaluación de riesgos de la gestión de riesgos, y un proceso paso a paso para las organizaciones sobre cómo:

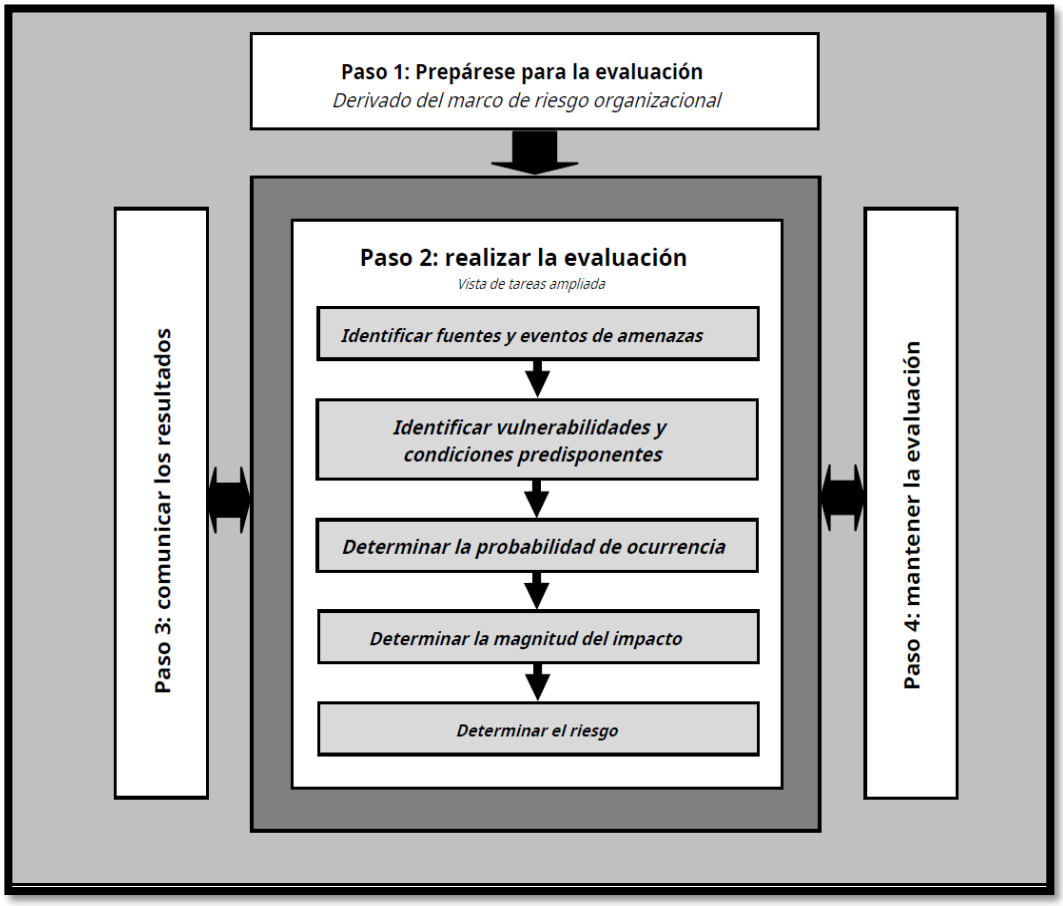
- Prepararse para las evaluaciones de riesgos.
- Realizar evaluaciones de riesgo.
- Comunicar los resultados de la evaluación de riesgos al clave personal.
- Mantener las evaluaciones de riesgos a lo largo del tiempo.”[38]

En la figura 3 se muestra el proceso para realizar la evaluación de riesgos basado en el marco NIST 800-30.

---

[35] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.14.
[36] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.16.
[37] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.14-16.
[38] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.14.

Figura 3. Proceso para la evaluación del riesgo.



Fuente: *NIST U.S. DEPARTMENT OF COMMERCE*. Publicación Especial del NIST 800-30.

4.2.1.4 Factores de riesgos. "Los factores de riesgo son características que se utilizan en los modelos de riesgo como entradas para determinar los niveles de riesgo en las evaluaciones de riesgo. Los factores de riesgo típicos incluyen amenaza, vulnerabilidad, impacto, probabilidad y condición predisponente."[39]

- **Amenaza**: "Los tipos de fuentes de amenazas incluyen: (i) ataques físicos o cibernéticos hostiles; (ii) errores humanos de omisión o comisión; (iii) fallas estructurales de los recursos controlados por la organización (por ejemplo, *hardware*, software, controles ambientales); y (iv) desastres naturales y provocados por el hombre, accidentes y fallas fuera del control de la organización."[40]

[39] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.17.
[40] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.17.

- **Vulnerabilidad**: “La mayoría de las vulnerabilidades del sistema de información pueden estar asociadas con controles de seguridad que no se han aplicado, o que se han aplicado, pero conservan alguna debilidad. Existe la posibilidad de vulnerabilidades emergentes que pueden surgir naturalmente con el tiempo a medida que evolucionan las misiones organizacionales / funciones comerciales, los entornos de operación cambian, las nuevas tecnologías proliferan y surgen nuevas amenazas.”[41]

- **Condición Predisponente**: “Es una condición que existe dentro de una organización, una misión o proceso comercial, arquitectura empresarial, sistema de información o entorno de operación, que afecta (es decir, aumenta o disminuye) la probabilidad de que los eventos de amenaza, una vez iniciados, tengan como resultado impactos adversos en la organización.”[42]

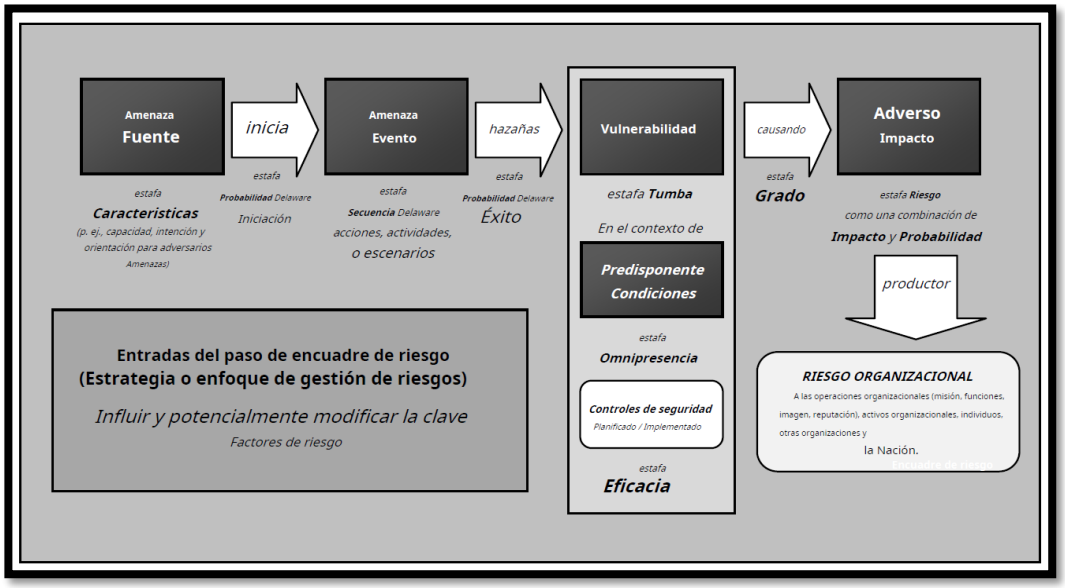
- **Probabilidad**: “Para las amenazas adversas, una evaluación de la probabilidad de ocurrencia se basa típicamente en: (i) adversario intención; (ii) adversario capacidad; y (iii) adversario focalización.”[43]

- **Impacto**: “El nivel de impacto de un evento de amenaza es la magnitud del daño que se puede esperar que resulte de las consecuencias de la divulgación, la modificación, la destrucción no autorizada de información, o la pérdida de información o la disponibilidad del sistema de información.”[44]

En la figura 4 se muestra la estrategia del modelo de gestión de riesgos.

[41] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.18.
[42] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.19.
[43] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.19.
[44] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.20.

Figura 4. Modelo de riesgo con factores claves.



Fuente: *NIST U.S. DEPARTMENT OF COMMERCE*. Publicación Especial del NIST 800-30. p.21.

4.2.1.5 Aplicación de la evaluación de riesgos. “Las evaluaciones de riesgos se pueden realizar en los tres niveles de la jerarquía de gestión de riesgos: nivel 1 de organización, misión / nivel 2 de proceso empresarial, y nivel 3 del sistema de información. Las evaluaciones de riesgo tradicional generalmente se enfocan en el nivel de Nivel 3.”[45]

"Las evaluaciones de riesgo del nivel 3, implementan 6 pasos: categorizar, seleccionar, implementar, evaluación, autorizar y supervisión.”[46]

4.2.2 Marco NIST SP 800-53 para la Implementación de Controles de Seguridad y Privacidad. “Los controles de seguridad y privacidad se seleccionan e implementan para satisfacer los requisitos de seguridad y privacidad impuestos a un sistema u organización.”[47]

“Los requisitos de seguridad y privacidad se derivan de las leyes, órdenes ejecutivas, directivas, regulaciones, políticas, estándares y necesidades de la misión aplicables para garantizar la confidencialidad, integridad y disponibilidad de

[45] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.26.
[46] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.29-30.
[47] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.28.

la información procesada, almacenada o transmitida y para administrar los riesgos a la privacidad individual."[48]

"Los criterios de selección de control pueden ser guiados e informados por muchos factores, incluidas la misión y las necesidades comerciales, las necesidades de protección de las partes interesadas, las amenazas, las vulnerabilidades y los requisitos para cumplir con las leyes federales, órdenes ejecutivas, directivas, regulaciones, políticas, estándares y pautas."[49]

4.2.2.1 Requisitos. "Las organizaciones pueden dividir los requisitos de seguridad y privacidad en categorías más granulares, según dónde se empleen los requisitos en el ciclo de vida de desarrollo del sistema (SDLC) y con qué propósito."[50]

"Las organizaciones pueden usar el término requisito como capacidad, especificación, (pertenecen a componentes particulares de *hardware*, software y firmware) y de trabajo."[51]

"Los controles son seleccionados e implementados por la organización para satisfacer los requisitos del sistema y pueden incluir aspectos administrativos, técnicos y físicos. También pueden requerir especificaciones adicionales en forma de requisitos derivados. Los requisitos derivados y los valores de los parámetros de control pueden ser necesarios para proporcionar el nivel apropiado de detalle de implementación para controles particulares dentro del SDLC."[52]

4.2.2.2 Estructura. En este estándar se utiliza una clasificación de controles de seguridad, los cuales se organizan en 20 familias. Cada familia contiene controles relacionados con el tema específico de la familia, las cuales se muestra con un identificador de dos caracteres y están conformadas por tres clases: Administrativo, operacional y técnico. A continuación, se clasifica las familias de controles y su identificador asociado.

En la Tabla 1 se muestra la clasificación de controles de seguridad basados en la NIST SP 800-53.

[48] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.28.
[49] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.30.
[50] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.34.
[51] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.34.
[52] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.35.

Tabla 1. Identificadores, familias y clases de control.

ID	Familia	Clase	Subcategorías
AC	Control de Acceso	Técnico	25
AT	Concientización y entrenamiento	Operacional	6
AU	Auditoria y responsabilidad	Técnico	16
CA	Evaluación, Autorización y Monitoreo	Administración	9
CM	Administración de Configuraciones	Operacional	14
CP	Planificación de Contingencia	Operacional	13
IA	Identificación y Autenticación	Técnico	12
IR	Respuesta a Incidentes	Operacional	10
MA	Mantenimiento	Operacional	7
MP	Protección de Medios	Operacional	8
PE	Protección física y de entorno	Operacional	23
PL	Planeación	Administración	11
PM	Administración del Programa	Administración	32
PS	Seguridad en el Personal	Operacional	9
PT	Transparencia y Procesamiento de PII	Operacional	8
RA	Evaluación de Riesgos	Administración	10
SA	Adquisición de sistemas y servicios	Administración	23
SC	Protección de sistemas y Comunicaciones	Técnico	51
SI	Sistema e Integridad de la Información	Operacional	23
SR	Gestión de Riesgos de la cadena de suministro	Operacional	12

Fuente: *NIST U.S. DEPARTMENT OF COMMERCE*. Publicación Especial del NIST 800-53. p.35.

“Las familias de controles contienen controles básicos y mejoras de control, que están directamente relacionados con sus controles básicos. Las mejoras de control agregan funcionalidad o especificidad a un control base o aumentan la fuerza de un control base. Las mejoras de control se utilizan en sistemas y entornos de operación que requieren mayor protección que la protección proporcionada por el control base.”[53].

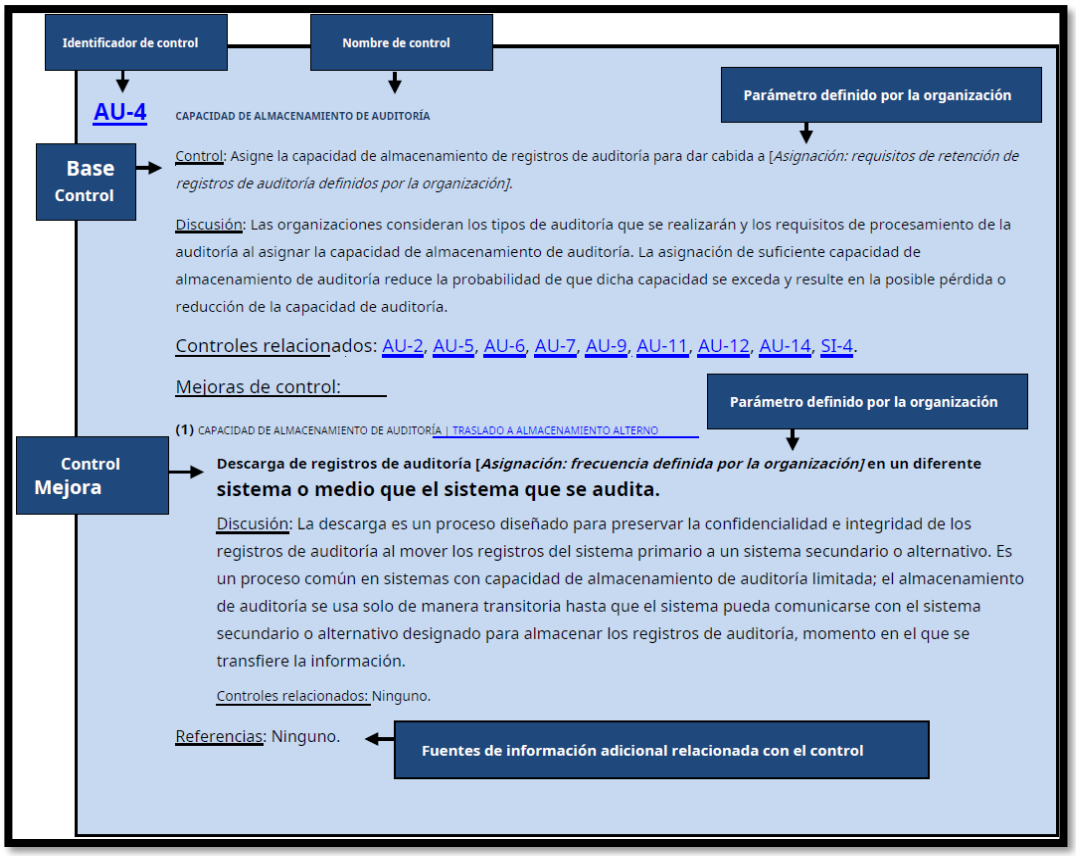
“Las familias están ordenadas alfabéticamente, mientras que los controles y las mejoras de control dentro de cada familia están en orden numérico. El orden de las familias, los controles y las mejoras de control nono Implica cualquier progresión lógica, nivel de priorización o importancia, u orden en el que se implementarán los

[53] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.35.

controles o las mejoras de control. Más bien, refleja el orden en que se incluyeron en el catálogo."[54]

En la figura 5 se muestra la estructura de controles de seguridad basados en la NIST SP 800-53.

Figura 5. Estructura de los controles de seguridad y privacidad.



Fuente: *NIST U.S. DEPARTMENT OF COMMERCE*. Publicación Especial del NIST 800-53. p.36.

La sección proporciona:

- Control: prescribe una capacidad de seguridad o privacidad que debe implementarse.
- Discusión: información adicional sobre un control.

[54] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.36.

- Controles Relacionados: proporciona una lista de controles del catálogo de controles que impactan o apoyan la implementación de un control particular.

- Mejoras de Control: proporciona declaraciones de seguridad y capacidad de privacidad que aumentan un control básico.

- Referencias: incluye una lista de leyes, políticas, estándares, pautas, sitios web y otras referencias útiles que son relevantes para un control específico o una mejora de control."[55]

4.2.2.3 Enfoques. "Hay tres enfoques para implementar los controles: (1) un común enfoque de implementación de control (heredable), (2) un específico del sistema enfoque de implementación de control, y (3) un híbrido enfoque de implementación de control."[56]

"Los enfoques de implementación del control definen el alcance de aplicabilidad del control, la naturaleza compartida o heredabilidad del control y la responsabilidad del desarrollo, implementación, evaluación y control del control."[57]

4.2.2.4 Catálogo de controles. "Este catálogo de controles de seguridad y privacidad proporciona medidas de protección para sistemas, organizaciones e individuos. Los controles están diseñados para facilitar la gestión de riesgos y el cumplimiento de las leyes, órdenes ejecutivas, directivas, regulaciones, políticas y estándares federales aplicables."[58]

"Los controles de seguridad y privacidad del catálogo son neutrales en cuanto a políticas, tecnologías y sectores, lo que significa que los controles se centran en las medidas fundamentales necesarias para proteger la información y la privacidad de las personas a lo largo del ciclo de vida de la información."[59]

[55] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.36-38.
[56] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.38.
[57] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.38.
[58] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.43.
[59] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53. Op.Cit., p.43.

4.3 HERRAMIENTAS EQUIVALENTES EN EL MERCADO

Se realiza una búsqueda de herramientas disponibles en el mercado con opción gratuita y que sus funcionalidades cumplieran con el objetivo de evaluar los riesgos. Adicionalmente a esto, que su resultado final fueran controles que permitieran realizar posteriormente el tratamiento de los riesgos en G0 S.A.S. Como resultado de la búsqueda se encuentran las siguientes opciones:

4.3.1 Topia. Es una plataforma de gestión de riesgos que analiza todo el ecosistema de aplicaciones/sistema operativo de una organización para identificar y mapear cada riesgo según la prioridad. Con la capacidad de realizar un seguimiento de las interacciones entre una aplicación y el sistema operativo, TOPIA mitiga el riesgo antes de que se pueda transformar en una amenaza para la integridad de la organización. Una plataforma de gestión de riesgos que permite a las organizaciones gestionar el riesgo en todo el entorno único de aplicaciones y sistemas operativos.[60]

4.3.2 *AuditComply*. Es una plataforma de gestión de riesgos empresariales basada en SaaS. Así mismo, es integral y flexible lo que le permite a las organizaciones implementar metodologías de evaluación complejas y sólidas, tanto a través de aplicaciones de escritorio como móviles. Además, proporciona una comprensión precisa de los riesgos en toda la organización y una visibilidad clara del perfil de riesgo de una organización. Utilizando estos datos, para mitigar el riesgo, impulsar el cumplimiento, mejorar la calidad y el rendimiento energético, todo desde un sistema centralizado.[61]

4.3.3 *GlobalSuit*. *Information Security*, Esta plataforma facilita la automatización y gestión de la norma ISO 27001 para optimizar un Sistema de Seguridad de la Información (SGSI). Es el software para la implantación, gestión y mantenimiento de Sistemas de Gestión de Seguridad de la Información basados en la norma ISO 27001. La versatilidad del software hace que cumpla con los requerimientos más complejos de una forma asequible e intuitiva, ofrece las siguientes funcionalidades: Identificación de Riesgos, Gestión de Riesgos, Análisis de Riesgos, Evaluación de

[60] TOPIA. Capterra [en línea], [sin fecha]. [Consulta: 25 noviembre 2021]. Disponible en: https://www.capterra.co/software/201047/topia.
[61] AuditComply. *Capterra* [en línea], [sin fecha]. [Consulta: 25 noviembre 2021]. Disponible en: https://www.capterra.co/software/171748/auditcomply.

Riesgos, Procesos SGSI, Planes de Continuidad, Capacidad y Capacitación, Integración con *Power BI*, Gestor Documental y Cuadro de mando.[62]

Luego de validar las funcionalidades de las herramientas encontradas en la web, y confrontando la entrega de resultados de estas frente al prototipo propuesto en este documento, se encontraron varias limitantes: entre estas, que las herramientas encontradas ofrecen varias funcionalidades que desbordan las necesidades de G0 S.A.S. De igual manera, al ser gratuitas, muchas veces no entregan los controles o las funcionalidades que la empresa debe implementar; por otra parte, las herramientas licenciadas ofrecen muchas funcionalidades, que si bien se adaptan a las necesidades que G0 S.A.S necesita, el pago de la licencia hace que no sea rentable para la organización, a diferencia del prototipo propuesto, el cual se alinea a los procesos de la empresa sin ofrecer funcionalidades innecesarias y entregando como resultado final los controles que G0 S.A.S necesita implementar.

4.4 MODELO WEB BASADO EN PROTOTIPO

En este prototipo presentado, se pretende suplir las necesidades básicas de Ciberseguridad que tiene actualmente G0 S.A.S para evaluar los riesgos identificados y proponer controles que se acerquen más a sus necesidades para su respectiva mitigación. Es importante tener en cuenta que la propuesta de los controles y funcionalidades de la herramienta no se sobredimensionen.

El prototipo presentado a continuación se basó en el ciclo de vida y desarrollo de software, en la cual se encuentran varias técnicas que permiten entender mejor las necesidades del cliente. Entre estas se encuentran los *wireframes* que son un esbozo, los *MockUps* que muestran la sensación y la textura del diseño y los prototipos, los cuales proporcionan vida a la experiencia del usuario.

“Un prototipo es un modelo experimental de un sistema o de un componente de un sistema que tiene los suficientes elementos que permiten su uso.”[63]

“Los prototipos están conformados por tres enfoques de desarrollo: Desechable, Evolutivo y Mixto.”[64]

---

[62] Seguridad de la información ISO 27001. GlobalSUITESolutions [en línea], [sin fecha]. [Consulta: 26 noviembre 2021]. Disponible en: https://www.globalsuitesolutions.com/co/seguridad-informacion-iso-27001/.

[63] Universidad de Salamanca Departamento de Informática y Automática: Ingeniería de Software I [en línea]. 2020. 17 p. [Consultado: 29 de julio de 2021]. Disponible en: https://repositorio.grial.eu/bitstream/grial/1940/1/IS_I%20Tema%203%20-%20Modelos%20de%20Proceso.pdf

[64] Ibid., p.18

4.4.1 Generalidades del modelo. “El prototipo es una versión rudimentaria del sistema que posteriormente es desechada.”[65]

Características:

- “Se desarrolla código para explorar factores críticos para el éxito del sistema.”[66]
- “La implementación usa lenguajes y/o métodos de desarrollo más rápidos que los definitivos.”[67]
- “Se usa como herramienta auxiliar de la especificación de requisitos y el diseño.”[68]
- “Este enfoque suele derivar en un modelo lineal una vez que el prototipo ha cumplido su misión.”[69]

[65] Ibid., p.18
[66] Ibid., p.19
[67] Ibid., p.19
[68] Ibid., p.19
[69] Ibid., p.19

4.5 G0 S.A.S

4.5.1 Generalidades de la empresa. “La empresa G0 S.A.S fue creada en el año 2014 y desde su fundación, ha contado con profesionales de gran experiencia para brindar a sus clientes soluciones tecnológicas de alta calidad que incrementan su productividad mediante la construcción de productos a la medida.”[70]

La empresa G0 S.A.S pertenece al sector TI, y se encuentra ubicada en Chía, Cundinamarca, con una trayectoria de 7 años en el mercado, está dedicada actividades de desarrollo de software y soluciones integrales con productos de auto gestión. De igual forma, aplican modelos de investigación que automatizan los diferentes proyectos.[71]

“La empresa G0 S.A.S presenta como pilar la actualización tecnológica constante, aplicando modelos de investigación formales de la mano de las instituciones educativas, investigando, creando y difundiendo, impregnando a la humanidad de la necesidad de automatizar todas las tareas que consumen y desgastan la vida al brindar herramientas altamente tecnológicas para obtener más valor por su tiempo.”[72]

Misión: “Nuestra razón de ser es brindar soluciones de sistemas de información e infraestructuras tecnológicas, en las fases de: planificación, análisis, diseño, programación y pruebas, haciendo uso de tecnologías innovadoras y de calidad, para proponer y ejecutar en nuestros clientes soluciones a la medida, estableciendo la fiabilidad, seguridad, veracidad, disponibilidad y oportunidad de los datos.”[73]

“Así mismo nuestros productos y servicios se implementan bajo la premisa de compartir esfuerzo, favoreciendo el ahorro y la optimización de los costos y la sostenibilidad de los sistemas establecidos, en alineación con las exigencias del mercado y el cuidado del planeta.”[74]

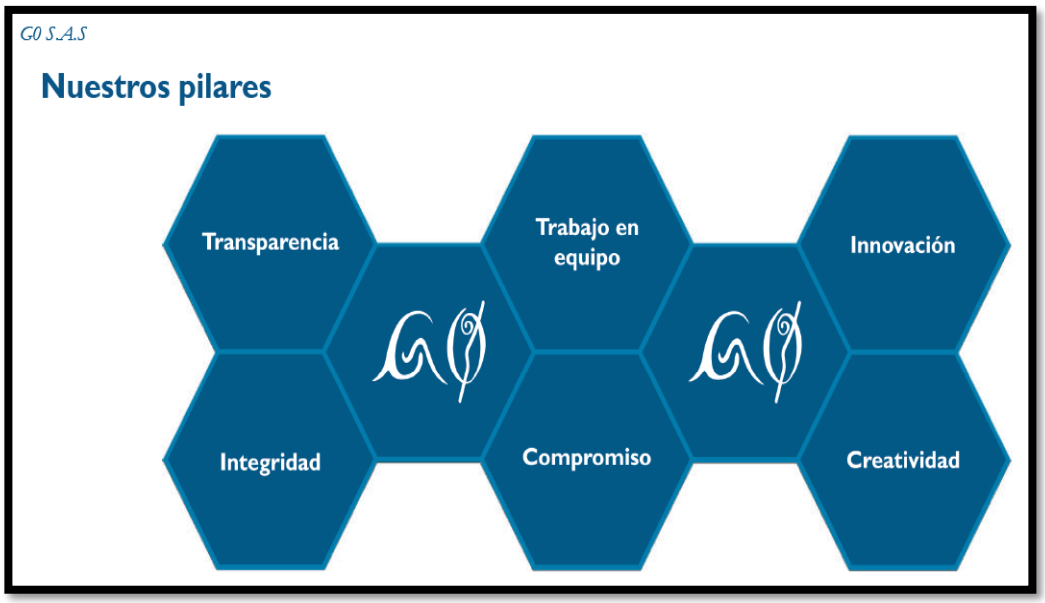
Visión: “G0 S.A.S. se proyecta en el 2025 como una compañía líder, pionera y posicionada en el sector de tecnologías de la información a nivel global, utilizando los más altos estándares de desarrollo de software y de Investigación para la implementación de nuevas tecnologías, siendo un generador en el avance de la ciencia para el campo de la informática y la Inteligencia Artificial.”[75]

---

[70] G0 S.A.S. [en línea]. [Consulta: 18 agosto 2021]. Disponible en: https://g0tech.com/es.
[71] Ibid.
[72] Ibid.
[73] Ibid.
[74] G0 S.A.S. Op.Cit.
[75] G0 S.A.S. Op.Cit.

En la figura 6 se representan los Pilares Organizacionales. de la empresa *G0 S.A.S.*

Figura 6. Pilares organizacionales G0 S.A.S.

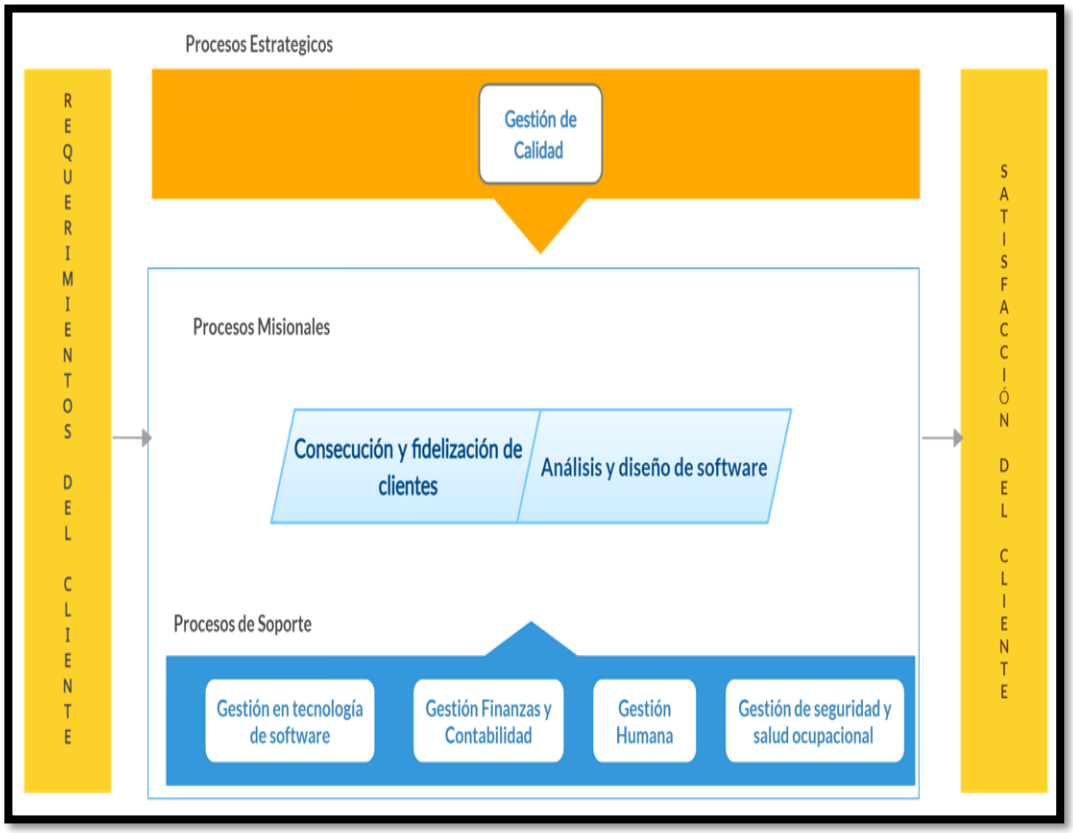


Fuente: G0 S.A.S. Disponible en: https://g0tech.com/es.

4.5.2 Estructura De Procesos G0 S.A.S. Los procesos con los que cuenta G0 S.A.S, se encuentran implementados como la base estructural para alcanzar los principios de calidad y operar con el fin de garantizar la satisfacción de sus clientes.

En la figura 7 se muestra el mapa de procesos establecidos en la empresa G0 S.A.S.

Figura 7. Mapa de procesos de la empresa G0 S.A.S.



Fuente: G0 S.A.S. adaptado por Autores de la Investigación.

Cada proceso constituye un conjunto de actividades y los diferentes procedimientos que intervienen para desarrollar el proceso, generando los resultados que se establecen en las salidas del sistema.

Procesos Estratégicos: Permiten a G0 S.A.S, definir los mecanismos y directrices con base a los objetivos y lineamientos corporativos garantizando el cumplimiento y seguimiento de su labor.

- Gestión de Calidad.

Procesos Misionales: Permiten a G0 S.A.S, centrar la mayoría de los servicios que la empresa presta a los usuarios y apoya la misión de la entidad.

- Consecución y fidelización de clientes.
- Análisis y diseño de software.
- Proceso Comercial.

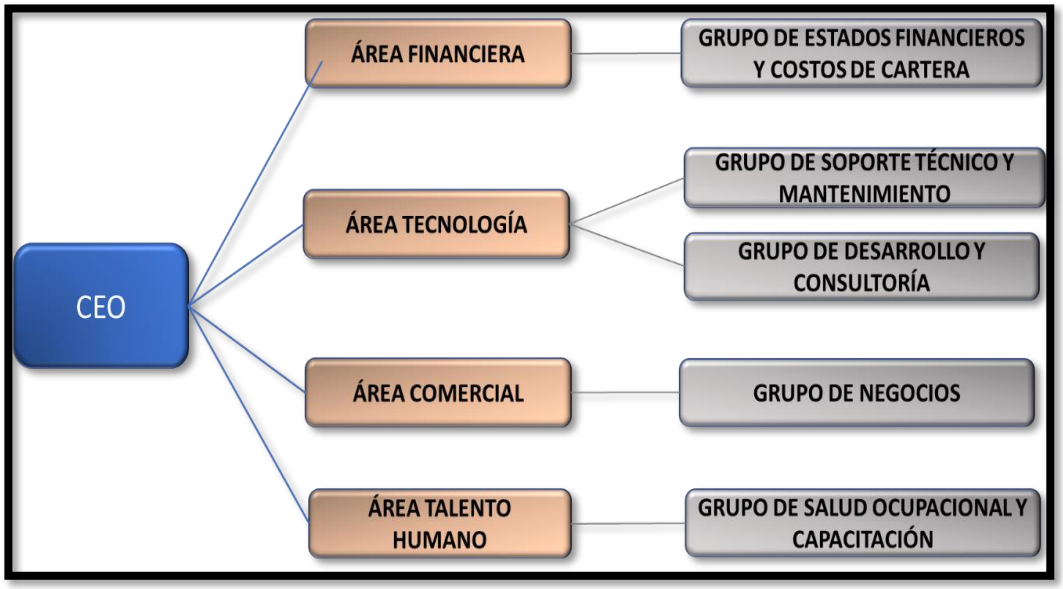
- Proceso de análisis y diseño.

Procesos de Soporte: Permiten a G0 S.A.S, el desarrollo de los procesos estratégicos y misionales brindando los recursos necesarios para su operatividad.

- Gestión de finanzas y contabilidad.
- Gestión en tecnología de software.
- Gestión humana.
- Gestión de seguridad y salud ocupacional.

En la figura 8 se muestra la Estructura Organizacional de la empresa G0 S.A.S.

Figura 8. Estructura organizacional GO S.A.S.



Fuente: G0 S.A.S. adaptado por Autores de la Investigación.

4.5.3 Servicios: Desarrollo de Software a la Medida. Ofrecen una unidad de negocio enfocada a prestar servicios en *hardware* para soporte, mantenimiento, montaje de redes y actualización de infraestructura.

En su portafolio de servicios, G0 S.A.S cuenta con alta experiencia, cumpliendo los más altos estándares de calidad en el desarrollo de software que mejoran la productividad organizacional de sus clientes con productos y servicios hechos a la medida: WEB, móvil, de escritorio o en infraestructura de redes.

“Crecimiento y mejora de procesos dentro de las organizaciones basados en la creatividad y la innovación con prácticas seguras y fácil usabilidad. Nuestros servicios y productos: infraestructura web, móvil, de escritorio o de red se basan en las mejores prácticas de TI (ITIL).”[76]

a) Desarrollo Web

- .NET.
- PHP.
- DRUPAL.
- HTML, Java Script, Css.

b) Desarrollo Móvil

- Angular.
- Lonic.

c) Desarrollos Especiales

- Phyton.
- C++.
- Desarrollos de escritorio.

d) Consultoría de Base de Datos

- SQL Server.
- MySQL.
- PostgreSQL.
- MongDB.

e) Inteligencia de Negocios

- ETL.
- Cognos.
- Reporting.
- Microsoft SSIS.
- IBM- Informatic Power Center.

f) Investigación para la implementación de nuevas Tecnologías

- Inteligencia artificial.
- Minería de datos.

[76] G0 S.A.S. Op.Cit.

- Automatización de procesos (RPA)
- Chat bots.
- Visión artificial.
- Diseño de videojuegos.
- Realidad Aumentada.

g) Implementación de soluciones apoyados CMS y LMS

- Drupal.
- Joomla.
- Moodle.

h) Infraestructura, Redes y Seguridad Informática

- Diseño, implementación, administración y mantenimiento en redes LAN, WLAN, WAN y seguridad informática.
- Adaptación de protocolo IPv4 a IPv6.

4.5.4 Clientes. G0 S.A.S le presta servicios de desarrollo de software y soporte a los siguientes clientes.

- "CORFERIAS (Corporación de Ferias y Exposiciones SA).
- CANAL CAPITAL.
- FINAGRO (Fondo para el Financiamiento del Sector Agropecuario).
- EMSERCHIA (Empresa se Servicios Públicos de Chía).
- CE&S (Consultoría Especializada y Servicios de Ingeniería).
- VASS (Consultoría de Sistemas de Colombia)."[77]

4.6 MARCO LEGAL

El marco legal será analizado según los conceptos legales que enmarcan el funcionamiento de las TIC, en el área comercial de las empresas.

4.6.1 Protección de la Información y de los Datos. "La Ley 1273 del 5 enero de 2009, adiciona al código penal, implementando un nuevo orden jurídico para la protección de la información y de los datos."[78]

[77] G0 S.A.S. Op.Cit.

[78] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). Por 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 [en línea]. En: Diario Oficial. Bogotá, 2009. 47223. p. 1-3.

En la tabla 2 se describen los artículos relacionados con la protección de datos y delitos informáticos.

Tabla 2. Ley 1273 de 2009 delitos informáticos.

Artículo	Descripción
269A	Acceso abusivo a un sistema informático
269B	Obstaculización ilegítima de sistema informático o red de telecomunicación
269C	Interceptación de datos informáticos.
269D	Daño informático
269E	Uso de software malicioso
269F	Violación de datos personales
269G	Suplantación de sitios web para capturar datos personales
269I	Hurto por medios informáticos y semejantes

Fuente: COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). p. 1-3.

4.6.2 Protección de Datos Personales. "La Ley estatutaria 1581 de 2012 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."[79]

4.6.3 Disposiciones Generales del Hábeas Data. "La Ley 1266 del 2008, la cual 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 bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política. Artículos 3, 4, 5 y 6."[80]

[Consultado: 11 de agosto de 2021]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[79] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales [en línea]. En: Diario Oficial. Bogotá, 2012. 48587. p.1_8 [Consultado: 12 de julio de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

[80] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones [en línea]. En: Diario Oficial. Bogotá,

4.6.4 Recolección, Tratamiento y Circulación de Datos. En la Constitución Política de la República de Colombia en los artículos 15 y 16, se mencionan las regulaciones para el tratamiento de datos y el uso de los medios de comunicación.

ARTÍCULO 15: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas."[81]

ARTICULO 20: "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación."[82]

4.6.5 Uso Mensajes de Datos. La Ley 527 de 1999, reglamenta el uso de los mensajes de datos, y expone en detalle la aplicabilidad y definición de los conceptos. A continuación, se nombran los artículos que establecen el tratamiento de los datos:

- ARTÍCULO 1º. "Ámbito de aplicación."[83]
- ARTÍCULO 2º. "Definiciones (Mensaje de datos, Comercio electrónico, Firma digital, Entidad de Certificación, Intercambio Electrónico de Datos (EDI), Sistema de Información)."[84]
- ARTÍCULO 3º. "Interpretación."[85]
- ARTÍCULO 4º. "Modificación mediante acuerdo."[86]

2008. 47219. p.1_10. [Consultado: 15 de agosto de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[81] COLOMBIA, Constitución Política de la República de Colombia. (20, julio, 1991). Por la cual se decreta, sanciona y promulga la Constitución Política de Colombia [en línea]. En: Gaceta Constitucional. 1991. 116. p.4 [Consultado: 16 de agosto de 2021]. Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

[82] Ibid., p.5.

[83] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 527 (18, agosto, 1999). Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [en línea]. En: Diario Oficial. Bogotá, 1999. 43673. p.1_2. [Consultado: 16 de agosto de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=4276

[84] Ibid.,

[85] Ibid.,

[86] Ibid.,

- ARTÍCULO 5º. “Reconocimiento jurídico de los mensajes de datos.”[87]

4.6.6 Competencia Desleal. La ley 256 de 1996, dicta las normas sobre competencia desleal y en el artículo 16 establece la aplicabilidad del ámbito desleal a nivel comercial.

ARTÍCULO 16. VIOLACIÓN DE SECRETOS: “Se considera desleal la divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquiera otra clase de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de algunas de las conductas previstas en el inciso siguiente o en el artículo 18 de esta Ley.”[88]

“Tendrá así mismo la consideración de desleal, la adquisición de secretos por medio de espionaje o procedimientos análogos, sin perjuicio de las sanciones que otras normas establezcan. Las acciones referentes a la violación de secretos procederán sin que para ello sea preciso que concurran los requisitos a que hace referencia el artículo 2o. de este Ley.”[89]

[87] Ibid.,

[88] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 256 (18, enero, 1996). Por la cual se dictan normas sobre competencia desleal [en línea]. En: Diario Oficial. Bogotá, 1996. 42692. p.3. [Consultado: 17 de agosto de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0256_1996.html

[89] Ibid.,

5. DISEÑO METODOLÓGICO

5.1 ENFOQUE DE LA INVESTIGACIÓN: CUANTITATIVO

El enfoque cuantitativo para el análisis de riesgos informáticos según el marco de trabajo CSF NIST 800-30, en la infraestructura tecnológica de G0 S.A.S, se desarrolla con base en datos estadísticos, interpretación de causa y efecto, en un proceso de análisis objetivo de la situación actual de la empresa en su área de seguridad informática, respecto a la operación que realiza en el desarrollo del objeto social. Este enfoque busca medir la realidad investigada, empleando técnicas de recolección de la información estandarizadas, para la generación de resultados.

5.2 TIPO DE INVESTIGACIÓN: DESCRIPTIVA

La investigación descriptiva identifica los principales elementos o factores de riesgo existentes en G0 S.A.S, así como las vulnerabilidades y amenazas, que conforman el problema de investigación. También, genera descripciones de cada uno de los servicios que presta la empresa y sus respectivas características, para determinar el grado de riesgo que se presenta al ofertar el portafolio de servicios tecnológicos.

Este diseño metodológico construye el conocimiento, al realizar la descripción del Marco de Trabajo NIST CSF, implementado por las organizaciones para evaluar el riesgo y generar los respectivos controles de seguridad y privacidad. Así mismo, presenta las características técnicas, funcionalidades, aplicaciones, ventajas y enfoques, direccionando a la empresa G0 S.A.S, en la generación de prácticas de seguridad por medio de una gestión tecnológica en los procesos desarrollados.

Otro factor esencial que describe la investigación, es la identificación de las áreas funcionales y los colaboradores con su respectiva gestión del riesgo que realizan y los conocimientos e información que administran acerca de la seguridad informática. Asimismo, el proceso de análisis contribuye al conocimiento de cada cliente que asiste la empresa, el grado y nivel de información registrada, almacenada y administrada en la infraestructura tecnológica de G0 S.A.S y las herramientas de respaldo y soporte de datos.

Finalmente, la aplicación de la metodología descriptiva basada en el análisis del riesgo y la observación directa en las áreas de trabajo de la empresa, permiten extraer conceptos confeccionados en el marco de trabajo NIST CFS, generando resultados que contribuyen al fortalecimiento del sector en la línea tecnológica y aportan como fuente de gestión para la construcción y fortalecimiento de la seguridad informática, forjando valor y ventajas competitivas a nivel empresarial.

5.3 POBLACIÓN PARTICIPANTE

En la tabla 3, se encuentra la población participante para el desarrollo de la investigación del análisis de riesgos informáticos según el marco de trabajo CSF NIST 800-30, en la infraestructura tecnológica de G0 S.A.S.

Tabla 3. Población participante de la operación tecnológica de G0 S.A.S.

Responsable	Cargo	Proceso que Administra
Luis Gabriel Rojas	Presidente & CEO	Análisis y desarrollo de software y Tecnología
Alexandra rozo	Gerente general	Facturación y cartera, Talento Humano y SST
Oscar Angulo	Ventas y marketing	Consecución, Fidelización de clientes y reconocimiento de la marca
Daian Pinilla	Finanzas y contabilidad	costos, facturación y cartera liquidación de impuestos, Revisión de nomina

Fuente G0 S.A.S. adaptado por Autores de la Investigación.

5.4 RECOLECCIÓN DE INFORMACIÓN

En este proceso se emplearon las técnicas de la observación, entrevista y encuesta, empleando cuestionarios como los instrumentos de recolección de la información.

- Visita de inspección a la empresa G0 S.A.S.
- Entrevista a funcionarios de G0 S.A.S.
- Encuesta a funcionarios de G0 S.A.S.
- Identificación de Activos de Información de G0 S.A.S.

5.4.1 Visita de inspección G0 S.A.S. Se realizó el reconocimiento físico a las oficinas, observando la infraestructura tecnológica, área de análisis, diseño de software y seguridad física. En la tabla 4 se evidencian los hallazgos obtenidos.

Tabla 4. Hallazgos de la visita de inspección G0 S.A.S.

Gestión y Áreas	Hallazgos
Protección Físico y Ambiental	No se evidencia peligros por causas naturales como inundaciones u otros factores ambientales que pongan en peligro la infraestructura y bienestar de los colaboradores. De igual forma se implementa el programa de seguridad y salud en el trabajo y cada área esta señalizada y separada por módulos. La empresa no cuenta con un sistema CCTV, ni tampoco con un sistema de red de alarmas en caso de presentarse una emergencia.
Seguridad Personal	No se evidencia que personal externo frecuente las instalaciones. La empresa cuenta con procedimientos en la gestión de talento humano. El personal no maneja un control de acceso como parte de su identificación. Una misma persona administra dos áreas.
Protección de los Medios	No se tiene una seguridad en la Documentación confidencial de los procesos de la empresa. La empresa implementa un sistema de almacenamiento en un repositorio. No tienen un control interno de políticas y procedimientos.
Control de Acceso	La información almacenada en el repositorio no está cifrada. Cualquier persona no puede ingresar, sin ser anunciado y sin su debida identificación.

Tabla 4. (Continuación)

Gestión y Áreas	Hallazgos
Adquisición de Sistemas y Servicios	La empresa tiene los procesos definidos en el análisis y desarrollo de software, bajo la implementación de metodologías agiles para el diseño de software, pero esta información no está debidamente documentada.
Infraestructura Tecnológica	Las estaciones de trabajo se conectan a internet por medio de red inalámbrica desde sus computadores portátiles, hay un modem de telecomunicaciones cuyo operador es ETB, que da acceso a internet a los 4 computadores que se utilizan en la operación mediante la tecnología FTTH. No se encuentran equipos activos como *switches*, *routers*, *firewalls* ni servidores. No cuentan con un flujo eléctrico regulado. No cuentan con circuito eléctrico de respaldo
Procesamiento de la Información	La información no es procesada debidamente en todas las áreas. La documentación es operada en medios digitales, no tienen una gestión de documentación establecida. Toda la información es almacenada en un repositorio virtual y no realizan copias de seguridad.

Fuente: Autores de la Investigación.

5.4.2 Entrevista a funcionarios de G0 S.A.S. En la entrevista realizada a la población participante, se determinó la gestión realizada por la empresa en cuanto a temas de seguridad de la información.

En la tabla 5 se muestra el formato de entrevista realizada a G0 S.A.S.

Tabla 5. Formato de entrevista G0 S.A.S.

Formato de Entrevista G0 S.A.S
Fecha _____
Nombre del Entrevistador_____
Funcionario Entrevistado_____
Tema 1: Políticas de seguridad Pregunta: ¿La empresa G0 S.A.S cuenta con manuales y procedimientos debidamente documentados relacionados con seguridad de la información? Respuesta: Procedimiento de Manejo:
Tema 2: Gobierno de seguridad de la información Pregunta: ¿La empresa G0 S.A.S cuenta con un plan de acción debidamente documentados? Respuesta: Procedimiento de Manejo:
Tema 3: Perfiles de usuario Pregunta: ¿La empresa G0 S.A.S para el acceso a la información contenida en el repositorio virtual, tiene establecidos unos perfiles de usuario? Respuesta: Procedimiento de Manejo:

Fuente: Autores de la Investigación.

Esta encuesta fue realizada a 5 personas, en donde los resultados más relevantes están relacionados a: 1) La empresa solo implementa controles para impedir el acceso no autorizado a la información; 2) La empresa solo desarrolla procedimientos para el manejo de incidentes; y 3) La empresa G0 S.A.S tiene establecidos unos perfiles de usuario de acuerdo a sus roles y responsabilidades.

5.4.3 Encuesta a funcionarios de G0 S.A.S. La encuesta es aplicada a la población participante de la investigación, conformada por el presidente & CEO, el Gerente General, y los directores de los departamentos de Ventas - marketing y Finanzas - contabilidad, empleando la herramienta tecnológica Google Form.

En la tabla 6 se muestra el formato de encuesta realizada a G0 S.A.S.

Tabla 6. Formato de encuesta G0 S.A.S.

UNIVERSIDAD PILOTO DE COLOMBIA FACULTAD DE INGENIERÍA

Encuesta de gobierno de Seguridad Informática en la empresa G0 S.A.S

Nombre del Entrevistado_____

Cargo _____, Fecha _____

1. ¿En qué Área desempeña su cargo? Marque las casillas que sean necesarias:
   __Gestión de calidad
   __Consecución y fidelización de clientes
   __Análisis y diseño de software
   __Proceso Comercial
   __Proceso de análisis y diseño
   __Gestión de finanzas y contabilidad
   __Gestión de tecnología del software
   __Gestión humana
   __Gestión de seguridad y salud ocupacional

2. ¿Conoce el gobierno de seguridad de la información implementado en su organización?
   SI___ NO___ NO TIENE ___

3. ¿Conoce en que consiste la seguridad de la información y cuál es su importancia?
   SI___ NO___

4. En su organización, ¿Qué área es responsable de seguridad de la información?
   __Tecnología __Todas las áreas
   __Talento humano __Ninguna

Tabla 6. (Continuación)

5. ¿En la organización existe una persona responsable de seguridad de la información?
   SI___ NO___ NO TIENE ___

6. ¿Tienen implementado una arquitectura de seguridad?
   SI___ NO___ NO SABE ___

7. ¿Considera que la seguridad de la información debería formar parte de la cultura organizacional?
   SI___ NO___ NO SABE ___

8. ¿Conoce las políticas de seguridad implementadas en la Organización?
   SI___ NO___ NO TIENE ___

9. ¿Ha sido capacitado o tenido algún proceso de concientización en el tema de seguridad de la información en el último año?
   SI___ NO___

10. ¿Ha tenido algún incidente de seguridad en su puesto de trabajo en los últimos 6 meses?
    SI___ NO___

11. ¿Cree que la información confidencial de la organización está bien resguardada?
    SI___ NO___

12. ¿La organización ha sido víctima de algún ataque Cibernético?
    SI___ NO___

Tabla 6. (Continuación)

13. ¿Cuándo se ausenta de su puesto de trabajo, deja su computadora bloqueada?
    SI___ NO___

14. ¿Considera que la contraseña que usa cumple con las características de una contraseña segura?
    __Solo letras incluyendo mayúsculas y minúsculas con más de 8 caracteres
    __Solo números con más de 8 caracteres
    __Más de 8 caracteres alfanuméricos

15. ¿Tienen implementado algún factor de doble autenticación para acceso al correo electrónico?
    SI___ NO___

16. ¿Existe algún control para el acceso a la información almacenada en los repositorios?
    SI___ NO___

17. ¿La organización tiene alguna certificación en Sistema de Gestión de seguridad de la información?

    SI___ NO___ NO SABE ___

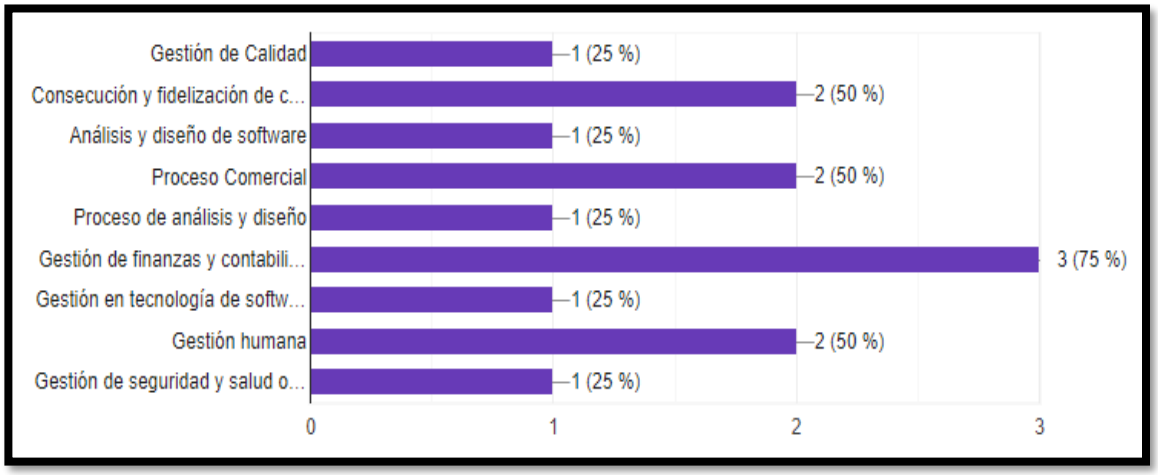
Fuente: Autores de la Investigación.

5.4.3.1 Análisis de la Información de la Encuesta. Esta encuesta tiene como finalidad evidenciar la situación real que actualmente la empresa G0 S.A.S refiere en aspectos de Seguridad de la Información en las diferentes áreas de la empresa y resalta los criterios de cada entrevistado en su conocimiento al tema tratado.

1. ¿En qué Área desempeña su cargo?

En la figura 9 se muestran las dependencias existentes en la empresa G0 S.A.S relacionando la cantidad de personal que intervienen de los procesos de la empresa.

Figura 9. Dependencias administradas.



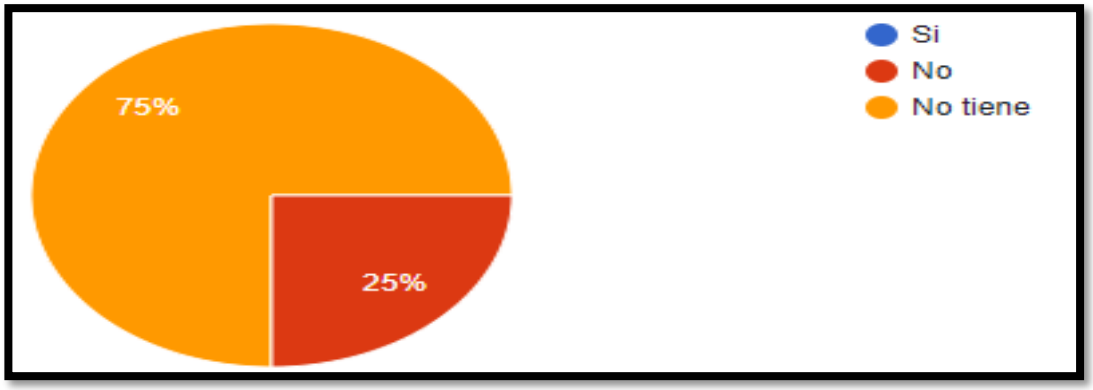
Fuente: Autores de la Investigación.

Se evidencia que una dependencia es operada por tres colaboradores. El proceso más crítico es la gestión de finanzas y contabilidad debido a que el 75 % de colaboradores en la empresa intervienen en la gestión, lo que hace que exista una falencia en la dependencia de roles, y se constituye en un factor de vulnerabilidad que puede ser explotado.

2. ¿Conoce el gobierno de seguridad de la información implementado en su organización?

En la figura 10 se representa el porcentaje relacionado a la pregunta 2.

Figura 10. Existencia de gobierno de seguridad en la organización.



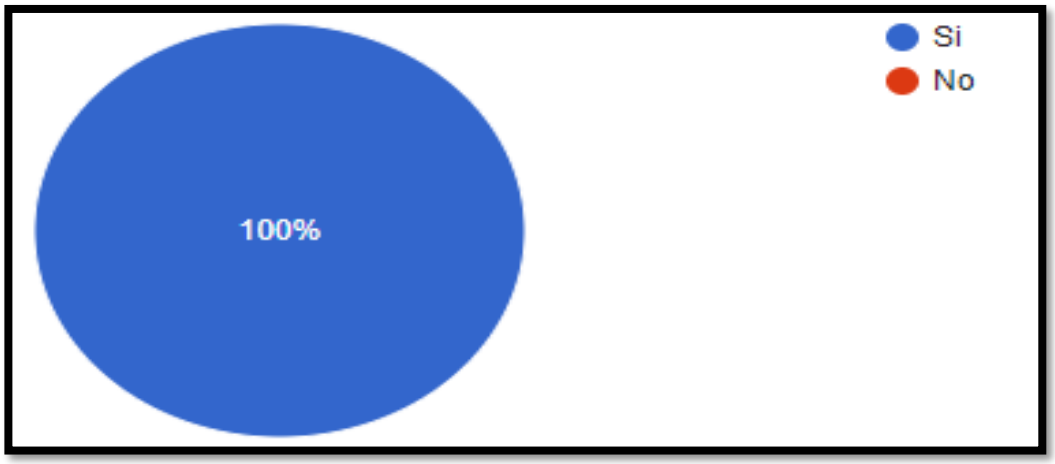
Fuente: Autores de la Investigación.

El 75% de la encuesta indica que no existe un gobierno de seguridad implementado en la organización, y el 25% de los colaboradores manifiestan no conocer el gobierno, evidenciando que la empresa no tiene implementado un gobierno de seguridad, acarreando que los sistemas de información privados pueden ser utilizados con fines maliciosos produciendo consecuencias productivas y financieras críticas.

3. ¿Conoce en que consiste la seguridad de la información y cuál es su importancia?

En la figura 11 se representa el porcentaje relacionado a la pregunta 3.

Figura 11. Conocimiento sobre seguridad de la información.



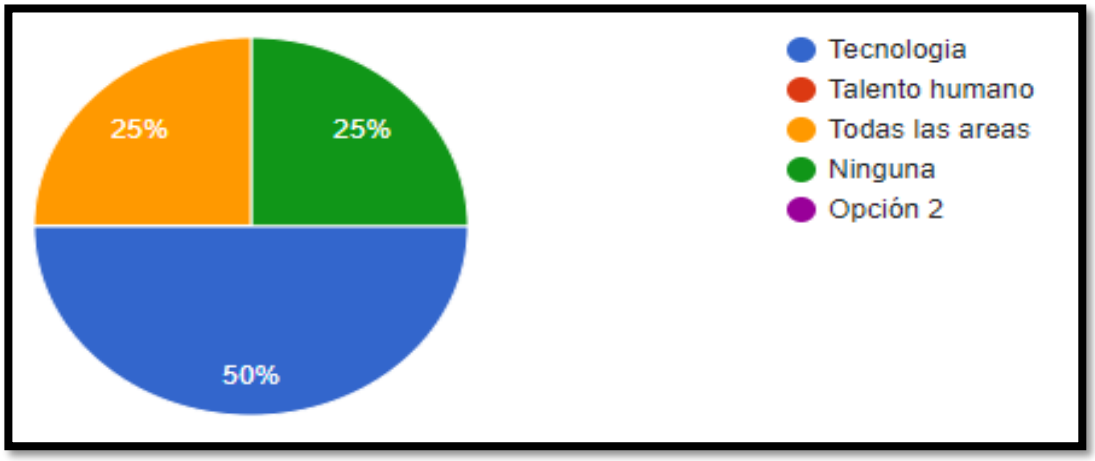
Fuente: Autores de la Investigación.

Se evidencia que el 100% de los colaboradores conocen sobre el tema de seguridad de la información, siendo una ventaja para la implementación de un sistema de gestión de la información que permita preservar los tres principios de la seguridad (confidencialidad, integridad y disponibilidad), en el interior de la empresa y los clientes.

4. En su organización, ¿Qué área es responsable de seguridad de la información?

En la figura 12 se representa el porcentaje relacionado a la pregunta 4.

Figura 12. Áreas responsables de Seguridad de la información.



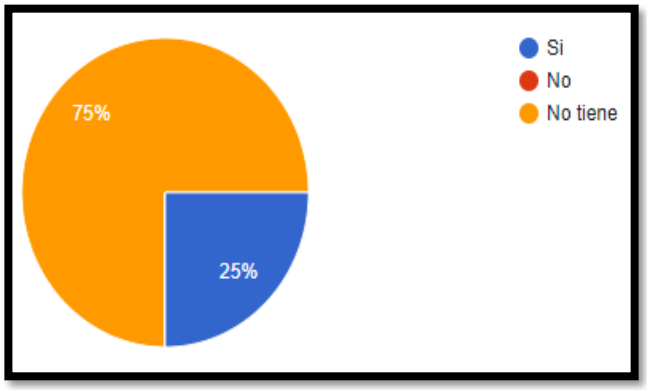
Fuente: Autores de la Investigación.

El 50% de los colaboradores conocen la existencia de un área encargada de la seguridad de la información, un 25% considera que todas las áreas son responsables, mientras que otro 25% desconoce la existencia de un área responsable. Se concluye que existe un área encargada de la seguridad de la información, pero no está definida correctamente y esta gestión debe ser llevada a cabo por el área de tecnología.

5. ¿En la organización existe una persona responsable de seguridad de la información?

En la figura 13 se representa el porcentaje relacionado a la pregunta 5.

Figura 13. Existencia de un responsable de Seguridad de la Información.



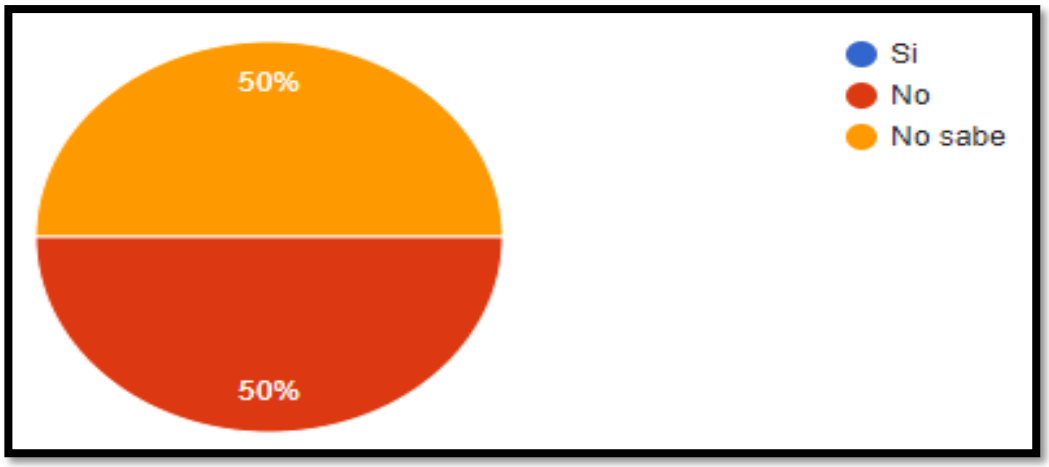
Fuente: Autores de la Investigación.

El 75% de los colaboradores desconoce la persona responsable en la seguridad de la información, mientras que el 25% conocen la existencia de un encargado. Esto traduce a que existe una persona o grupo de personas responsables de la seguridad de la información, pero no están bien definidas sus funciones, y es necesario notificar a todos los colaboradores y esta gestión debe ser llevada a cabo por el área de tecnología.

6. ¿Tienen implementado una arquitectura de seguridad?

En la figura 14 se representa el porcentaje relacionado a la pregunta 6.

Figura 14. Existencia de arquitectura de seguridad.



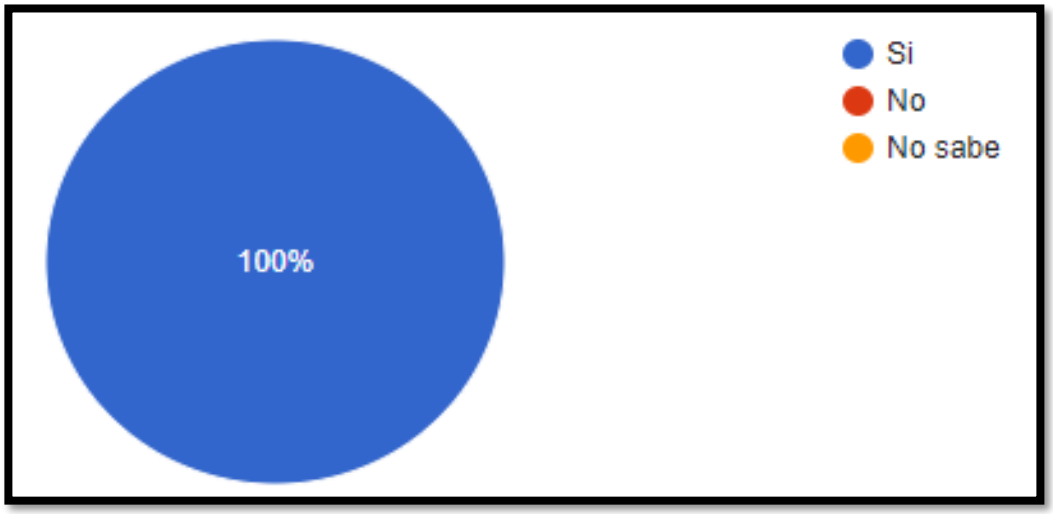
Fuente: Autores de la Investigación.

El 50% de los colaboradores afirman no tener implementado una arquitectura de seguridad, mientras que el otro 50% no saben. Se puede apreciar que no tienen una arquitectura de seguridad, generando un impacto de muy alto riesgo en la información almacenada en equipos, siendo altamente afectada.

7. ¿Considera que la seguridad de la información debería formar parte de la cultura organizacional?

En la figura 15 se representa el porcentaje relacionado a la pregunta 7.

Figura 15. Seguridad de la Información como Cultura Organizacional.



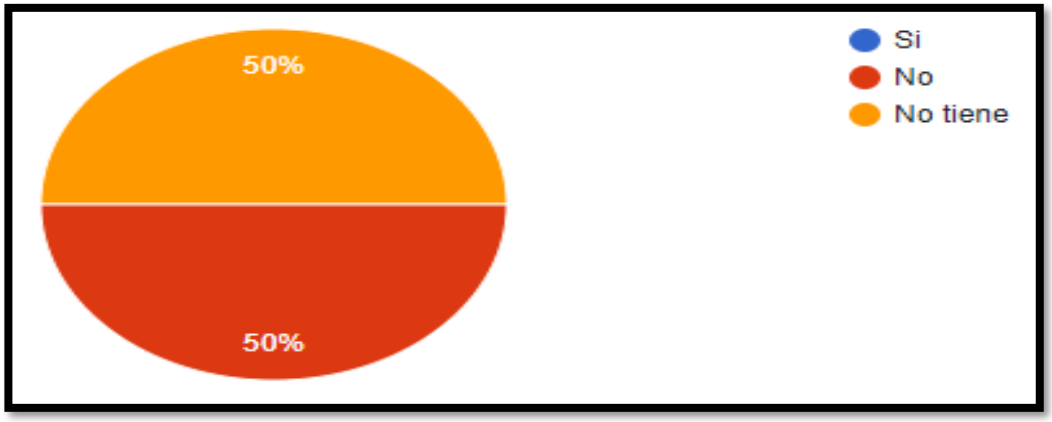
Fuente: Autores de la Investigación.

Se evidencia que el 100% de los colaboradores desea que la seguridad de la información sea implementada y haga parte de una cultura al interior de la empresa.

8. ¿Conoce las políticas de seguridad implementadas en la Organización?

En la figura 16 se representa el porcentaje relacionado a la pregunta 8.

Figura 16. Implementación de políticas de seguridad.



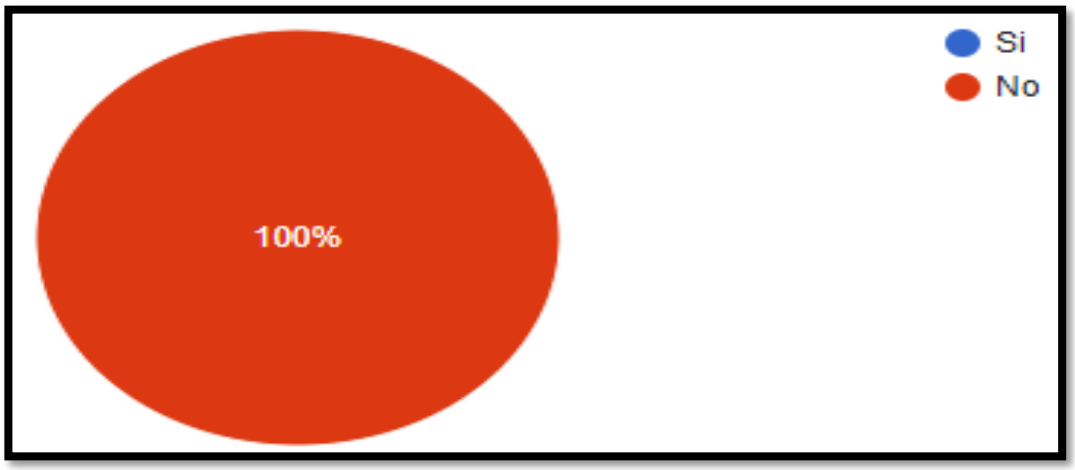
Fuente: Autores de la Investigación.

El 50% de los colaboradores afirman que no conocen las políticas de seguridad al interior de la organización, mientras que el otro 50% afirman que no tienen. Se puede apreciar que no tienen definido un manual de políticas de seguridad, que permita salvaguardar la información en la organización y esta falencia se puede convertir en un impacto de muy alto riesgo, para proteger la confidencialidad, integridad y disponibilidad de la información.

9. ¿Ha sido capacitado o tenido algún proceso de concientización en el tema de seguridad de la información en el último año?

En la figura 17 se representa el porcentaje relacionado a la pregunta 9.

Figura 17. Formación dentro de la organización en seguridad informática.



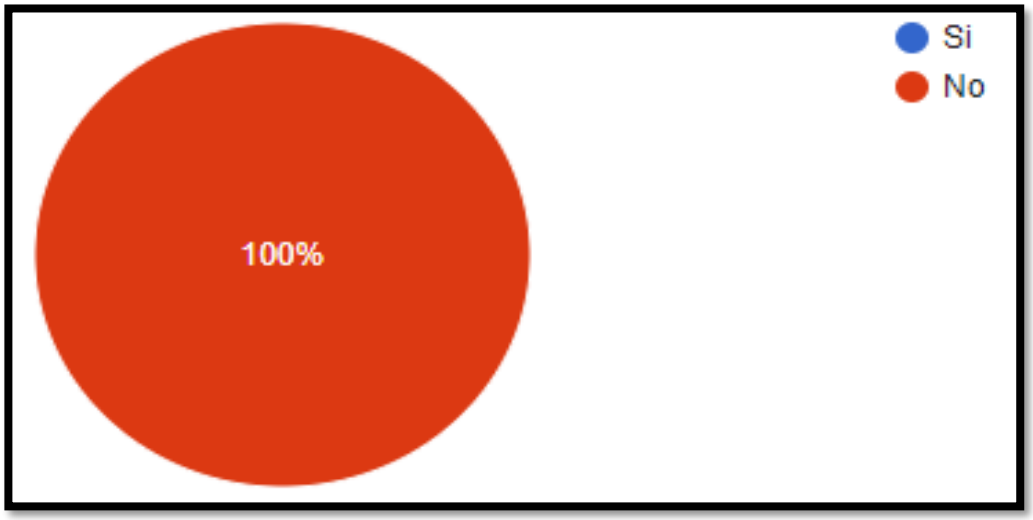
Fuente: Autores de la Investigación.

Se puede apreciar, en primera instancia, que la ausencia de capacitaciones hacia los colaboradores genera una brecha muy amplia de seguridad. En segundo lugar, se evidencia el grave daño en la información al ser manipulada inadecuadamente por desconocimiento.

10. ¿Ha tenido algún incidente de seguridad en su puesto de trabajo en los últimos 6 meses?

En la figura 18 se representa el porcentaje relacionado a la pregunta 10.

Figura 18. Ocurrencia de incidentes de seguridad en la organización.



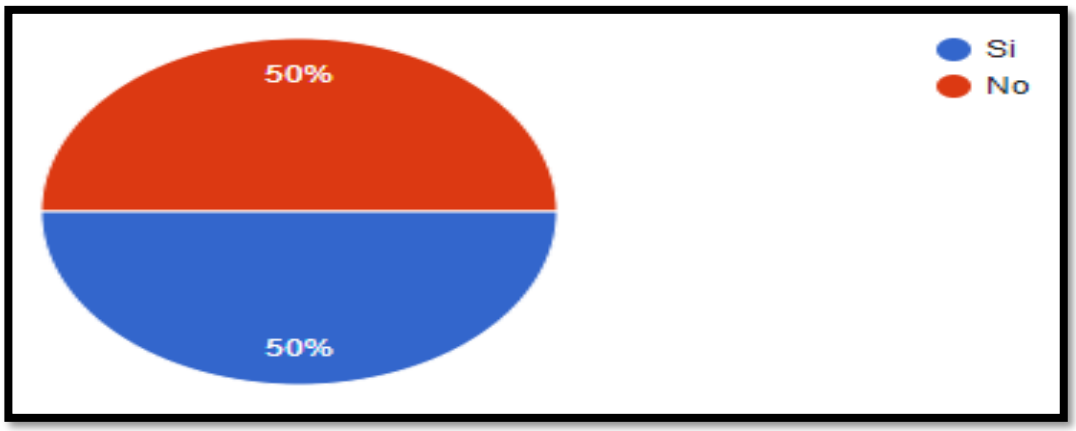
Fuente: Autores de la Investigación.

El 100% de los colaboradores manifiestan no haber sufrido algún incidente durante los últimos 6 meses de trabajo.

11. ¿Cree que la información confidencial de la organización está bien resguardada?

En la figura 19 se representa el porcentaje relacionado a la pregunta 11.

Figura 19. Resguardo de información confidencial dentro de la organización.



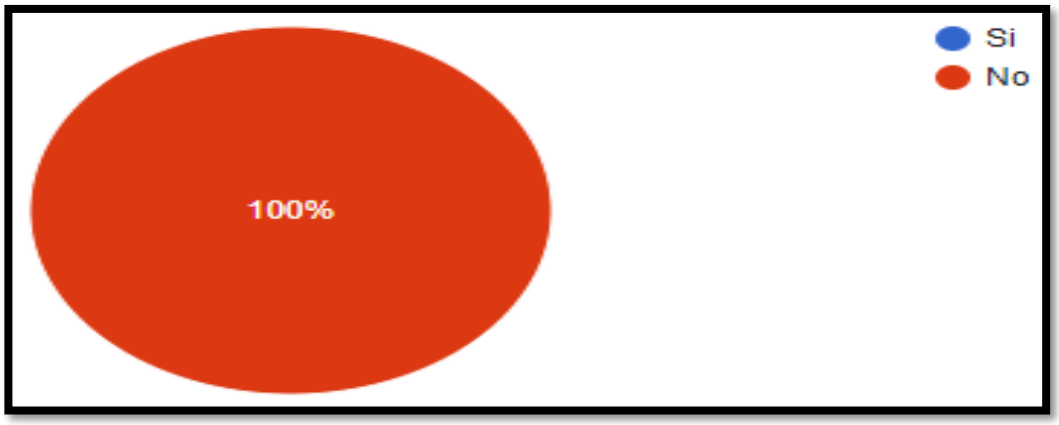
Fuente: Autores de la Investigación.

El 50% de los colaboradores confían que la información que administran está protegida, mientras que el otro 50% desconfían. Se evidencia la necesidad prioritaria de implementar políticas de seguridad o controles para proteger la información.

12. ¿La organización ha sido víctima de algún ataque Cibernético?

En la figura 20 se representa el porcentaje relacionado a la pregunta 12.

Figura 20. Ataques Cibernéticos presentados en la Organización.



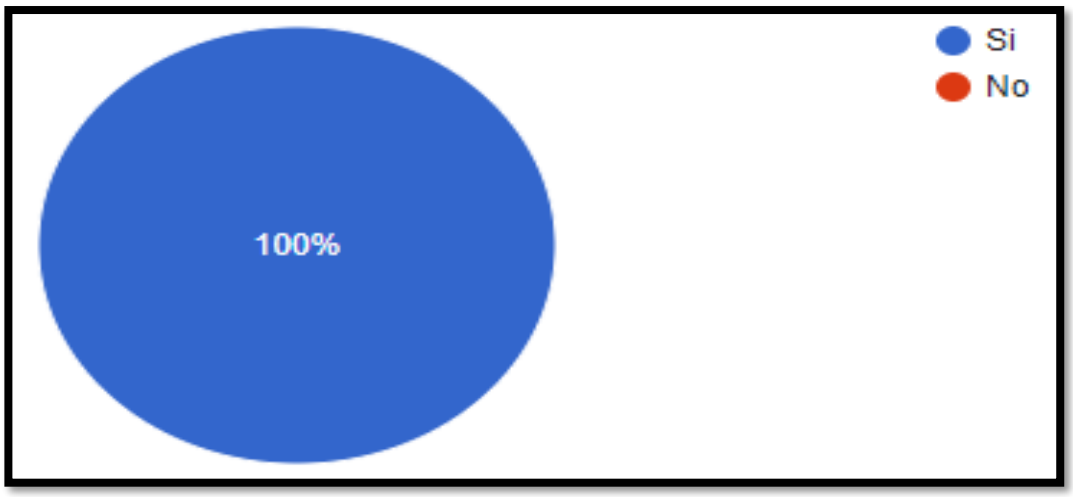
Fuente: Autores de la Investigación.

El 100% de los colaboradores manifiestan no haber sido víctima de algún ataque de ciberseguridad.

13. ¿Cuándo se ausenta de su puesto de trabajo, deja su computadora bloqueada?

En la figura 21 se representa el porcentaje relacionado a la pregunta 13.

Figura 21. Control de bloqueo de automático a los ordenadores de la organización.



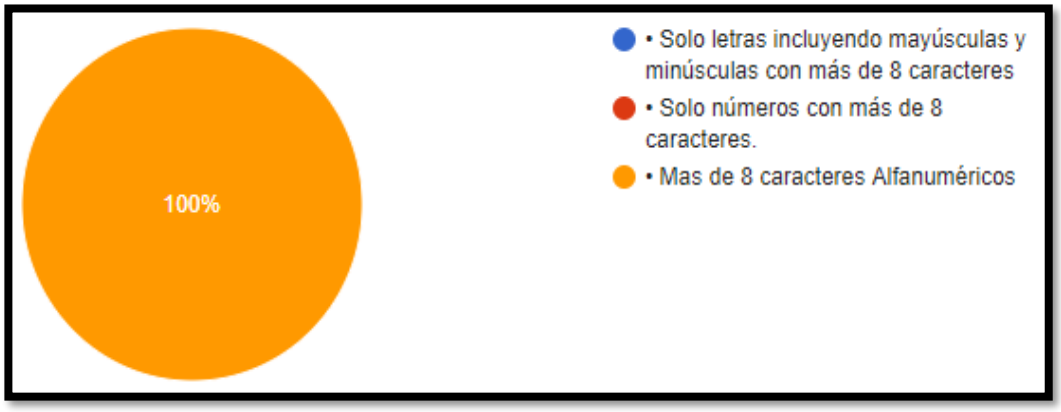
Fuente: Autores de la Investigación.

Se evidencia que el 100% de los colaboradores tienen conciencia y la mejor practica de proteger el acceso a la información confidencial de personas no autorizadas.

14. ¿Considera que la contraseña que usa cumple con las características de una contraseña segura?

En la figura 22 se representa el porcentaje relacionado a la pregunta 14.

Figura 22. Control de contraseña segura.



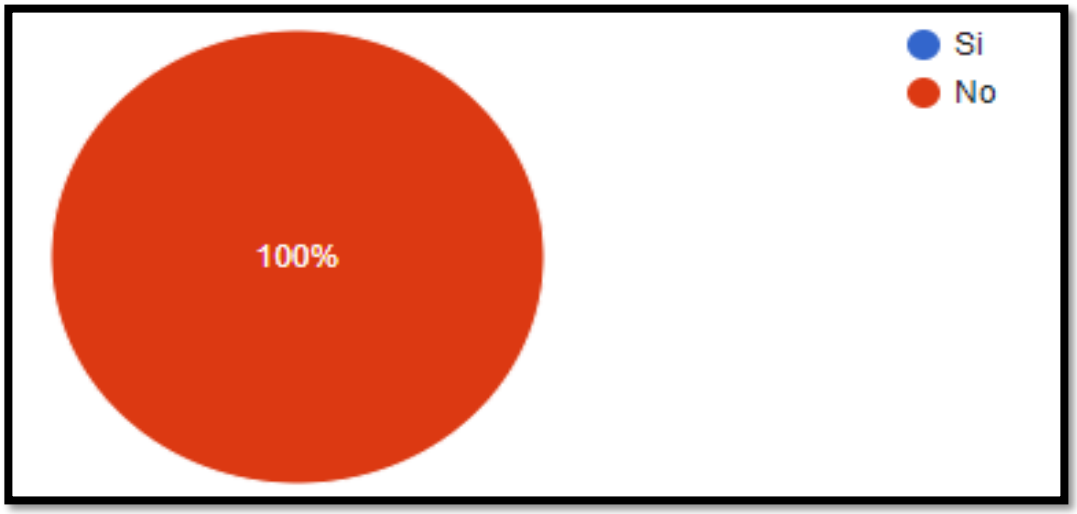
Fuente: Autores de la Investigación.

El 100% de los colaboradores tienen la mejor practica de incluir en sus contraseñas al menos un carácter especial o alfanumérico, una longitud considerable de más de 8 caracteres, al igual que mezcla entre letras y números o mayúsculas y minúsculas lo que genera una contraseña segura.

15. ¿Tienen implementado algún factor de doble autenticación para acceso al correo electrónico?

En la figura 23 se representa el porcentaje relacionado a la pregunta 15.

Figura 23. Implementación de control de acceso a correo electrónico.



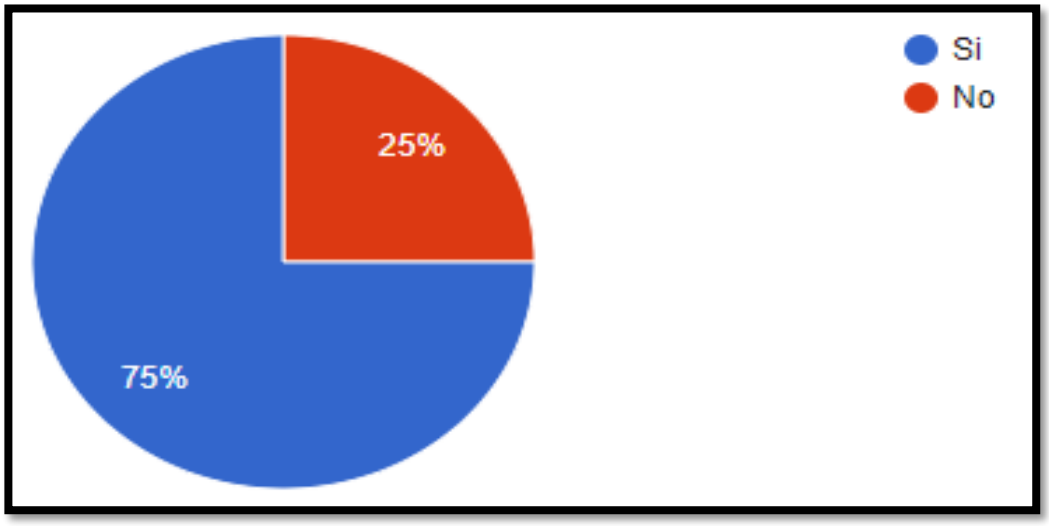
Fuente: Autores de la Investigación.

El 100% de los colaboradores manifiestan no implementar cifrado al acceder a su cuenta de correo, lo que hace más vulnerable el acceso a la información. Se aprecia una falencia en la implementación de controles de seguridad y privacidad.

16. ¿Existe algún control para el acceso a la información almacenada en los repositorios?

En la figura 24 se representa el porcentaje relacionado a la pregunta 16.

Figura 24. Implementación de control de acceso a medios de almacenamiento.



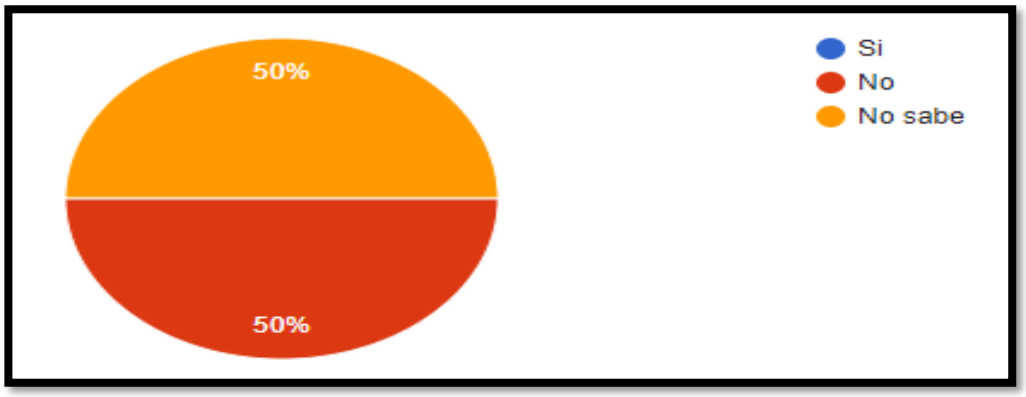
Fuente: Autores de la Investigación.

El 75% de los colaboradores usan un control para acceder a la información en el repositorio, sin embargo, el 25% señala no hacer uso de estos controles. Esto evidencia que no todos los colaboradores acceden a la información de forma segura, lo que ocasiona una vulnerabilidad para una posible pérdida de la información.

17. ¿La organización tiene alguna certificación en Sistema de Gestión de seguridad de la información?

En la figura 25 se representa el porcentaje relacionado a la pregunta 17.

Figura 25. Existencia de certificación en Sistema de Gestión de Seguridad de la Información.



Fuente: Autores de la Investigación.

El 50% de los colaboradores no saben de la existencia de alguna norma de certificación de la organización, mientras que el 50% restante afirman que la empresa no la tiene.

Se puede apreciar que no están certificados en una norma de seguridad de la información, las cuales contribuyen a la administración eficaz de los procesos en la organización.

6. GESTIÓN Y CLASIFICACIÓN DE ACTIVOS G0 S.A.S

6.1 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN DE G0 S.A.S

La identificación de los activos de información se realizó con la colaboración de los líderes de cada área basándose en los siguientes criterios:

- Clasificación de los procesos que cada área maneja.
- Los servicios que presta la organización.
- Las instalaciones físicas en las cuales se encuentran ubicadas las oficinas y los recursos tecnológicos.
- El personal de cada una de las áreas de la organización que hacen parte del desarrollo de los procesos, usuarios y clientes de la organización.

A continuación, se establecen los parámetros para la recolección de los activos de información fundamentales en procesos críticos que pueden generar un riesgo a la organización:

- ID: Número de identificación del activo.
- Proceso de Negocio: Proceso dentro de su estructura al que pertenece el activo.
- Categoría de Activo.

  Clasificación de los activos según corresponda:
  - **Información**: Tipo de datos que son conservados en físico o digital como Documentación, archivos, bases de datos, contratos, formatos, entre otros.
  - **Comunicaciones**: Son servicios contratados por la organización como páginas Web, correo electrónico, entre otros.
  - **Software**: aplicaciones de desarrollo, herramientas de software, software de los sistemas, entre otros.
  - ***Hardware***: Equipos físicos que almacenan información sensible.
  - **Personas**: Recurso Humano que están involucrados en el desarrollo de la operación como clientes, usuarios, entre otros.
  - **Instalaciones Físicas**: Lugares donde se encuentran los activos de información de la organización.

- Activo de Información: Nombre del activo de acuerdo con el proceso al que pertenece.
- Descripción: Observaciones o detalle del activo para ser fácilmente referenciado por las partes del proceso. Anexo 1. Acta de inventario de activos tecnológicos de G0 S.A.S.

Teniendo en cuenta los parámetros anteriormente citados los cuales sirven de insumo, para la elegir la metodología de evaluación de los riesgos de seguridad de la información, en el cuadro 1 se realiza un listado del inventario de activos de información utilizados por G0 S.A.S.

Cuadro 1. Identificación de Activos y Procesos de G0 S.A.S.

ID	Proceso de Negocio		Categoría de Activo	Activo de Información	Descripción
1	Estratégico	Gestión de calidad	Información	Gestor de proyectos	Pruebas de testing
2			Información	Documentos legales de proyectos	Registro donde se almacena la descripción y elaboración del proyecto.
3			Software	Gestor de proyectos	Herramienta para medir los procesos del proyecto
4	Misional	Marketing	Información	Catálogo de servicios	Registro donde se almacena el archivo físico de administrativa y servicios.
5			Información	base de datos clientes en aplicativo	Base datos donde se almacenan los clientes activos con que cuenta la empresa.
6			Personas	Aliados y/o Clientes	Empresas del sector con las cuales se puede establecer relaciones en proyectos.
7			Personas	funcionarios	Personal de ventas y marketing
8	Apoyo	Gestión humana	Información	Documentos de salud ocupacional y talento humano	Registro donde se almacena los archivos de talento humano, como hojas de vidas, capacitaciones, entre otros
9			Personas	funcionarios	Selección y formación del recurso humano
10		Tecnología	Hardware	Portatiles	Equipos de cómputo / estaciones de trabajo

Cuadro 1. (Continuación)

ID	Proceso de Negocio		Categoría de Activo	Activo de Información	Descripción
11	Apoyo	Tecnología	Hardware	Impresora, Fotocopiadora, Escáner	Equipos periféricos
12			Comunicaciones	Hosting y Dominio	servicio de alojamiento y contenido web y accesos al sitio
13			Comunicaciones	Servicio de correo	herramienta de comunicación exclusiva de la empresa
14			Comunicaciones	Página Web	https://g0tech.com/
15			Comunicaciones	Repositorio virtual	Control de versiones de código fuente de los aplicativos desarrollados
16			Comunicaciones	Servidores en la nube (AWS)	para publicaciones de servicios o para uso temporal como el caso de la etapa de pruebas de software.
17			Información	Documentos de Tecnología	Documentos de procedimientos y formatos para las diferentes etapas de los proyectos
18			Software	Plataforma De Reuniones	Plataforma para socializar algún tema en específico en conferencias, se realiza por video, audio o mixto
19			Software	Múltiples softwares de desarrollo y uso interno.	aplicaciones de desarrollo, herramientas de software, software de los sistemas, entre otros

Cuadro 1. (Continuación)

ID	Proceso de Negocio		Categoría de Activo	Activo de Información	Descripción
20	Apoyo	Finanzas y contabilidad	Información	Documentos de nómina	Registro donde se almacena el archivo físico de administrativa y servicios.
21			Información	Documentación Financiera	Registro donde se almacena los archivos de Facturación y comprobantes contables.
22			Software	Software contable Clientes G0	herramienta contable.

Fuente. G0 S.A.S.

6.2 VALORACIÓN DE ESCENARIOS DE RIESGOS DE G0 S.A.S

6.2.1 Objetivos de seguridad. Los escenarios de riesgos identificados en cada uno de los diferentes procesos deben conservar los principios de la seguridad de la información, Confidencialidad, Integridad y Disponibilidad. En caso de que el proceso anterior no se cumpla, se necesita conocer su consecuencia al ser afectado. Esta valoración es importante considerarlo, aunque bajo el marco NIST 800-30, no está establecido.

Confidencialidad
"Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados."[90]

Integridad
"Es la propiedad de salvaguardar la exactitud y estado completo de los activos, que la informacion este completa e inalterada."[91]

Disponibilidad
"Ppropiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada."[92]

En el cuadro 2 se dan los valores de calificación de los objetivos de seguridad.

[90] NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (sgsi). Requisitos [en línea]. 22 de marzo de 2006. 10 p. [Consultado: 29 de agosto de 2021]. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf
[91] Ibid., p.11.
[92] Ibid., p.12.

Cuadro 2. Valores de Calificación Objetivos de Seguridad de Información.

Descriptor	Descripción	Nivel
Bajo	Activos de información en los que se ven afectados los principios de la seguridad de la información. (confidencialidad, integridad y disponibilidad) y su clasificación es baja	1
Importante	Activos de información en los que se ven afectados (1) uno de los principios de la seguridad de la información. (confidencialidad, integridad y disponibilidad) y su clasificación es importante	2
Mayor	Activos de información en los que se ven afectados (2) dos de los principios de la seguridad de la información. (confidencialidad, integridad y disponibilidad) y su clasificación es mayor	3
Significativo	Activos de información en los que se ven afectados todos los principios de la seguridad de la información. (confidencialidad, integridad y disponibilidad) y su clasificación es alta	4

Fuente. Autores de la Investigación.

7. EVALUACIÓN DE RIESGOS

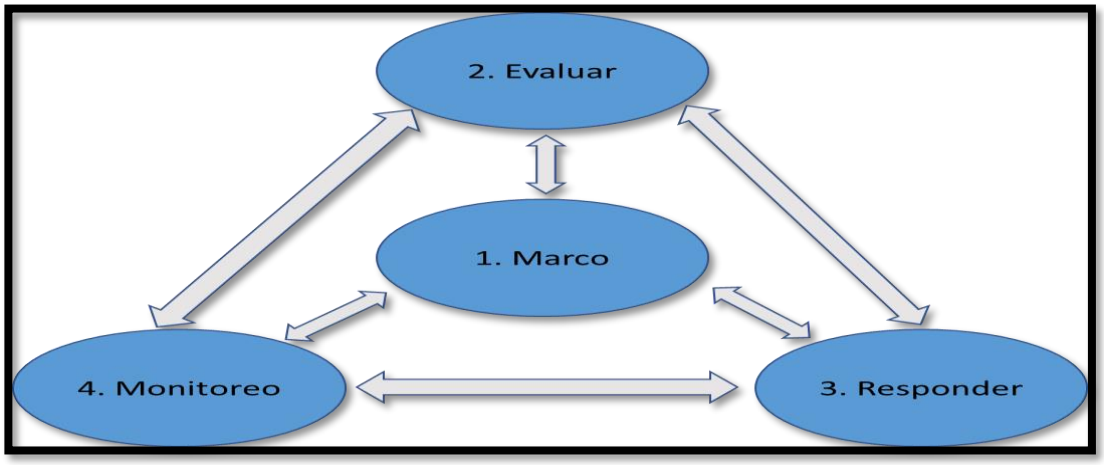
La metodología aplicada para realizar la evaluación de riesgos para los sistemas de información en la empresa G0 S.A.S es la NIST SP800-30 revisión 1, en la cual se establecen las diferentes actividades para cumplir con los objetivos propuestos en la presente investigación. Esta guía específica los pasos que se debe tener en cuenta para identificar, evaluar y priorizar los riesgos de seguridad de la información en la organización. También la guía orienta la identificación de factores de riesgo, para ser monitoreado de forma continua, definiendo los siguientes cuatro (4) pasos: marco, evaluar, responder y monitoreo del riesgo, al igual que los métodos en cada uno de los niveles de jerarquía de gestión de riesgos, Nivel 1: La Organización, Nivel 2: La misión y funciones del negocio y Nivel 3: Los sistemas de información.

Las fases del proceso de evaluación de riesgos asisten en la mejora continua, contribuyendo en el ciclo de vida del desarrollo del sistema a través de los siguientes cuatro pasos, i) incluir el riesgo, ii) evaluar el riesgo, iii) responder al riesgo y monitorear o seguimiento del riesgo. En la figura 26, se muestran los componentes del proceso de gestión de riesgos de NIST SP800-30 R1.

En los niveles 1 y 2 está enfocado a evaluar los riesgos y en el nivel 3, se utiliza para respaldar la implementación de la evaluación de riesgos, y es aquí donde es fundamental el gobierno de seguridad de la información.

En la figura 26, se muestran los componentes del proceso de gestión de riesgos de NIST SP800-30 R1.

Figura 26. Componentes en el proceso de la gestión de riesgos.



Fuente. *NIST U.S. DEPARTMENT OF COMMERCE*. Publicación Especial del NIST 800-30. Adaptado p.4.

En el proceso de la evaluación de riesgos, cada componente desarrolla los pasos y tareas que le permiten a la empresa evaluar y administrar los riesgos mediante los tres niveles: Nivel 1: La Organización, Nivel 2: La misión y funciones del negocio y Nivel 3: Los sistemas de información.

Pasos para desarrollar:

1. Preparación para la evaluación de riesgos.
2. Evaluar los riesgos.
3. Comunicar los resultados obtenidos.
4. Mantener la evaluación de riesgos.

7.1 PREPARACION PARA LA EVALUACION DE RIESGOS

A continuación, se realiza la preparación de riesgos de acuerdo con las tareas relacionadas:

FINALIDAD TAREA 1-1: Conocer el estado actual de seguridad en las diferentes dependencias de la organización, para elaborar un plan de acción de las actividades de gestión, con el fin de aceptar, rechazar, compartir o mitigar el riesgo en cada uno de sus procesos.

ALCANCE TAREA 1-2: Consideraciones que se debe tener en cuenta para realizar la evaluación de riesgos a los sistemas, servicios e infraestructuras de la organización para determinar que partes se ven afectados y toma de decisiones, así como la información que se compartirá como parte de los resultados.

SUPUESTOS Y LIMITACIONES - TAREA 1-3: Identificar criterios que son tenidos en cuenta como supuestos, limitaciones y la tolerancia al riesgo en áreas significativas de la organización, para toma de decisiones dentro del desarrollo de la evaluación de riesgos.

IDENTIFICAR FUENTES DE INFORMACIÓN - TAREA 1-4: Determinar las fuentes de información internas o externas con respecto a las amenazas, vulnerabilidades e impacto para llevar a cabo la evaluación de riesgos.

IDENTIFICAR EL MODELO DE RIESGO Y EL ENFOQUE ANALÍTICO - TAREA 1-5: Definir uno o más modelos de riesgo, enfoque a utilizar en la evaluación de riesgos, en las escalas de evaluación, cualitativo, cuantitativo y semicuantitativo, este último es el más implementado porque combina resultados, con valores numéricos y no numéricos.

RESULTADO PARA LA PREPARACION DE EVALUACION: Se debe crear un plan estratégico el cual está constituido con toda la información recopilada en cada

una de las tareas de la preparación para la evaluación de riesgos y servir de insumo para la elaboración del paso 2 de la guía.

7.2 ANALISIS DE RIESGOS

Entendiendo que G0 SAS no maneja una estructura para una evaluación de riesgos actualmente, se propone una estructura de matriz que cumpla con las expectativas de evaluación de riesgos para reducir el riesgo identificado, y los posibles controles que se deberán implementar.

Este método incorpora el inventario de activos tecnológicos identificados en las diferentes áreas, relacionándola con los escenarios de riesgos para determinar el riesgo inherente como resultado de la operación de estos activos.

La metodología de evaluación de los riesgos está basada en la siguiente estructura:

- Finalidad y alcance.
- Enfoque de evaluación.
- Enfoque de análisis.
- Proceso para para la evaluación de riesgos.

Finalidad y alcance: La funcionalidad de la evaluación de riesgos ofrece el ingreso y consulta de información.

- Escenarios de Riesgo: Es la Identificación de los escenarios de riesgo, y sus afectaciones a la operación de G0 S.A.S según su naturaleza y circunstancias.

- Gestión de Controles: Como actividades de tratamiento del riesgo, se podrán enumerar y dar seguimiento a su ejecución, incluyendo el apartado de Mejora Continua.

- Continuidad de Negocio: Identificación de los Procesos Críticos (Con foco en los relacionados con la operación tecnológica), incluyendo también los elementos tecnológicos que los soportan (Aplicativos y Activos de Información Críticos) y sus necesidades para la continuidad del negocio -En este caso, continuidad de la operación)- como el aseguramiento de la información y su disponibilidad.

Enfoque de evaluación: La evaluación se obtiene a través de tres métodos para el análisis de datos: cuantitativo, cualitativo y semicuantitativo, dependiendo de la condición con la cual se desea analizar y la información que disponible.

- **Método Cualitativo**: Es el método de análisis de riesgos que opera la información basada en términos descriptivos (Raro, Poco probable, Medianamente probable, Probable, Casi certeza).

- **Método Semicuantitativo**: Es el método de análisis de riesgos que mezcla la evaluación cualitativa y cuantitativa obteniendo la información en términos de escalas descriptivas.

- **Método Cuantitativo**: Es el método de análisis de riesgos que opera la información basada en números (valores).

Con todo lo anterior, el enfoque de evaluación para analizar la información que arroje la evaluación de riesgos es cualitativa, determinando los niveles de probabilidad y la magnitud del impacto.

Proceso de evaluación: El proceso de evaluación está conformado por 5 pasos, cada uno asociado a tareas específicas.

- Identificar las Amenazas.
- Identificar las Vulnerabilidad.
- Determinar la Probabilidad.
- Determinar el Impacto.
- Determinar los riesgos de seguridad de la información.

Objetivo: Definir la metodología para la identificación, clasificación y valoración de los riesgos de seguridad de la información, empleando la identificación de activos y amenazas.

Campo de aplicación: Aplica para todos los activos de información, según el alcance del Sistema de Gestión de Seguridad de la Información.

7.2.1 Identificación de riesgos. Se debe determinar los escenarios de riesgos que se pueden presentar entorno a la operación de la empresa G0 S.A.S, mediante los activos de información establecidos en los procesos de las diferentes áreas. De igual forma, se debe identificar las amenazas que estarían comprometidas, las vulnerabilidades que podrían ser explotadas, y el impacto generado a la organización.

Un riesgo representa el nivel de incertidumbre para el cumplimiento de los objetivos de la empresa, de acuerdo con las amenazas y oportunidades en los procesos, servicios, proyectos e iniciativas existentes.

En el cuadro 3 se describe la identificación de activos.

Cuadro 3. Inventario de activos de información de la empresa G0 S.A.S.

Categoría de Activo	Activo de Información	Descripción
Información	Base de datos de clientes en aplicativo clientes G0 Documentos de procedimientos y formatos para las diferentes etapas de los proyectos Documentos de imagen Documentos legales de proyectos Gestor de proyectos Documentos de nómina Catálogo de servicios Documentos de salud ocupacional y talento humano Documentación Financiera	Tipo de datos que son conservados en físico o digital como Documentación, archivos, bases de datos, contratos, formatos, entre otros
Hardware	Equipos de cómputo / portátiles	Equipos físicos que almacenan información sensible
	Impresora, Fotocopiadora, Escáner	
Software	Sistema contable “Clientes G0” Gestor de proyectos (software redmine en servidor en la nube) Plataforma De Reuniones (software para video conferencias en servidor propio) Software de desarrollo “Visual Code”.	Aplicaciones de desarrollo, herramientas de software, software de los sistemas, entre otros
Comunicaciones	Página web Repositorio virtual (control de versiones de código fuente de los aplicativos desarrollados) Servicio de correos Servidores en la nube (AWS): para publicaciones de servicios o para uso temporal como el caso de la etapa de pruebas de software. Hosting y Dominio	Son servicios contratados por la organización como páginas Web, correo electrónico, entre otros
Personas	Funcionarios Aliados o clientes: Empresas del sector con las cuales se puede establecer relaciones en proyectos.	Recurso Humano que están involucrados en el desarrollo de la operación como clientes, usuarios, entre otros

Fuente. G0 S.A.S.

7.2.2 Identificación de amenazas. En la presente metodología las amenazas y oportunidades, se clasifican desde las siguientes perspectivas:

En la tabla 7 se clasifican las amenazas de acuerdo a su activo de información.

Tabla 7. Amenazas y oportunidades por activo.

Software	A: Ataques informáticos, fallas de aplicaciones o sistemas de información, sobrecarga, configuración indebida, etc. O: Sistemas robustos, integraciones con sistemas de otras entidades o compañías, procesos digitalizados, automatización, monetización de datos, etc.
Hardware	A: Fallas en el suministro eléctrico, recalentamiento, daño en un componente, sobrecarga, configuración indebida, sabotaje, golpes, robo, problemas de humedad, etc. O: Infraestructura disponible, redundancia geográfica, centros de datos certificados, esquemas de alta disponibilidad, equipos de última generación, etc
Personas	A: Coacción, errores de operación, mala aplicación de los procedimientos, etc. O: Personal experto, colaboradores motivados, equipos de alto desempeño, programas de desarrollo y capacitación continua, etc
Infraestructura Física	A: Acceso no autorizado a una pantalla, acceso no autorizado a documentos físicos, fuego, inundación, terremoto, vendaval, ataques terroristas, sabotaje, etc. O: Presencia nacional, ubicación de bienes inmuebles, oficinas y centros de datos de alta tecnología, etc.

Fuente: Autores de la Investigación.

7.2.2.1 Identificación fuentes de amenazas. Dentro del NIST SP 800-30 este marco brinda una taxonomía de fuentes de amenaza que son aplicables a cualquier organización. Se da la aplicabilidad de las fuentes de amenazas en la empresa G0 S.A.S. En el cuadro 4. Se identifican las fuentes de amenaza que se agrupan en cuatro (4) tipos: adversidad, accidental, estructural y ambiental.

Cuadro 4. Identificación Fuentes de Amenaza.

Tipo de fuente de amenaza	Subtipo	Fuente de Amenaza	Descripción
Adversidad	Individual	Agente externo Agente interno	Individuos, grupos, organizaciones o estados que buscan explotar la dependencia de la organización de los recursos cibernéticos (es decir, información en forma electrónica, tecnologías de la información y las comunicaciones, y capacidades de comunicación y manejo de información que brindan esas tecnologías).
Accidental	Humano	Usuario Privilegios de administrador	Acciones erróneas realizadas por personas en el transcurso de la ejecución de sus responsabilidades cotidianas.
Estructural	Equipos de tecnología de la información (TI)	Comunicaciones	Fallas de equipos, controles ambientales o software debido al envejecimiento, agotamiento de recursos u otras circunstancias que exceden los parámetros operativos esperados.
	Controles Ambientales	Fuente de alimentación	
	Software	Redes Aplicación uso general	

Fuente: NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30.

7.2.2.2 Identificación eventos de amenazas. Basado en el marco NIST, se define los posibles criterios determinados para identificar los eventos de amenazas presentados en la empresa G0 S.A.S.

En el cuadro 5. Se identifican los eventos de amenaza que se agrupan en ocho (8) tipos: Agente Externo, Agente Interno, Usuario, Administrador, Comunicaciones, Fuente de Alimentación, Red, Aplicación de uso General.

Cuadro 5. Identificación eventos de amenazas.

Fuentes de Amenazas	Eventos de Amenazas
Agente Externo	Realice un rastreo de redes expuestas.
	Recopile información utilizando el descubrimiento de código abierto de información organizacional.
	Realizar reconocimiento y vigilancia de organizaciones específicas.
	Crea ataques de phishing.
	Crea ataques específicamente basados en el entorno de tecnología de la información implementada.
	Crear un sitio web falsificado o falso.
	Elaborar certificados falsificados.
	Causar pérdida de integridad al crear, eliminar y / o modificar datos en sistemas de información de acceso público.
	Causar pérdida de integridad al contaminar o corromper datos críticos.
	Realizar ataques de interceptación de comunicaciones.
	Realice ataques de eliminación de datos en un entorno de nube.
	Llevar a cabo un secuestro de sesiones externo.
	Obtener acceso no autorizado.

Cuadro 5. (Continuación)

Fuentes de Amenazas	Eventos de Amenazas
	Obtenga información confidencial a través del rastreo de redes externas.
	Explotar VPNs.
Agente Interno	Entregue malware conocido a los sistemas de información internos de la organización (por ejemplo, virus por correo electrónico).
	Aprovechar las vulnerabilidades de los sistemas de información internos de la organización.
	Comprometer el software de los sistemas de información críticos de la organización.
	Realizar ingeniería social basada en información privilegiada para obtener información.
	Causar deterioro / destrucción de componentes y funciones críticos del sistema de información.
	Causar la divulgación de información crítica y / o sensible por parte de usuarios autorizados.
	Obtenga acceso no autorizado.
	Obtenga información / datos sensibles de sistemas de información de acceso público.
	Obtener información robando o recolectando sistemas / componentes de información de manera oportunista.
Usuario	Inserte malware dirigido en los sistemas de información organizacional y los componentes del sistema de información.
	Comprometer los sistemas de información críticos a través del acceso físico.
	Realizar ingeniería social basada en personas externas para obtener información.
	Causar la divulgación de información crítica y / o sensible por parte de usuarios autorizados.
Administrador	Inserte malware especializado en los sistemas de información de la organización según las configuraciones del sistema.

Cuadro 5. (Continuación)

Fuentes de Amenazas	Eventos de Amenazas
	Explotar sistemas de información mal configurados o no autorizados expuestos a Internet.
	Realice intentos de inicio de sesión por fuerza bruta / ataques de adivinación de contraseñas.
	Realizar ingeniería social basada en información privilegiada para obtener información.
	Compromiso de Funciones
	Aprovechar las vulnerabilidades de los sistemas de información internos de la organización.
	Provocar divulgación no autorizada y / o indisponibilidad al derramar información confidencial.
Comunicaciones	Falla en componentes tecnológicos
	deterioro / destrucción de componentes tecnológicos
	Perdida de equipos
Fuente de alimentación	Falla de energía eléctrica
	Sobrecalentamiento de componentes
Red	Falla en el servicio de internet
	Pérdida de servicios esenciales (Falla en el servicio de correo, falla en la página web, falla del servidor en la nube)
	Corrupción de datos
Aplicación de uso general	Falla en los aplicativos desarrollados por mal funcionamiento de software
	Falla en los aplicativos desarrollados por código fuente

Fuente. NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30.

7.2.3 Identificación de vulnerabilidades. La asociación de las amenazas y oportunidades con los tipos de activos está relacionada con los factores de vulnerabilidad o fortaleza, es decir, los puntos por donde una amenaza puede generar riesgo para la organización, o una oportunidad que puede generar una capacidad de explotación. Los factores de vulnerabilidad y fortaleza son: personas, procesos, tecnología e infraestructura física.

En la tabla 8, se da la relación entre tipo de activo y los factores de vulnerabilidad o fortaleza.

Tabla 8. Activos y factores de vulnerabilidad y fortaleza.

Tipo de activo donde se encuentra la vulnerabilidad o se destaca la fortaleza	Factor de vulnerabilidad o fortaleza
Software	Tecnología: Integra lo relacionado con los activos tipo hardware y software.
Hardware	
Personas	Recurso Humano.
Infraestructura Física	Infraestructura Física
Definición de procesos	Procesos: Están relacionados con todos los activos.

Fuente: Autores de la Investigación.

Es importante considerar que para cada amenaza u oportunidad identificada, se analiza qué debilidades (vulnerabilidades) o fortalezas pueden estar asociadas a un escenario de riesgo, y este así mismo a un tipo de activo. A continuación se listan los posibles factores de vulnerabilidad o fortaleza.

En la tabla 9, se da la relación entre los escenarios de riesgos y los factores de vulnerabilidad o fortaleza.

Tabla 9. Factores de vulnerabilidad o fortaleza

Humano	Fallas o capacidades de las personas relacionadas con su idoneidad, preparación, motivación, habilidades, condiciones éticas y morales, etc.
Proceso	Fallas o fortalezas en los procesos relacionados con: • La definición del proceso. • La segregación de funciones. • La manualidad o automatización. • Verificaciones y validaciones. • Repetición de funciones • Sobrecarga de funciones • Documentación o caracterización de los procesos y procedimiento
Tecnología	Cuando se presentan fallas, o por el contrario oportunidades de explotación, relacionadas con el *hardware* o el software de la compañía
Infraestructura Física	Relacionado con problemas, o por el contrario oportunidades de explotación, relacionados con los edificios, oficinas, aire acondicionado, racks, servicio eléctrico, cableado, entre otras.

Fuente. Autores de la Investigación.

En el cuadro 6 se relacionan las amenazas y vulnerabilidades, valorando los factores de vulnerabilidad, es decir, los factores que hace que una vulnerabilidad pueda ser explotada y generar su determinado riesgo para la organización en los siguientes aspectos: personas, procesos, tecnología e infraestructura física.

Cuadro 6. valores de los factores de vulnerabilidad categoría De Activo.

No.	Categoría de Activo	Eventos de Amenazas	Vulnerabilidades	Recurso Humano	Procesos	Tecnología	Infraestructura Física
R-1	Comunicaciones	Realice un rastreo de redes expuestas.	Ausencia de mecanismos de protección perimetral y de redes.			X	X
R-2	Software	Recopile información utilizando el descubrimiento de código abierto de información organizacional.	Modificación de software (no autorizado)	X	X		
R-3	Comunicaciones	Realizar reconocimiento y vigilancia de organizaciones específicas.	Insuficiente monitoreo.	X	X	X	
R-4	Comunicaciones	Crea ataques de *phishing.*	Revelación de Información	X		X	
R-5	Comunicaciones	Crea ataques específicamente basados en el entorno de tecnología de la información implementada.	Ausencia de procesos y procedimientos contingentes para (infraestructura física, *hardware*, software, personas y proveedores)	X	X	X	X
R-6	Comunicaciones	Crear un sitio web falsificado o falso.	Robo de Información	X		X	

Cuadro 6. (Continuación)

No.	Categoría de Activo	Eventos de Amenazas	Vulnerabilidades	Recurso Humano	Procesos	Tecnología	Infraestructura Física
R-7	Comunicaciones	Elaborar certificados falsificados.	Ausencia de mecanismos de verificación de integridad: *hashing* firmas digitales, monitoreo de la integridad de archivos.	X	X	X	
R-8	Información	Causar pérdida de integridad al crear, eliminar y / o modificar datos en sistemas de información de acceso público.	Ausencia de procedimientos para el control de la información	X	X		
R-9	Información	Causar pérdida de integridad al contaminar o corromper datos críticos.	Ausencia de registro del acceso de lectura a los archivos.	X	X		
R-10	Comunicaciones	Realizar ataques de interceptación de comunicaciones.	Líneas de comunicación desprotegidas			X	X
R-11	Información	Realice ataques de eliminación de datos en un entorno de nube.	Ausencia de copias de respaldo.	X	X	X	
R-12	Comunicaciones	Llevar a cabo un secuestro de sesiones externo.	Ausencia de mecanismos para identificación y autenticación de usuarios	X	X	X	
R-13	Información	Obtener acceso no autorizado.	Ausencia de una política de control de acceso.	X	X	X	X

Cuadro 6. (Continuación)

No.	Categoría de Activo	Eventos de Amenazas	Vulnerabilidades	Recurso Humano	Procesos	Tecnología	Infraestructura Física
R-14	Comunicaciones	Obtenga información confidencial a través del rastreo de redes externas.	Ausencia de mecanismos de protección perimetral y de redes			X	X
R-15	Comunicaciones	Explotar VPNs.	Ausencia de cifrado			X	
R-16	Comunicaciones	Entregue malware conocido a los sistemas de información internos de la organización (por ejemplo, virus por correo electrónico).	Ausencia de procedimientos de control para licenciamiento de software	X	X	X	
R-17	Comunicaciones	Aprovechar las vulnerabilidades de los sistemas de información internos de la organización.	Inexistencia de gestión y administración de vulnerabilidades sobre activos de TI	X	X	X	X
R-18	Software	Comprometer el software de los sistemas de información críticos de la organización.	Especificaciones incompletas, incorrectas o no documentadas para desarrolladores	X	X		
R-19	Información	Realizar ingeniería social basada en información privilegiada para obtener información.	Ausencia de programas de concientización	X	X		

Cuadro 6. (Continuación)

No.	Categoría de Activo	Eventos de Amenazas	Vulnerabilidades	Recurso Humano	Procesos	Tecnología	Infraestructura Física
R-20	*Hardware*	Causar deterioro / destrucción de componentes y funciones críticos del sistema de información.	Ausencia de planes de recuperación tecnológico	X	X	X	
R-21	Personas	Causar la divulgación de información crítica y / o sensible por parte de usuarios autorizados.	Ausencia de responsabilidades de seguridad de la información	X	X		
R-22	Comunicaciones	Obtenga acceso no autorizado.	ausencia de control de acceso (físico y lógico)	X	X	X	X
R-23	Información	Obtenga información / datos sensibles de sistemas de información de acceso público.	Ausencia de clasificación de información	X	X		
R-24	Información	Obtener información robando o recolectando sistemas / componentes de información de manera oportunista.	Ausencia de gobierno (Estructura organizacional, políticas, procesos y procedimientos en seguridad de la Información)	X	X		
R-25	Comunicaciones	Inserte malware dirigido en los sistemas de información organizacional y los componentes del sistema de información.	Uso no controlado de software descargado	X	X	X	

Cuadro 6. (Continuación)

No.	Categoría de Activo	Eventos de Amenazas	Vulnerabilidades	Recurso Humano	Procesos	Tecnología	Infraestructura Física
R-26	Información	Comprometer los sistemas de información críticos a través del acceso físico.	ausencia de control de acceso físico	X	X		X
R-27	Personas	Realizar ingeniería social basada en personas externas para obtener información.	Ausencia de cláusulas sobre seguridad de la información en contratos con empelados y terceros	X	X		
R-28	Personas	Causar la divulgación de información crítica y / o sensible por parte de usuarios autorizados.	Ausencia de matriz de roles y perfiles	X	X		
R-29	Software	Inserte malware especializado en los sistemas de información de la organización según las configuraciones del sistema.	Ausencia de procedimientos de control para licenciamiento de software	X	X	X	
R-30	Comunicaciones	Explotar sistemas de información mal configurados o no autorizados expuestos a Internet.	Incorrecta asignación de privilegios	X	X	X	
R-31	Comunicaciones	Realice intentos de inicio de sesión por fuerza bruta / ataques de adivinación de contraseñas.	Contraseña insegura	X	X		

Cuadro 6. (Continuación)

No.	Categoría de Activo	Eventos de Amenazas	Vulnerabilidades	Recurso Humano	Procesos	Tecnología	Infraestructura Física
R-32	Personas	Realizar ingeniería social basada en información privilegiada para obtener información.	Ausencia de programas de capacitación y sensibilización en seguridad de la información	X	X		
R-33	Personas	Compromiso de Funciones	Falta de segregación de funciones.	X	X		
R-34	Información	Aprovechar las vulnerabilidades de los sistemas de información internos de la organización.	Inexistencia de gestión y administración de vulnerabilidades sobre activos de TI	X	X	X	X
R-35	Personas	Provocar divulgación no autorizada y/o indisponibilidad al derramar información confidencial.	Ausencia de responsabilidades de seguridad de la información	X	X		
R-36	*Hardware*	Falla en componentes Tecnológicos	Falta o ausencia de mantenimiento o ausencia de programa de reemplazo de partes	X	X		X
R-37	*Hardware*	Deterioro / destrucción de componentes tecnológicos	Ausencia de procedimiento de destrucción de medios		X		X
R-38	*Hardware*	Perdida de equipos	Robo de medios	X	X		X

Cuadro 6. (Continuación)

No.	Categoría de Activo	Eventos de Amenazas	Vulnerabilidades	Recurso Humano	Procesos	Tecnología	Infraestructura Física
R-39	*Hardware*	Falla de energía eléctrica	Ausencia o mal funcionamiento de una UPS.	X	X		X
R-40	*Hardware*	Sobrecalentamiento de componentes	Mantenimiento insuficiente de la infraestructura para el servicio eléctrico.	X	X	X	X
R-41	Comunicaciones	Falla en el servicio de internet	Ausencia de un canal de internet alterno			X	X
R-42	Comunicaciones	Pérdida de servicios esenciales (Falla en el servicio de correo, falla en la página web, falla del servidor en la nube)	Ausencia de procesos y procedimientos contingentes para (infraestructura física, *hardware*, software, personas y proveedores)	X	X	X	X
R-43	Información	Corrupción de datos	Ausencia de copias de respaldo.	X	X	X	
R-44	Software	Falla en los aplicativos desarrollados por mal funcionamiento de software	Ausencia de planes de contingencia		X		
R-45	Software	Falla en los aplicativos desarrollados por código fuente	Ausencia de gestión de accesos		X		

Fuente. Autores de la Investigación.

7.3 EVALUACION DE RIESGOS

7.3.1 Identificación de Riesgos. En este bloque se identifican los diferentes escenarios de riesgos y el criterio que se debe tener en cuenta para determinar la consecuencia de este. Dentro de las actividades y definiciones que componen un proceso, proyecto, servicio o iniciativa, los factores de amenaza y vulnerabilidades identificadas …en la sección 7.2… deben conservar los principios de la seguridad de la información. Una vez identificados los riesgos, se procede a estimar la probabilidad de ocurrencia y el impacto de sus consecuencias.

Criterios de calificación: Teniendo en cuenta los riesgos identificados se debe medir el grado de criticidad de las consecuencias de los riesgos encontrados en las diferentes calificaciones: Económico, Operativo, Reputacional, Socioambiental, Legal. Esta valoración es importante considerarla, aunque bajo el marco NIST 800-30, no está establecido.

Económico
Pérdida de activos >= 100.000 SMMLV.
Impacto sobre los estados financieros por un valor >= 10% sobre el EBITDA anual.

Operativo
La afectación puede suspender la operación o los servicios prestados por la empresa de forma indefinida con imposibilidad de recuperación, inexistencia de plan de contingencia y continuidad, generación de daños irreparables o destrucción de equipos o instalaciones.

Reputacional
Difusión externa a nivel internacional. Pérdida total o muy grave del apoyo o credibilidad de los grupos de interés prioritarios.

Socioambiental
Muertes o daño ambiental no recuperable.
Indisponibilidad de >=20% de los cargos de una misma área crítica.

Legal
Multas acumuladas anuales superior a dos impuestas por órganos de control u otras entidades por incumplimiento normativo o contractual. Declaratoria de caducidad del contrato.

7.3.2 Evaluación de riesgos. Este bloque es la revisión de las actividades y definiciones que componen un proceso, proyecto, servicio o iniciativa, para identificar las amenazas u oportunidades que puedan influir negativa o positivamente en el cumplimiento de los objetivos. Una vez identificada la amenaza

u oportunidad, se procede a estimar la probabilidad de ocurrencia y el impacto de sus consecuencias.

7.3.2.1 Probabilidad. "Las organizaciones evalúan la probabilidad de que se inicie un evento de amenaza tomando en consideración las características de las fuentes de amenaza de interés, incluidas la capacidad, la intención y la focalización.
La probabilidad general de un evento de amenaza es una combinación de: (i) la probabilidad de que el evento ocurra (por ejemplo, debido a un error humano o desastre natural) o bien sea iniciado por un atacante y (ii) la probabilidad de que el inicio / ocurrencia resulte en impactos adversos."[93]

Para cada amenaza u oportunidad identificada, se analiza el número de veces que ésta puede ocurrir en un lapso determinado, evaluando la probabilidad de que una vulnerabilidad pueda ser explotada por cada amenaza u oportunidad identificada tomando como base, la guía del siguiente cuadro:

En el cuadro 7, se presentan los valores para evaluar los riesgos basados en la probabilidad.

Cuadro 7. Valoración de probabilidad.

Valores calificación probabilidad de Ocurrencia		
Descriptor	**Descripción**	**Nivel**
Raro	Eventualidad que no es probable. No se ha presentado en los últimos 5 años	1
Poco probable	Eventualidad poco común. Máximo una vez al año.	2
Medianamente probable	Puede ocurrir en algún momento. De 3 a 6 veces al año.	3
Probable	Hay buenas razones para creer que el riesgo ocurriría en muchas circunstancias. Desde semanalmente hasta mensualmente	4
Casi certeza	Se espera que el riesgo ocurra en la mayoría de las circunstancias. Diariamente	5

Fuente. Autores de la Investigación.

[93] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.42

7.3.2.2 Impacto. “La evaluación del impacto puede implicar la identificación de activos u objetivos potenciales de fuentes de amenazas, incluidos los recursos de información (por ejemplo, información, datos repositorios, sistemas de información, aplicaciones, tecnologías de la información, enlaces de comunicaciones), personas y recursos físicos (por ejemplo, edificios, fuentes de alimentación), que podrían verse afectados por eventos de amenaza.”[94]

Para cada amenaza u oportunidad se evalúa el efecto que ésta pueda tener sobre los objetivos de la organización, para ello es necesario que el dueño del riesgo tome como base el siguiente cuadro.

En el cuadro 8, se presentan los valores para evaluar los riesgos basados en el impacto.

Cuadro 8. Valores de Calificación del Impacto.

Valores Calificación Del Impacto		
Descriptor	**Descripción**	**Nivel**
Raro	• No hay interrupción de las operaciones. • No genera sanciones legales, regulatorias, económicas y/o administrativas. • No afecta las relaciones con los clientes. • No se genera una afectación económica. • No hay afectación a la imagen. • No se identifica un beneficio claro	1
	• Afectación operativa en los procesos. • Se generan procesos legales y/o regulatorios directos con sanciones o multas leves.	2

[94] NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30. Op.Cit., p.44

Cuadro 8. (Continuación)

Valores Calificación Del Impacto		
Descriptor	**Descripción**	**Nivel**
Bajo	• Se presentan algunas reclamaciones por parte de clientes, accionistas, proveedores, pero no se afecta continuidad de la relación. • El costo estimado de la afectación es manejado sin intervención de niveles directivos. • Ocurrencia de una situación que puede afectar la reputación de la organización a nivel de área o proceso. • Se identifica un beneficio a nivel interno para un proceso, proyecto o servicio.	
Medio	• Afectación operativa en ventas. • Reproceso de actividades y aumento de la carga operativa. • Se generan procesos legales y/o regulatorios directos con sanciones o multas graves Reclamaciones de clientes, accionistas, proveedores que requieren de un plan de acción de corto plazo. • El costo estimado de la afectación requiere la aprobación de niveles directivos. • Ocurrencia de una situación que puede afectar la reputación de la organización. • Se identifica un beneficio económico, operativo o de imagen para la organización.	3

Cuadro 8. (Continuación)

Valores Calificación Del Impacto		
Descriptor	**Descripción**	**Nivel**
Alto	• Se generan procesos legales y/o regulatorios directos que obligan a suspender la operación y/o la comercialización en alguna línea de negocio y/o requieran un plan de acción a corto plazo. • Se generan procesos legales y/o regulatorios que impliquen responsabilidad patrimonial o penal de un directivo de la compañía. • Ocurrencia de una situación que puede afectar la reputación de la organización. • Se identifica un beneficio que permita a la organización impulsar su crecimiento, recomendación y/o mejorar su rentabilidad en las líneas de producto y servicios existentes	4
Muy Alto	• Afectación operativa sobre toda la organización • Cualquier impacto en la prestación de servicio que afecte por más de 24 horas al 20% o más de la base clientes de la organización. • Se generan procesos legales y/o regulatorios directos que podrían significar el cierre de las operaciones. • Se identifica un beneficio que permita a la organización impulsar su crecimiento, recomendación y/o mejorar su rentabilidad a través de nuevos productos o servicios.	5

Fuente: Autores de la Investigación.

Para determinar el nivel de riesgo se utilizan los resultados obtenidos sobre el impacto y la probabilidad aplicando el producto cartesiano entre los valores de la probabilidad y los del impacto. En el siguiente cuadro se relaciona los criterios de valoración del riesgo, en donde E=Extremo, A=Alto, M=Moderado, B=Bajo

En el cuadro 9, se presentan la correlación para evaluar los riesgos basados en la probabilidad e impacto.

Cuadro 9. Valoración del Riesgo.

Matriz de calificación y respuesta a los riesgos					
Probabilidad	**Impacto**				
	Muy bajo (1)	**Bajo (2)**	**Medio (3)**	**Alto (4)**	**Muy alto (5)**
Casi certeza (5)	A	A	E	E	E
Muy probable (4)	M	A	A	E	E
Probable (3)	B	M	A	E	E
Poco probable(2)	B	B	M	A	E
Raro (1)	B	B	M	A	A

Fuente: Autores de la Investigación.

7.3.2.3 Riesgo Inherente. Es el que se presenta por la naturaleza de la actividad que se está realizando, no se puede separar de la situación donde se presenta, siendo propio de las acciones que conlleva el proceso, proyecto, iniciativa o servicio evaluado. Para evaluar el riesgo inherente no se deben considerar los controles existentes.

Con base a la matriz de riesgos planteada para esta evaluación se genera el riesgo para ser valorado dando como resultado el valor de riesgo Inherente. Ver anexo 2.

En el cuadro 10 se relaciona la matriz de riesgos con su respectiva valoración obteniendo como resultado el riesgo inherente.

Cuadro 10. Matriz de Riesgos G0 S.A.S.

Identificación del riesgo		Análisis de riesgos		
ID Riesgo	**Descripción de Riesgo**	**Probabilidad**	**Impacto**	**Valoración del riesgo**
R1	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Externo que Realice un rastreo de redes expuestas. Debido a Ausencia de mecanismos de protección perimetral y de redes. Causando Información comprometida afectando el principio de Confidencialidad.	Probable	Alto	4-Extrema
R2	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo Legal y operativo por Agente Externo que Recopile información utilizando el descubrimiento de código abierto de información organizacional. Debido a Modificación de software (no autorizado) causando Funcionamiento deficiente de software afectando todos los principios de	Probable	Muy Alto	4-Extrema
R3	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y Operativo por Agente Externo que Realizar reconocimiento y vigilancia de organizaciones específicas. Debido a Insuficiente monitoreo. Causando Divulgación de información afectando el principio de Confidencialidad.	Probable	Medio	3-Alta

Cuadro 10. (Continuación)

Identificación del riesgo		Análisis de riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del riesgo**
R4	Riesgo de seguridad de la información de categoría de activo: comunicaciones, con una afectación de tipo legal, operativo y económico por agente externo que crea ataques de phishing. Debido a revelación de información causando información comprometida afectando todos los principios de seguridad.	Casi Certeza	Muy Alto	4-Extrema
R5	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Externo que Crea ataques específicamente basados en el entorno de tecnología de la información implementada. Debido a Ausencia de procesos y procedimientos contingentes para (infraestructura física, *hardware*, software, personas y proveedores) causando Pérdida de servicios esenciales afectando todos los principios de seguridad.	Probable	Alto	4-Extrema
R6	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal, Operativo y Económico por Agente Externo que Crear un sitio web falsificado o falso. Debido a Robo de Información causando Información comprometida afectando todos los principios de seguridad.	Probable	Muy Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del riesgo		Análisis de riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R7	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal por Agente Externo que Elaborar certificados falsificados. Debido a Ausencia de mecanismos de verificación de integridad: *hashing* firmas digitales, monitoreo de la integridad de archivos. Causando Modificación indebida afectando el principio de Integridad.	Probable	Muy Alto	4-Extrema
R8	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal y operativo por Agente Externo que Causar pérdida de integridad al crear, eliminar y / o modificar datos en sistemas de información de acceso público. Debido a Ausencia de procedimientos para el control de la información causando Información comprometida afectando el principio de Integridad.	Probable	Muy Alto	4-Extrema
R9	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal y operativo por Agente Externo que Causar pérdida de integridad al contaminar o corromper datos críticos. Debido a Ausencia de registro del acceso de lectura a los archivos. causando Información comprometida afectando el principio de Disponibilidad.	Probable	Muy Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R10	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y Operativo por Agente Externo que Realizar ataques de interceptación de comunicaciones. Debido a Líneas de comunicación desprotegidas causando Información comprometida afectando todos los principios de seguridad.	Casi Certeza	Alto	4-Extrema
R11	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal, Operativo y Económico por Agente Externo que Realice ataques de eliminación de datos en un entorno de nube. Debido a Ausencia de copias de respaldo. Causando Indisponibilidad afectando el principio de Disponibilidad.	Probable	Muy Alto	4-Extrema
R12	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal, Operativo y Económico por Agente Externo que Llevar a cabo un secuestro de sesiones externo. Debido a Ausencia de mecanismos para identificación y autenticación de usuarios causando Información comprometida afectando todos los principios de seguridad.	Poco Probable	Alto	3-Alta

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R13	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Operativo por Agente Externo que Obtener acceso no autorizado. Debido a Ausencia de una política de control de acceso. Causando Accesos no autorizados a sistemas de información afectando el principio de Confidencialidad.	Casi Certeza	Muy Alto	4-Extrema
R14	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Externo que Obtenga información confidencial a través del rastreo de redes externas. Debido a Ausencia de mecanismos de protección perimetral y de redes causando Información comprometida afectando el principio de Confidencialidad.	Casi Certeza	Alto	4-Extrema
R15	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Externo que Explotar VPNs. debido a Ausencia de cifrado causando Divulgación de información afectando todos los principios de seguridad.	Probable	Muy Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R16	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y operativo por Agente Interno que Entregue malware conocido a los sistemas de información internos de la organización (por ejemplo, virus por correo electrónico). debido a Ausencia de procedimientos de control para licenciamiento de software causando Corrupción de datos afectando todos los principios de seguridad.	Probable	Muy Alto	4-Extrema
R17	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Interno que Aprovechar las vulnerabilidades de los sistemas de información internos de la organización. Debido a Inexistencia de gestión y administración de vulnerabilidades sobre activos de TI causando Información comprometida afectando todos los principios de seguridad.	Casi Certeza	Muy Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R18	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo Operativo por Agente Interno que Comprometer el software de los sistemas de información críticos de la organización. Debido a Especificaciones incompletas, incorrectas o no documentadas para desarrolladores causando Funcionamiento deficiente de software afectando el principio de Disponibilidad.	Probable	Alto	4-Extrema
R19	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal por Agente Interno que Realizar ingeniería social basada en información privilegiada para obtener información. Debido a Ausencia de programas de concientización causando Información comprometida afectando el principio de Confidencialidad.	Casi Certeza	Muy Alto	4-Extrema
R20	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo Operativo por Agente Interno que Causar deterioro / destrucción de componentes y funciones críticos del sistema de información. Debido a Ausencia de planes de recuperación tecnológico causando Indisponibilidad en la entrega de productos y servicios afectando el principio de Disponibilidad.	Casi Certeza	Muy Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R21	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Legal por Agente Interno que Causar la divulgación de información crítica y / o sensible por parte de usuarios autorizados. Debido a Ausencia de responsabilidades de seguridad de la información causando Información comprometida afectando el principio de Confidencialidad.	Casi Certeza	Alto	4-Extrema
R22	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y operativo por Agente Interno que Obtenga acceso no autorizado. Debido a ausencia de control de acceso (físico y lógico) causando Accesos no autorizados a sistemas de información afectando todos los principios de seguridad.	Probable	Alto	4-Extrema
R23	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal por Agente Interno que Obtenga información / datos sensibles de sistemas de información de acceso público. Debido a Ausencia de clasificación de información causando Información comprometida afectando el principio de Confidencialidad.	Probable	Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R24	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal y operativo por Agente Interno que Obtener información robando o recolectando sistemas / componentes de información de manera oportunista. Debido a Ausencia de gobierno (Estructura organizacional, políticas, procesos y procedimientos en seguridad de la Información) causando Información comprometida afectando todos los principios de seguridad.	Probable	Alto	4-Extrema
R25	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y operativo por Usuario que Inserte malware dirigido en los sistemas de información organizacional y los componentes del sistema de información. Debido a Uso no controlado de software descargado causando Funcionamiento deficiente de software afectando el principio de Integridad.	Probable	Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R26	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Operativo por Usuario que Comprometer los sistemas de información críticos a través del acceso físico. Debido a ausencia de control de acceso físico causando Accesos no autorizados a sistemas de información afectando el principio de Confidencialidad.	Probable	Alto	4-Extrema
R27	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Legal por Usuario que Realizar ingeniería social basada en personas externas para obtener información. Debido a Ausencia de cláusulas sobre seguridad de la información en contratos con empelados y terceros causando Información comprometida afectando el principio de Confidencialidad.	Probable	Alto	4-Extrema
R28	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Legal por Usuario que Causar la divulgación de información crítica y / o sensible por parte de usuarios autorizados. Debido a Ausencia de matriz de roles y perfiles causando Información comprometida afectando el principio de Confidencialidad.	Probable	Muy Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R29	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo Legal y operativo por Administrador que Inserte malware especializado en los sistemas de información de la organización según las configuraciones del sistema. Debido a Ausencia de procedimientos de control para licenciamiento de software causando Información comprometida afectando todos los principios de seguridad.	Probable	Alto	4-Extrema
R30	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Administrador que Explotar sistemas de información mal configurados o no autorizados expuestos a Internet. Debido a Incorrecta asignación de privilegios causando Acciones no autorizadas afectando el principio de Confidencialidad.	Probable	Alto	4-Extrema
R31	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Administrador que Realice intentos de inicio de sesión por fuerza bruta / ataques de adivinación de contraseñas. Debido a contraseña insegura causando Información comprometida afectando el principio de Disponibilidad.	Casi Certeza	Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R32	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Legal y operativo por Administrador que Realizar ingeniería social basada en información privilegiada para obtener información. Debido a Ausencia de programas de capacitación y sensibilización en seguridad de la información causando Información comprometida afectando el principio de Confidencialidad.	Casi Certeza	Alto	4-Extrema
R33	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Operativo por Administrador que Compromiso de Funciones debido a Falta de segregación de funciones. Causando Compromiso de Funciones (Abuso de privilegios) afectando todos los principios de seguridad.	Probable	Alto	4-Extrema
R34	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo operativo por Administrador que Aprovechar las vulnerabilidades de los sistemas de información internos de la organización. Debido a Inexistencia de gestión y administración de vulnerabilidades sobre activos de TI causando Indisponibilidad afectando el principio de Disponibilidad.	Casi Certeza	Medio	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R35	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo operativo por Administrador que Provocar divulgación no autorizada y / o indisponibilidad al derramar información confidencial. Debido a Ausencia de responsabilidades de seguridad de la información causando Información comprometida afectando todos los principios de seguridad.	Casi Certeza	Medio	4-Extrema
R36	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Comunicaciones que Falla en componentes Tecnológicos debido a Falta o ausencia de mantenimiento o ausencia de programa de reemplazo de partes causando Funcionamiento deficiente de equipos afectando el principio de Disponibilidad.	Probable	Alto	4-Extrema
R37	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Comunicaciones que deterioro / destrucción de componentes tecnológicos debido a Ausencia de procedimiento de destrucción de medios causando Daños Físicos afectando el principio de Disponibilidad.	Medianamente Probable	Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R38	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Comunicaciones que Perdida de equipos debido a Robo de medios causando Información comprometida afectando el principio de Confidencialidad.	Medianamente Probable	Alto	4-Extrema
R39	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Fuente de alimentación que Falla de energía eléctrica debido a Ausencia o mal funcionamiento de una UPS. causando Indisponibilidad afectando el principio de Disponibilidad.	Medianamente Probable	Medio	3-Alta
R40	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Fuente de alimentación que Sobrecalentamiento de componentes debido a Mantenimiento insuficiente de la infraestructura para el servicio eléctrico. causando Indisponibilidad afectando el principio de Disponibilidad.	Medianamente Probable	Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R41	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo operativo por Red que Falla en el servicio de internet debido a Ausencia de un canal de internet alterno causando Indisponibilidad afectando el principio de Disponibilidad.	Medianamente Probable	Medio	3-Alta
R42	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo operativo por Red que Pérdida de servicios esenciales (Falla en el servicio de correo, falla en la página web, falla del servidor en la nube) debido a Ausencia de procesos y procedimientos contingentes para (infraestructura física, *hardware*, software, personas y proveedores) causando Indisponibilidad de servicios, afectando el principio de Disponibilidad.	Probable	Alto	4-Extrema
R43	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo operativo por Red que Corrupción de datos debido a Ausencia de copias de respaldo. Causando Información comprometida afectando todos los principios de seguridad.	Probable	Alto	4-Extrema

Cuadro 10. (Continuación)

Identificación del Riesgo		Análisis de Riesgos		
ID Riesgo	**Descripción del Riesgo**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
R44	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo operativo por Aplicación de uso general que Falla en los aplicativos desarrollados por mal funcionamiento de software debido a Ausencia de planes de contingencia causando Información comprometida afectando el principio de Integridad.	Medianamente Probable	Alto	4-Extrema
R45	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo operativo por Aplicación de uso general que Falla en los aplicativos desarrollados por código fuente debido a Ausencia de gestión de accesos causando Funcionamiento deficiente de software afectando todos los principios de seguridad.	Medianamente Probable	Alto	4-Extrema

Fuente: Autores de la Investigación.

- **Clasificación de incidentes e impacto**

Es importante para la definición de protocolos de gestión, y para facilitar el entendimiento por todas las partes del tipo de incidente que se ha producido, la unión, en una taxonomía común, de los tipos de incidentes a los que G0 S.A.S está expuesto.

El cuadro 11 se resume la taxonomía citada.

Cuadro 11. Clasificación de la taxonomía de los ciber-incidentes.

Clasificación/Taxonomía De Los Ciber incidentes		
Clasificación	**Tipo de Incidente**	**Descripción**
Contenido Abusivo	*Spam*	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito de odio	Contenido difamatorio o discriminatorio. Ej: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido Dañino	Sistema infectado	Sistema infectado con *malware*. Ej: Sistema, computadora o teléfono móvil infectado con un *rootkit*
	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante *malware* o sistemas infectados.
	Distribución de *malware*	Recurso usado para distribución de *malware*. Ej: recurso de una organización empleado para distribuir *malware*.
	Configuración de *malware*	Recurso que aloje ficheros de configuración de malware Ej: ataque de *webinjects* para troyano.
	Malware dominio DGA	Nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por *malware* para contactar con un servidor de Mando y Control (C&C).

Cuadro 11. (Continuación)

Clasificación/Taxonomía De Los Ciber incidentes		
Clasificación	**Tipo de Incidente**	**Descripción**
Obtención de Información	Escaneo de redes (*scanning*)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (*sniffing*)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas.
Intento de Intrusión	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: desbordamiento de *buffer*, puertas traseras, *cross site scripting* (XSS).
	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando *exploit* desconocido.
Intrusión	Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej: inyección SQL.
	Robo	Intrusión física. Ej: acceso no autorizado a Centro de Proceso de Datos.

Cuadro 11. (Continuación)

Clasificación/Taxonomía De Los Ciber incidentes		
Clasificación	**Tipo de Incidente**	**Descripción**
Disponibilidad	DoS (Denegación de servicio)	Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural.
Compromiso de la información	Acceso no autorizado a información	Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante *ransomware*.
	Pérdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.
Fraude	Uso no autorizado de recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.

Cuadro 11. (Continuación)

Clasificación/Taxonomía De Los Ciber incidentes		
Clasificación	**Tipo de Incidente**	**Descripción**
	Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: *Warez*.
	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	Criptografía débil	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador *DDoS*	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques *DDoS*. Ej: DNS *open-resolvers* o Servidores NTP con monitorización *monlist*.
	Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
	Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
	Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Otros	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.

Cuadro 11. (Continuación)

Clasificación/Taxonomía De Los Ciber incidentes		
Clasificación	**Tipo de Incidente**	**Descripción**
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.
	Ciberterrorismo	Uso de redes o sistemas de información con fines de carácter terrorista.
	Daños informáticos PIC	Borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

Fuente: Autores de la Investigación.

Continuando con la taxonomía de los tipos de incidentes comunes, en el cuadro 12, se clasifica el tipo de incidente y valorando su nivel de criticidad.

Cuadro 12. Nivel, clasificación y tipo de incidente.

Nivel	Clasificación	Tipo de Incidente
Crítico	Otros	APT
		Ciberterrorismo
		Daños informáticos PIC
Muy Alto	Código dañino	Distribución de *malware*
		Configuración de *malware*
	Intento de intrusión	Ataque desconocido
	Intrusión	Robo
	Disponibilidad	Sabotaje
		Interrupciones

Cuadro 12. (Continuación)

Nivel	Clasificación	Tipo de Incidente
Alto	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Sistema infectado
		Servidor C&C (Mando y Control)
		Malware dominio DGA
	Intento de intrusión	Compromiso de aplicaciones
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos
	Fraude	*Phishing*
Medio	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social
	Intento de intrusión	Explotación de vulnerabilidades conocidas
		Intento de acceso con vulneración de credenciales
	Intrusión	Compromiso de cuentas con privilegios
	Fraude	Uso no autorizado de recursos
		Derechos de autor
		Suplantación
	Vulnerable	Criptografía débil
		Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información
		Sistema vulnerable

Cuadro 12. (Continuación)

Nivel	Clasificación	Tipo de Incidente
Bajo	Contenido abusivo	Spam
	Obtención de información	Escaneo de redes (*scanning*)
		Análisis de paquetes (*sniffing*)
	Intrusión	Compromiso de cuenta sin privilegio
	Otros	Otros

Fuente: Autores de la Investigación.

7.3.3 Tratamiento del Riesgo. En este bloque, una vez identificado los escenarios de riesgos descritos anteriormente, se procede con el tratamiento de los mismos que consiste en definir la manera en la que se implementarán las opciones de manejo del riesgo con el objetivo de lograr que se encuentre en el Nivel de Riesgo Aceptable (NRA) estableciendo un plan de acción para el tratamiento de los mismos, y buscando disminuir el impacto del riesgo generado por la materialización sobre la infraestructura de la organización

La metodología de gestión de riesgos busca que el riesgo residual se encuentre siempre dentro del Nivel de Riesgo Aceptable (NRA), es decir, el nivel de riesgo con el que el negocio tiene confianza para avanzar en sus tareas, procesos, proyectos, iniciativas o servicios, teniendo en cuenta la siguiente gestión de los riesgos:

- **Evitar**: Se decide no seguir adelante con la actividad que genera el riesgo.

- **Transferir**: Involucrar a terceras partes para compartir el riesgo, mediante contratos, compras de seguros, entre otros.

- **Mitigar**: Implementación de controles para reducir la probabilidad de ocurrencia o minimizar su impacto.

- **Aceptar**: Convivir con el riesgo existente, por alguna de las siguientes razones: o Si por una justificación de negocio se decide aceptar un riesgo por fuera del NRA, se debe proceder con la firma de carta de aceptación de riesgos por parte del dueño del riesgo.

En el caso de los riesgos positivos (oportunidades), las opciones de tratamiento serán las siguientes:

- **Explotar**: Emprender acciones para asegurarse que la oportunidad relacionada se concrete, eliminando las incertidumbres asociadas al riesgo positivo.

- **Transferir**: Compartir el riesgo con una o varias partes (por ejemplo, a través de contratos y alianzas), que estén mejor capacitadas o en mejor posición para capturar la oportunidad.

- **Mejorar**: Acometer acciones que aumenten la probabilidad de ocurrencia y/o el impacto positivo de una oportunidad.

- **Aceptar**: Se toma el beneficio derivado de la oportunidad si se presenta, pero sin llevar a cabo acciones proactivas para que se presente. No se busca de manera activa tomar ventaja de la oportunidad.

Una vez identificado y ubicado el nivel de riesgo, se determina su tratamiento el cual se describe de la siguiente manera:

Para la implementación de controles, se realiza sobre los riesgos más críticos encontrados en la empresa G0 S.A.S, aquellos que son inaceptables para la alta gerencia y se deben tratar de inmediato. Debido a que G0 S.A.S no tiene implementado un Gobierno de Seguridad de la Información, en una primera Fase, Se recomienda seguir los siguientes pasos que permita mitigar el riesgo y así decidir en la toma de decisiones.

1. Deben establecer una estructura de gobierno para la seguridad de la Información
2. Implementar un sistema de gestión de continuidad que permita respaldar sus procesos y servicios críticos.
3. Establecer políticas, procesos y procedimientos que apoyen la seguridad de la información.
4. Implementar controles criptográficos.
5. Diseñar una matriz de roles y perfiles.
6. Implementar un sistema de Clasificación de información.
7. Implementar procedimientos de Tecnología y documentarlos.
8. Hacer análisis de Vulnerabilidades y gestionarlas.
9. Implementar un sistema de Gestión de incidentes de seguridad de la información.
10. Implementación de procesos de gestión de accesos.

7.3.3.1 Plan de Tratamiento. Dado que la empresa G0 S.A.S carece de implantación de controles en la mayoría de sus procesos, como análisis del informe, se toma como referencia la evaluación del riesgo residual, el cual se evaluará para proceso para el tratamiento del riesgo, sugiriendo los controles más adecuados para mitigar su riesgo.

- **Tipo de control**: se debe determinar si son controles preventivos, correctivo o detectivo.

- **Responsable**: Se debe tener a cargo un responsable o un área encargada para la implementación de los controles y este debe estar relacionado con su perfil y funciones dentro de la organización.

- **Frecuencia**: se debe establecer con qué periodo de tiempo el control debe ser monitoreado

    - Diario
    - Semanal
    - Mensual
    - Anual
    - En tiempo Real

En la figura 27, se propone a la empresa G0 S.A.S el siguiente formato para el tratamiento del riesgo.

Figura 27. Formato de tratamiento de riesgo.

IMPLEMENTACION DE CONTROLES					PLANES DE TRATAMIENTO		
DESCRIPCIÓN	EVIDENCIA	FRECUENCIA	RESPONSABLE DE SU EJECUCIÓN	TIPO (C, D, P)	FECHA INICIO	FECHA LIMITE	FECHA ÚLTIMO SEGUIMIENTO

Fuente: Autores de la Investigación.

7.3.3.1 Riesgo Residual. Es el que subsiste con la aplicación de los controles existentes, donde cada control puede modificar la probabilidad de ocurrencia, restringiendo las opciones para que la amenaza se materialice o impulsando las oportunidades, o reducir el impacto en caso de que se materialice el riesgo.

En el cuadro 13, se muestra el riesgo evaluado asociado al control de tratamiento propuesto.

Cuadro 13. Tratamiento del riesgo.

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R1	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Externo que Realiza un rastreo de redes expuestas. Debido a Ausencia de mecanismos de protección perimetral y de redes. Causando Información comprometida afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Protección de Límites". SC-7. Monitorear y controlar las comunicaciones en las interfaces administradas externas e internas en el sistema. La red debe estar protegida mediante seguridad perimetral como Firewall, ips, etc.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R2	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo Legal y operativo por Agente Externo que Recopila información utilizando el descubrimiento de código abierto de información organizacional. Debido a Modificación de software (no autorizado) causando Funcionamiento deficiente de software afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Software de Código Abierto". CM-10 (1). Utilice el software y la documentación asociada protegido por acuerdos de licencias de software y las leyes de derechos de autor para controlar la copia y distribución de este. Esta protección se realiza mediante gestión de accesos evitando configuraciones no autorizadas.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R3	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y Operativo por Agente Externo que Realiza reconocimiento y vigilancia de organizaciones específicas. Debido a Insuficiente monitoreo. Causando Divulgación de información afectando el principio de Confidencialidad.	3-Alta	3-Alta	Preventivo	Se relaciona con la implementación de control, "Monitoreo Continuo". CA-7. Desarrollar una estrategia de monitoreo continuo a nivel del sistema e implementar un seguimiento de acuerdo con la estrategia de monitoreo continuo a nivel de la organización.
R4	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal, Operativo y Económico por Agente Externo que Crea ataques de phishing. para Revelación de Información causando Información comprometida afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Protección de Límites". SC-7. Monitorear y controlar las comunicaciones en las interfaces administradas externas e internas en el sistema. La red debe estar protegida mediante seguridad perimetral como Firewall, ips, etc.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R5	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Externo que Crea ataques específicamente basados en el entorno de tecnología de la información implementada. Debido a Ausencia de procesos y procedimientos contingentes para (infraestructura física, *hardware*, software, personas y proveedores) causando Pérdida de servicios esenciales afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Aislamiento de Procesos". SC-39. Mantener un dominio de ejecución separado para cada proceso del sistema en ejecución, se debe garantizar que cada área separe sus procedimientos y los documente.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R6	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal, Operativo y Económico por Agente Externo que Crear un sitio web falsificado o falso. para Robo de Información causando Información comprometida afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Protección de Límites". SC-7. Monitorear y controlar las comunicaciones en las interfaces administradas externas e internas en el sistema. La red debe estar protegida mediante seguridad perimetral como Firewall, ips, etc.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R7	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal por Agente Externo que Elaborar certificados falsificados. Debido a Ausencia de mecanismos de verificación de integridad: hashing firmas digitales, monitoreo de la integridad de archivos. Causando Modificación indebida afectando el principio de Integridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "remoción, Enmascaramiento, Cifrado, Hash O Reemplazo de Identificadores Directos". SI-19 (4). Emplear algoritmos que requieren el uso de una clave, o un código de autenticación de mensajes basado en hash. usar una clave diferente para cada identificador proporciona un mayor grado de seguridad y privacidad, para verificación de integridad.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R8	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal y operativo por Agente Externo que Causar pérdida de integridad al crear, eliminar y / o modificar datos en sistemas de información de acceso público. Debido a Ausencia de procedimientos para el control de la información causando Información comprometida afectando el principio de Integridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Políticas y procedimientos". SC-1. Desarrollar, documentar y difundir a personal definidos por la organización o establecer roles, procedimientos para facilitar la implementación de la política de protección del sistema y las comunicaciones, designar un funcionario definido por la organización para gestionar estas tareas.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R9	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal y operativo por Agente Externo que Causar pérdida de integridad al contaminar o corromper datos críticos. Debido a Ausencia de registro del acceso de lectura a los archivos. causando Información comprometida afectando el principio de Disponibilidad.	4-Extrema	2-Moderada	Preventivo	Se relaciona con la implementación de control, "Privilegios Mínimos". AC-6. Emplee el principio de privilegio mínimo, permitiendo solo los accesos autorizados para los usuarios (o procesos que actúan en nombre de los usuarios) que son necesarios para realizar las tareas organizativas asignadas.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R10	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y Operativo por Agente Externo que Realizar ataques de interceptación de comunicaciones. Debido a Líneas de comunicación desprotegidas causando Información comprometida afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control," Herramientas y mecanismos automatizados para el análisis en tiempo real". SI-4 (2). Emplee herramientas y mecanismos automatizados para respaldar el análisis de eventos casi en tiempo real, Supervise el sistema para detectar: Conexiones locales, de red y remotas no autorizadas.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R11	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal, Operativo y Económico por Agente Externo que Realice ataques de eliminación de datos en un entorno de nube. Debido a Ausencia de copias de respaldo. Causando Indisponibilidad afectando el principio de Disponibilidad.	4-Extrema	4-Extrema	Correctivo	Se relaciona con la implementación de control, "Sitios de Procesamiento Alternativo". CP-7. Establecer un sitio de procesamiento alternativo, incluidos los acuerdos necesarios para permitir la transferencia y reanudación de operaciones del sistema definidas por la organización para funciones esenciales de misión y de negocios dentro de un período de tiempo definido por la organización coherente con el tiempo de recuperación y los objetivos del punto de recuperación cuando las capacidades de procesamiento primario no están disponibles.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R12	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal, Operativo y Económico por Agente Externo que Llevar a cabo un secuestro de sesiones externo. Debido a Ausencia de mecanismos para identificación y autenticación de usuarios causando Información comprometida afectando todos los principios de seguridad.	3-Alta	2-Moderada	Preventivo	Se relaciona con la implementación de control, "gestión dinámica de privilegios". AC-2 (6). Implementar capacidades de gestión de privilegios dinámicos definidas por la organización como el control de acceso basado en atributos. Si bien las identidades de los usuarios permanecen relativamente constantes a lo largo del tiempo, los privilegios de los usuarios generalmente cambian con mayor frecuencia en función de las necesidades operativas de las organizaciones.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R13	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Operativo por Agente Externo que Obtener acceso no autorizado. Debido a Ausencia de una política de control de acceso. Causando Accesos no autorizados a sistemas de información afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "política y Procedimientos". AC-1. Desarrollar, documentar y difundir a personal o roles definidos por la organización, abordar el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la gestión para su cumplimiento, de igual manera, procedimientos para facilitar la implementación de la política de control de acceso y los controles de acceso asociados.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R14	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Externo que Obtenga información confidencial a través del rastreo de redes externas. Debido a Ausencia de mecanismos de protección perimetral y de redes causando Información comprometida afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Protección de Límites". SC-7. Monitorear y controlar las comunicaciones en las interfaces administradas externas e internas en el sistema. La red debe estar protegida mediante seguridad perimetral como Firewall, ips, etc.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R15	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Externo que Explotar VPNs. debido a Ausencia de cifrado causando Divulgación de información afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Acceso Remoto". AC-17. Establecer y documentar restricciones de uso, requisitos de configuración / conexión y orientación de implementación para cada tipo de acceso remoto permitido, Mecanismos que autorice cada tipo de acceso remoto al sistema antes de permitir tales conexiones.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R16	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y operativo por Agente Interno que Entregue malware conocido a los sistemas de información internos de la organización (por ejemplo, virus por correo electrónico). debido a Ausencia de procedimientos de control para licenciamiento de software causando Corrupción de datos afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Protección de códigos maliciosos". SI-3. Realice análisis periódicos del sistema y escaneos en tiempo real de archivos de fuentes externas en puntos de entrada y salida de la red, a medida que los archivos se descargan, abren o ejecutan de acuerdo con la política de la organización con una frecuencia definida por la organización.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R17	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Agente Interno que Aprovechar las vulnerabilidades de los sistemas de información internos de la organización. Debido a Inexistencia de gestión y administración de vulnerabilidades sobre activos de TI causando Información comprometida afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Seguimiento y Escaneo de Vulnerabilidad". RA-5. Monitorear y escanear en busca de vulnerabilidades en el sistema y aplicaciones alojadas en una frecuencia definida por la organización y / o aleatoriamente de acuerdo con el proceso definido por la organización, identificar y notificar nuevas vulnerabilidades que puedan afectar al sistema, empleando herramientas de monitoreo de vulnerabilidades que incluyan la capacidad de actualizar fácilmente las vulnerabilidades que se analizarán.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R18	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo Operativo por Agente Interno que Comprometer el software de los sistemas de información críticos de la organización. Debido a Especificaciones incompletas, incorrectas o no documentadas para desarrolladores causando Funcionamiento deficiente de software afectando el principio de Disponibilidad.	4-Extrema	4-Extrema	Detectivo	Se relaciona con la implementación de control, "Ciclo De Vida De Desarrollo De Sistemas". SA-3. Adquirir, desarrollar y administrar el ciclo de vida de desarrollo del sistema definido por la organización que incorpora consideraciones de seguridad y privacidad de la información, definir y documentar a las personas que tienen las funciones y responsabilidades en materia de seguridad y privacidad de la información a lo largo del ciclo de vida del desarrollo del sistema.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R19	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal por Agente Interno que Realizar ingeniería social basada en información privilegiada para obtener información. Debido a Ausencia de programas de concientización causando Información comprometida afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "ingeniería Social y minería". AT-2 (3). Brindar capacitación y concientización para reconocer y reportar instancias potenciales y reales de ingeniería y minería sociales. La ingeniería social es un intento de engañar a una persona para que revele información o emprenda una acción que pueda usarse para violar, comprometer o afectar negativamente un sistema, entretanto, la minería social es un intento de recopilar información sobre la organización que se puede utilizar para respaldar futuros ataques.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R20	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo Operativo por Agente Interno que Causar deterioro / destrucción de componentes y funciones críticos del sistema de información. Debido a Ausencia de planes de recuperación tecnológico causando Indisponibilidad en la entrega de productos y servicios afectando el principio de Disponibilidad.	4-Extrema	4-Extrema	Correctivo	Se relaciona con la implementación de control, "Plan de Contingencia". CP-2. Desarrolle un plan de contingencia para el sistema que proporcione objetivos de recuperación, prioridades de restauración y métricas, incorporando las lecciones aprendidas de las pruebas, la capacitación o las actividades de contingencia reales del plan de contingencia, coordinar las actividades de planificación de contingencias con las actividades de manejo de incidentes.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R21	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Legal por Agente Interno que Causar la divulgación de información crítica y / o sensible por parte de usuarios autorizados. Debido a Ausencia de responsabilidades de seguridad de la información causando Información comprometida afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "política y Procedimientos". AC-1. Desarrollar, documentar y difundir a personal o roles definidos por la organización, abordar el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la gestión para su cumplimiento, de igual manera, procedimientos para facilitar la implementación de la política de control de acceso y los controles de acceso asociados.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R22	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y operativo por Agente Interno que Obtenga acceso no autorizado. Debido a ausencia de control de acceso (físico y lógico) causando Accesos no autorizados a sistemas de información afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "política y Procedimientos". AC-1. Desarrollar, documentar y difundir a personal o roles definidos por la organización, abordar el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la gestión para su cumplimiento, de igual manera, procedimientos para facilitar la implementación de la política de control de acceso y los controles de acceso asociados.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R23	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal por Agente Interno que Obtenga información / datos sensibles de sistemas de información de acceso público. Debido a Ausencia de clasificación de información causando Información comprometida afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Contenido de Acceso Público". AC-22. Capacitar a las personas autorizadas para garantizar que la información de acceso público no contenga información privada, por otra parte, revisar el contenido propuesto de la información antes de publicarlo en el sistema de acceso público para asegurarse de que no se incluya información no pública.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R24	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Legal y operativo por Agente Interno que Obtener información robando o recolectando sistemas / componentes de información de manera oportunista. Debido a Ausencia de gobierno (Estructura organizacional, políticas, procesos y procedimientos en seguridad de la Información) causando Información comprometida afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Órgano de Gobierno de Datos". PM-23. Establecer un organismo de gobernanza de datos compuesto por roles definidos por la organización con responsabilidades definidas por la organización.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R25	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Legal y operativo por Usuario que Inserte malware dirigido en los sistemas de información organizacional y los componentes del sistema de información. Debido a Uso no controlado de software descargado causando Funcionamiento deficiente de software afectando el principio de Integridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Protección de códigos maliciosos". SI-3. Realice análisis periódicos del sistema y escaneos en tiempo real de archivos de fuentes externas en puntos de entrada y salida de la red, a medida que los archivos se descargan, abren o ejecutan de acuerdo con la política de la organización con una frecuencia definida por la organización.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R26	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo Operativo por Usuario que Comprometer los sistemas de información críticos a través del acceso físico. Debido a ausencia de control de acceso físico causando Accesos no autorizados a sistemas de información afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Control De Acceso Físico". PE-3. Controlar el acceso a las áreas dentro de la instalación designadas como de acceso público mediante la implementación de controles de acceso físico definidos por la organización, por otra parte, proteger las llaves, combinaciones y otros dispositivos de acceso físico.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R27	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Legal por Usuario que Realizar ingeniería social basada en personas externas para obtener información. Debido a Ausencia de cláusulas sobre seguridad de la información en contratos con empelados y terceros causando Información comprometida afectando el principio de Confidencialidad.	4-Extrema	2-Moderada	Preventivo	Se relaciona con la implementación de control, "ingeniería Social y minería". AT-2 (3). Brindar capacitación y concientización para reconocer y reportar instancias potenciales y reales de ingeniería social y minería social. La ingeniería social es un intento de engañar a una persona para que revele información o emprenda una acción que pueda usarse para violar, comprometer o afectar negativamente un sistema, entretanto, la minería social es un intento de recopilar información sobre la organización que se puede utilizar para respaldar futuros ataques.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R28	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Legal por Usuario que Causar la divulgación de información crítica y / o sensible por parte de usuarios autorizados. Debido a Ausencia de matriz de roles y perfiles causando Información comprometida afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Uso De Perfiles Definidos". IA-8 (4). Identificar y autenticar de forma única a los usuarios o procesos no organizativos que actúen en nombre de usuarios no organizativos, cumplir con los perfiles para la gestión de identidad definidos.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R29	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo Legal y operativo por Administrador que Inserte malware especializado en los sistemas de información de la organización según las configuraciones del sistema. Debido a Ausencia de procedimientos de control para licenciamiento de software causando Información comprometida afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Actualizaciones y parches de Software". MA-3 (6). Aprobar, controlar y monitorear el uso de herramientas de mantenimiento del sistema, inspeccionar las herramientas de mantenimiento para asegurarse de que estén instaladas las últimas actualizaciones y parches de software.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R30	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Administrador que Explotar sistemas de información mal configurados o no autorizados expuestos a Internet. Debido a Incorrecta asignación de privilegios causando Acciones no autorizadas afectando el principio de Confidencialidad.	4-Extrema	2-Moderada	Preventivo	Se relaciona con la implementación de control, "gestión dinámica de privilegios". AC-2-(6). Implementar capacidades de gestión de privilegios dinámicos definidas por la organización como el control de acceso basado en atributos. Si bien las identidades de los usuarios permanecen relativamente constantes a lo largo del tiempo, los privilegios de los usuarios generalmente cambian con mayor frecuencia en función de las necesidades operativas de las organizaciones.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R31	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo Operativo por Administrador que Realice intentos de inicio de sesión por fuerza bruta / ataques de adivinación de contraseñas. Debido a contraseña insegura causando Información comprometida afectando el principio de Disponibilidad.	4-Extrema	2-Moderada	Preventivo	Se relaciona con la implementación de control, "Administradores de Contraseñas". IA-5 (18). Emplear administradores de contraseñas definidos por la organización para generar y administrar contraseñas y proteger las contraseñas con controles definidos por la organización.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R32	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Legal y operativo por Administrador que Realizar ingeniería social basada en información privilegiada para obtener información. Debido a Ausencia de programas de capacitación y sensibilización en seguridad de la información causando Información comprometida afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "ingeniería Social y minería". AT-2 (3). Brindar capacitación y concientización para reconocer y reportar instancias potenciales y reales de ingeniería social y minería social. La ingeniería social es un intento de engañar a una persona para que revele información o emprenda una acción que pueda usarse para violar, comprometer o afectar negativamente un sistema, entretanto, la minería social es un intento de recopilar información sobre la organización que se puede utilizar para respaldar futuros ataques.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R33	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo Operativo por Administrador que Compromiso de Funciones debido a Falta de segregación de funciones. Causando Compromiso de Funciones (Abuso de privilegios) afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Control de Acceso Basado en Funciones". AC-3 (7). Aplicar una política de control de acceso basada en roles definidos por la organización y usuarios autorizados para asumir dichos roles.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R34	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo operativo por Administrador que Aprovechar las vulnerabilidades de los sistemas de información internos de la organización. Debido a Inexistencia de gestión y administración de vulnerabilidades sobre activos de TI causando Indisponibilidad afectando el principio de Disponibilidad.	4-Extrema	4-Extrema	Detectivo	Se relaciona con la implementación de control, "Plan de acción e hitos". CA-5. Desarrollar un plan de acción e hitos para que el sistema documente las acciones de remediación planificadas de la organización para corregir las debilidades o deficiencias observadas durante la evaluación de los controles y para reducir o eliminar las vulnerabilidades conocidas en el sistema.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R35	RIESGO de Seguridad de la Información de categoría de activo: Personas, con una afectación de tipo operativo por Administrador que Provocar divulgación no autorizada y / o indisponibilidad al derramar información confidencial. Debido a Ausencia de responsabilidades de seguridad de la información causando Información comprometida afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "política y Procedimientos". AC-1. Desarrollar, documentar y difundir a personal o roles definidos por la organización, abordar el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la gestión para su cumplimiento, de igual manera, procedimientos para facilitar la implementación de la política de control de acceso y los controles de acceso asociados.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R36	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Comunicaciones que Falla en componentes Tecnológicos debido a Falta o ausencia de mantenimiento o Ausencia de programa de reemplazo de partes causando Funcionamiento deficiente de equipos afectando el principio de Disponibilidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Actividades de Mantenimiento Automatizado". MA-2 (2). Programar, realizar y documentar acciones de mantenimiento, reparación y reemplazo del sistema que utiliza mecanismos automatizados definidos por la organización.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R37	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Comunicaciones que deterioro / destrucción de componentes tecnológicos debido a Ausencia de procedimiento de destrucción de medios causando Daños Físicos afectando el principio de Disponibilidad.	4-Extrema	4-Extrema	Correctivo	Se relaciona con la implementación de control, "Plan de Contingencia". CP-2. Desarrolle un plan de contingencia para el sistema que proporcione objetivos de recuperación, prioridades de restauración y métricas, incorporando las lecciones aprendidas de las pruebas, la capacitación o las actividades de contingencia reales del plan de contingencia, coordinar las actividades de planificación de contingencias con las actividades de manejo de incidentes.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R38	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Comunicaciones que Perdida de equipos debido a Robo de medios causando Información comprometida afectando el principio de Confidencialidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Carcasas con bloqueo". PE-3 (4). Utilice carcasas físicas con cerradura para proteger del acceso físico no autorizado.
R39	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Fuente de alimentación que Falla de energía eléctrica debido a Ausencia o mal funcionamiento de una UPS. causando Indisponibilidad afectando el principio de Disponibilidad.	3-Alta	3-Alta	Preventivo	Se relaciona con la implementación de control, "Fuente de alimentación Alternativa". PE-11 (1). Proporcione una fuente de alimentación alternativa para el sistema que está activado ya sea por medio manual o automáticamente y esto pueda mantener la capacidad operativa mínima requerida en caso de una pérdida prolongada de la fuente de energía primaria.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R40	RIESGO de Seguridad de la Información de categoría de activo: *Hardware*, con una afectación de tipo operativo por Fuente de alimentación que Sobrecalentamiento de componentes debido a Mantenimiento insuficiente de la infraestructura para el servicio eléctrico. causando Indisponibilidad afectando el principio de Disponibilidad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Actividades de Mantenimiento Automatizado". MA-2 (2). Programar, realizar y documentar acciones de mantenimiento, reparación y reemplazo del sistema que utiliza mecanismos automatizados definidos por la organización.
R41	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo operativo por Red que Falla en el servicio de internet debido a Ausencia de un canal de internet alterno causando Indisponibilidad afectando el principio de Disponibilidad.	3-Alta	3-Alta	Correctivo	Se relaciona con la implementación de control, "Puntos únicos de Falla". CP-8 (2). Obtenga servicios de telecomunicaciones alternativos para reducir la probabilidad de compartir un solo punto de falla con los servicios de telecomunicaciones primarios.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R42	RIESGO de Seguridad de la Información de categoría de activo: Comunicaciones, con una afectación de tipo operativo por Red que Pérdida de servicios esenciales (Falla en el servicio de correo, falla en la página web, falla del servidor en la nube) debido a Ausencia de procesos y procedimientos contingentes para (infraestructura física, *hardware*, software, personas y proveedores) causando Indisponibilidad de servicios, afectando el principio de Disponibilidad.	4-Extrema	4-Extrema	Detectivo	Se relaciona con la implementación de control, "Ciclo De Vida De Desarrollo De Sistemas". SA-3. Adquirir, desarrollar y administrar el ciclo de vida de desarrollo del sistema definido por la organización que incorpora consideraciones de seguridad y privacidad de la información, definir y documentar a las personas que tienen las funciones y responsabilidades en materia de seguridad y privacidad de la información a lo largo del ciclo de vida del desarrollo del sistema.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R43	RIESGO de Seguridad de la Información de categoría de activo: Información, con una afectación de tipo operativo por Red que Corrupción de datos debido a Ausencia de copias de respaldo. Causando Información comprometida afectando todos los principios de seguridad.	4-Extrema	3-Alta	Correctivo	Se relaciona con la implementación de control, "Sitios de Almacenamiento Alternativo". CP-6. Establecer un sitio de almacenamiento alternativo, incluidos los acuerdos necesarios para permitir el almacenamiento y la recuperación de la información de respaldo del sistema y asegúrese de que este sitio proporcione controles equivalentes a los del sitio principal.

Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R44	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo operativo por Aplicación de uso general que Falla en los aplicativos desarrollados por mal funcionamiento de software debido a Ausencia de planes de contingencia causando Información comprometida afectando el principio de Integridad.	4-Extrema	4-Extrema	Correctivo	Se relaciona con la implementación de control, "Plan de Contingencia". CP-2. Para establecer los procedimientos y mecanismos para preservar la seguridad de la información almacenada en los aplicativos y así garantizar la continuidad de las funciones de la empresa G0 S.A.S.

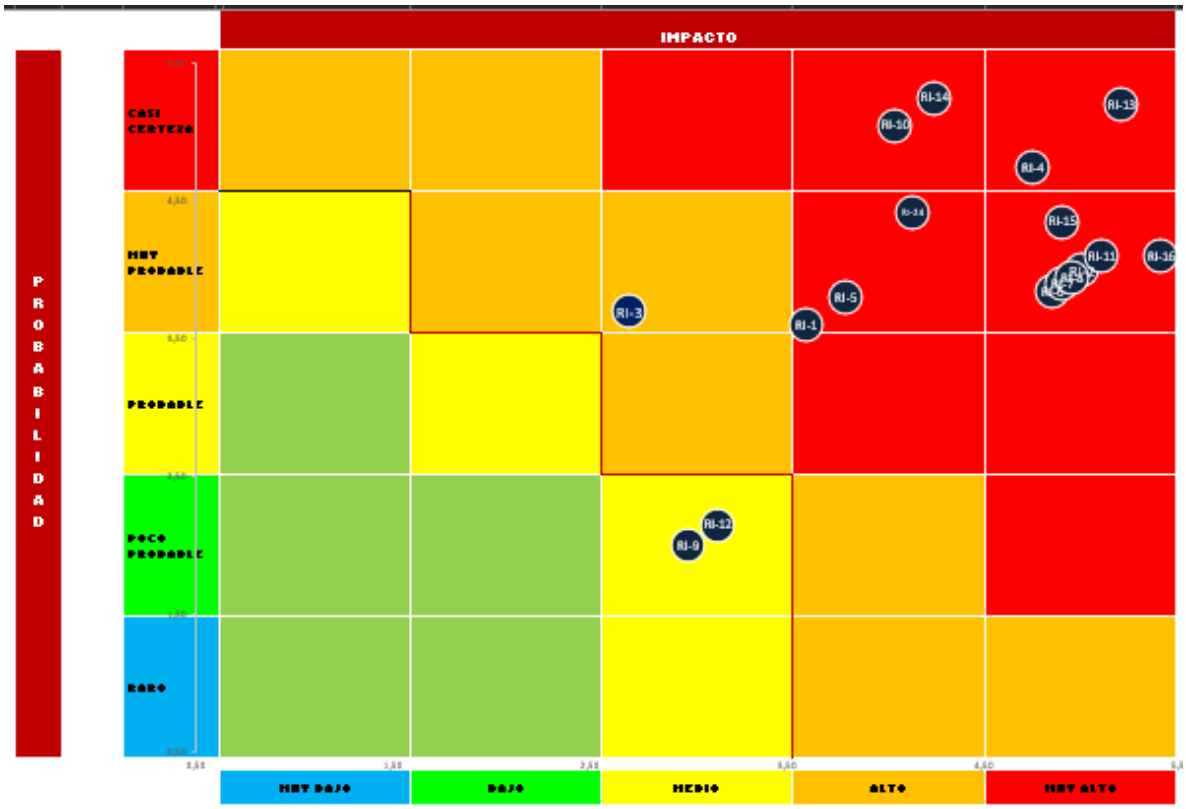
Cuadro 13. (Continuación)

ID Riesgo	Descripción del Riesgo	Zona de Riesgo Inherente	Zona de Riesgo Residual	Tipo de Control	Control de Tratamiento
R45	RIESGO de Seguridad de la Información de categoría de activo: Software, con una afectación de tipo operativo por Aplicación de uso general que Falla en los aplicativos desarrollados por código fuente debido a Ausencia de gestión de accesos causando Funcionamiento deficiente de software afectando todos los principios de seguridad.	4-Extrema	4-Extrema	Preventivo	Se relaciona con la implementación de control, "Decisiones de Control de Acceso". AC-24. Establecer procedimientos, implementar mecanismos para asegurar decisiones de control de acceso definidas por la organización.

Fuente: Autores de la Investigación.

En la figura 28 se muestra en un mapa de calor, los 45 riesgos ubicados en la zona de calor valorados en la matriz. Aquí se evidencia que, por la carencia de controles, estos están en un nivel inaceptable. Este resultado hace parte del informe presentado a la alta gerencia como parte del análisis de la evaluación del riesgo.

Figura 28. Mapa de claro de riesgos.



Fuente: Autores de la Investigación.

8. SUGERENCIA DE CONTROLES BASADOS EN CSF NIST SP800-53 PARA LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA TECNOLÓGICA DE G0 S.A.S

8.1 INTRODUCCIÓN

El objetivo de este apartado es recomendar una serie de controles, organizados en diferentes familias, que faciliten el seguimiento operativo del Riesgo Tecnológico de los aplicativos críticos de G0 S.A.S.

8.1.1 Contexto. Un desafío importante para las organizaciones es seleccionar un conjunto de controles de seguridad y privacidad que pueda proteger su misión y funciones comerciales, proporcionando la capacidad para administrar la seguridad y privacidad.

Los controles seleccionados, si se implementan correctamente y se determina que son efectivos, servirán para cumplir con los requisitos de seguridad y privacidad definidos por las leyes y normativas aplicables en Colombia, con foco en los procesos críticos que la operación de G0 S.A.S requiere.

No existe un conjunto único de controles que aborde toda la seguridad o la privacidad que siempre sean aplicables. Por ello, elegir los controles más apropiados para G0 S.A.S, aquellos que permitan gestionar adecuadamente el riesgo tecnológico, implica una comprensión fundamental de la misión de la organización y las prioridades comerciales, para entender cómo debe operar la tecnología dentro de la cadena de valor de la organización, lo que a su vez requiere de la estrecha colaboración con las partes interesadas.

Con ese entendimiento, G0 S.A.S puede definir cómo asegurar de manera eficiente y rentable la confidencialidad, integridad y disponibilidad de la información y de sus sistemas organizacionales, así como la privacidad de las personas en el contexto de apoyo a la misión y las funciones comerciales.

Tomando como base definiciones del NIST, que ya han sido utilizadas anteriormente en este proyecto, servirá de base para las definiciones de Ciberseguridad dentro de los procesos críticos. Para ello, se han seleccionado y priorizado los controles a los que se debería formalizar y dar seguimiento periódico, tanto en su cumplimiento, como en los resultados obtenidos.

8.1.2 Selección de controles. Las políticas y procedimientos de Seguridad de la Información son responsables de proteger la información y los sistemas contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados (Es decir, actividad o comportamiento no autorizado del sistema) con el fin de proporcionar confidencialidad, integridad y disponibilidad. Por otro lado, las medidas relacionadas con privacidad (Alineadas con la Ley 1581) son responsables de administrar los riesgos para las personas relacionados con la creación, recopilación, uso, procesamiento, difusión, almacenamiento, mantenimiento, divulgación o eliminación (Aspectos denominados colectivamente "Procesamiento") de información de identificación personal.

Cuando un sistema procesa información personal, las políticas de Seguridad de la Información y Privacidad tienen la responsabilidad compartida de gestionar los impactos para las personas que surgen de los riesgos de seguridad, por lo que en ambas gestiones se debe considerar cómo determinar la categorización de seguridad, y con base en ello, la selección y adaptación de los controles que se aplicarán, determinando la criticidad y sensibilidad de la información que deben procesar, almacenar o transmitir dichos sistemas. Los resultados de la categorización de seguridad ayudan a guiar e informar la selección de líneas de base de control de seguridad para proteger los sistemas y la información.

Los controles seleccionados para los sistemas son proporcionales al impacto potencial en las operaciones (Calculado en los BIAs) si hay una pérdida de confidencialidad, integridad o una falta de disponibilidad. Esto requiere que las organizaciones clasifiquen los sistemas como de bajo impacto, impacto moderado o alto impacto para los objetivos de seguridad declarados de confidencialidad, integridad y disponibilidad.

Dado que los valores de impacto potenciales para la confidencialidad, integridad y disponibilidad pueden no ser siempre los mismos para un sistema en particular, el nivel de impacto del sistema se utiliza con el propósito expreso de seleccionar los controles de seguridad aplicables.

En el cuadro 14, se detallan los diferentes controles aplicables, definidos dentro del núcleo del marco básico (*framework core*) agrupados por familias para facilitar su entendimiento y selección.

Cuadro 14.Controles de tratamiento.

Función	ID Control	Tipo de Control	Nivel 1	Nivel 2	Control
Identificar	RA-5	Preventivo	Evaluación riesgos	Seguimiento y escaneo de Vulnerabilidad	Seguimiento y Escaneo de Vulnerabilidad
Identificar	IA-5 (18)	Preventivo	Identificación y autenticación	Gestión de Autenticación	Administradores de Contraseñas
Identificar	IA-8 (4)	Preventivo	Identificación y Autenticación	Identificación y autenticación (usuarios no organizativos)	Uso De Perfiles Definidos
Proteger	AT-2 (3)	Preventivo	Conciencia y Capacitación	Capacitación y Sensibilización	Ingeniería Social y Minería
Proteger	AC-1	Preventivo	Control de Acceso	Política y Procedimientos	Política y Procedimientos
Proteger	AC-2-(6)	Preventivo	Control de Acceso	Gestión de Cuentas	Gestión dinámica de Privilegios
Proteger	AC-3 (7)	Preventivo	Control de Acceso	Cumplimiento de Acceso	Control de acceso basado en Funciones
Proteger	AC-6	Preventivo	Control de Acceso	Privilegios Mínimos	Privilegios Mínimos
Proteger	AC-17	Preventivo	Control de Acceso	Acceso Remoto	Acceso Remoto
Proteger	AC-22	Preventivo	Control de Acceso	Contenido de Acceso Publico	Contenido de Acceso Publico
Proteger	AC-24	Preventivo	Control de Acceso	Decisiones de control de Acceso	Decisiones de control de Acceso
Proteger	CM-10 (1)	Preventivo	Gestión de la Configuración	Restricciones de Uso de Software	Software de Código Abierto

Cuadro 14. (Continuación)

Función	ID Control	Tipo de Control	Nivel 1	Nivel 2	Control
Proteger	SI-3	Preventivo	Integridad Sistemas	Protección de códigos Maliciosos	Protección de códigos Maliciosos
Proteger	SI-4 (2)	Preventivo	Integridad Sistemas	Monitoreo del sistema	Herramientas y mecanismos automatizados para el análisis en tiempo real
Proteger	SI-19 (4)	Preventivo	Integridad Sistemas	Desidentificación	Enmascaramiento, Cifrado, Hash O Reemplazo De Identificadores Directos
Proteger	MA-2 (2)	Preventivo	Mantenimiento	Mantenimiento Controlado	Actividades de Mantenimiento Automatizado
Proteger	MA-3 (6)	Preventivo	Mantenimiento	Herramientas de Mantenimiento	Actualizaciones y parches de Software
Proteger	SC-1	Preventivo	Protección de Sistemas y Comunicación	Política y procedimientos	Política y procedimientos
Proteger	SC-7	Preventivo	Protección de Sistemas y Comunicación	Protección de Límites	Protección de Límites
Proteger	SC-39	Preventivo	Protección de Sistemas y Comunicación	Aislamiento de Procesos	Aislamiento de Procesos

Cuadro 14. (Continuación)

Función	ID Control	Tipo de Control	Nivel 1	Nivel 2	Control
Proteger	PE-3	Preventivo	Protección Física y Ambiental	Control de Acceso Físico	Control de Acceso Físico
Proteger	PE-3 (4)	Preventivo	Protección Física y Ambiental	Control de Acceso Físico	Carcasas con bloqueo
Proteger	PE-11 (1)	Preventivo	Protección Física y Ambiental	Energía de Emergencia	Fuente de alimentación Alternativa
Proteger	PM-23	Preventivo	Gestión de Programas	Órgano de Gobierno de Datos	Órgano de Gobierno de Datos
Detectar	CA-5	Detectivo	Evaluación, Autorización y Monitoreo	Plan de acción e hitos	Plan de acción e hitos
Detectar	CA-7	Detectivo	Evaluación, Autorización y Monitoreo	Monitoreo Continuo	Monitoreo Continuo
Detectar	SA-3	Detectivo	Adquisición de Sistemas y Servicios	Ciclo De Vida de Desarrollo de Sistemas	Ciclo De Vida de Desarrollo de Sistemas
Responder	CP-2	Correctivo	Planificación de Contingencia	Plan de Contingencia	Plan de Contingencia
Responder	CP-6	Correctivo	Planificación de Contingencia	Sitios de Almacenamiento Alternativo	Sitios de Almacenamiento Alternativo
Responder	CP-7	Correctivo	Planificación de Contingencia	Sitios de Procesamiento Alternativo	Sitios de Procesamiento Alternativo

Cuadro 14. (Continuación)

Función	ID Control	Tipo de Control	Nivel 1	Nivel 2	Control
Responder	CP-8 (2)	Correctivo	Planificación de Contingencia	Servicios de Telecomunicaciones	Puntos Únicos de Falla

Fuente: NIST U.S. Publicación Especial del NIST 800-53.

9. PRESENTACIÓN DEL MODELO WEB BASADO EN EL PROTOTIPO EXPERIMENTAL

9.1 MODELO VISTA CONTROLADOR (MVC)

Modelo Vista Controlador (MVC) es un estilo de arquitectura de software que separa los datos de una aplicación, la interfaz de usuario, y la lógica de control en tres componentes distintos. Se trata de un modelo muy maduro y que ha demostrado su validez a lo largo de los años en todo tipo de aplicaciones, y sobre multitud de lenguajes y plataformas de desarrollo.[95]

El Modelo: contiene una representación de los datos que maneja el sistema, su lógica de negocio, y sus mecanismos de persistencia.[96]

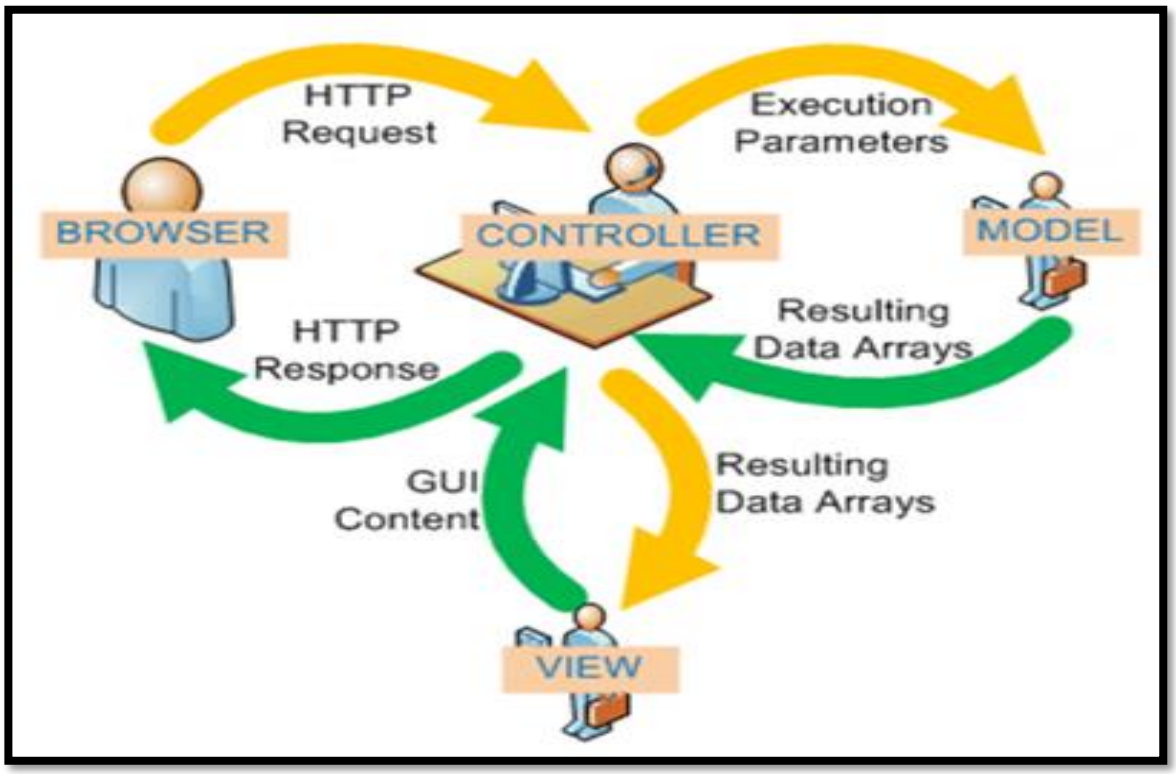
La Vista: o interfaz de usuario, que compone la información que se envía al cliente y los mecanismos interacción con éste.[97]

El Controlador: que actúa como intermediario entre el Modelo y la Vista, gestionando el flujo de información entre ellos y las transformaciones para adaptar los datos a las necesidades de cada uno.[98]

[95] Universidad de Alicante. “Modelo vista controlador (MVC)”. {En línea}. {31 octubre de 2021} disponible en: https://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html
[96] Ibíd.,
[97] Ibíd.,
[98] Ibíd.,

En la figura 29 se muestra el flujo que generalmente sigue el controlador.

Figura 29. Flujo del Modelo vista controlador (MVC).



Fuente: Universidad de Alicante, servicio de informática.

El Diseño del prototipo web permite hacer el seguimiento, la evaluación del riesgo y la generación de controles de seguridad, sugeridos para mitigar los riesgos asociados a la línea de trabajo de la empresa G0 S.A.S.

La implementación del prototipo web, parte de la necesidad que tiene la empresa G0 S.A.S de asegurar los activos de información, junto con la alineación de los objetivos estratégicos con la misión y visión, para así generar paralelamente confiabilidad y seguridad en los clientes. De igual forma, busca gestionar una herramienta web que agilice y simplifique los procesos según la metodología NIST, para evaluar e implementar controles de seguridad y privacidad en el desarrollo de la operación.

En la etapa de diseño del prototipo se utilizó el método *Storyboard Prototyping*, el cual consiste en una serie de dibujos o imágenes que representan la manera en que una interfaz gráfica es usada, para cumplir con una tarea en particular. En el

desarrollo del prototipo se emplea Visual .net Core, el cual es un lenguaje de programación moderno. El prototipo es *responsive* permitiendo al usuario operarlo en iPad, PC y celulares.

El prototipo es una herramienta creada con una interfaz simple, sencilla de entender y usar, el prototipo está basado en la metodología NIST, en donde entrega la funcionalidad necesaria para ser gestionada por un usuario no experto en seguridad de la información, permitiéndole identificar los diferentes riesgos que puede enfrentar la empresa, y le proporciona un listado de controles de seguridad direccionados para ser implementados, evitando una materialización de riesgos en la infraestructura tecnológica de G0 S.A.S.

De igual forma, el prototipo proporciona a la Gerencia con el perfil consultor disponer de reportes que le permiten conocer los movimientos operativos tecnológicos de la hoja de ruta de la empresa, frente a las mejores prácticas para la mitigación de los riesgos y la toma de decisiones de forma eficiente.

En el desarrollo del prototipo web se realizaron los diseños de la interfaz gráfica y el flujo de navegación que sigue la aplicación.

Para la construcción del prototipo se basó en una plantilla de la matriz de riesgos implementada que sirve como insumo para el desarrollo de este. Se creó un menú que corresponde a los bloques presentados en…Véase el numeral 7.2… de la evaluación de riesgos, donde se visualiza la interacción de las diferentes amenazas con sus respectivas vulnerabilidades.

En el cuadro 15 se presenta las herramientas usadas para desarrollar el prototipo, además se describe la configuración que debe tener el servidor con respecto a sus características de *hardware* y versiones de software.

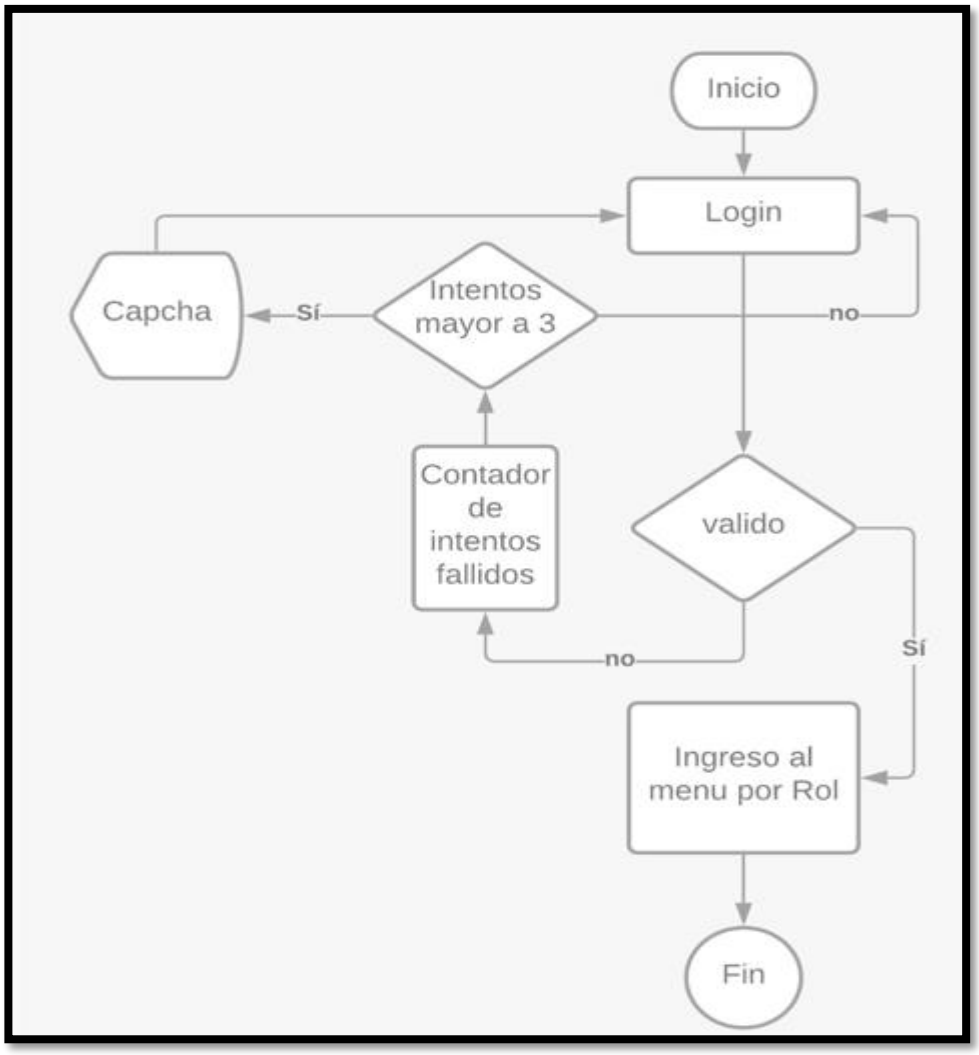
Cuadro 15. Características del servidor y lenguaje usado en el prototipo.

Componentes empleados	Descripción
Lenguaje de programación	*Visual.Net Core 5 Razor*
Motor de base de datos	*SQL Server Versión 15*
Proveedor *Hosting*	*Microsoft*
Características del servidor	Windows 16,04,2 CPU Virtuales, 30 Gigas de almacenamiento en disco, 4 Gigas en RAM
Método de consumo	Web

Fuente: Autores de la Investigación.

En la figura 30 se muestra los procedimientos y su paso a paso donde se refleja el comportamiento del actor cuando se autentica en el prototipo y de acuerdo con la lógica de negocio, este le permitirá ingresar o arrojará un mensaje de *login* fallido.

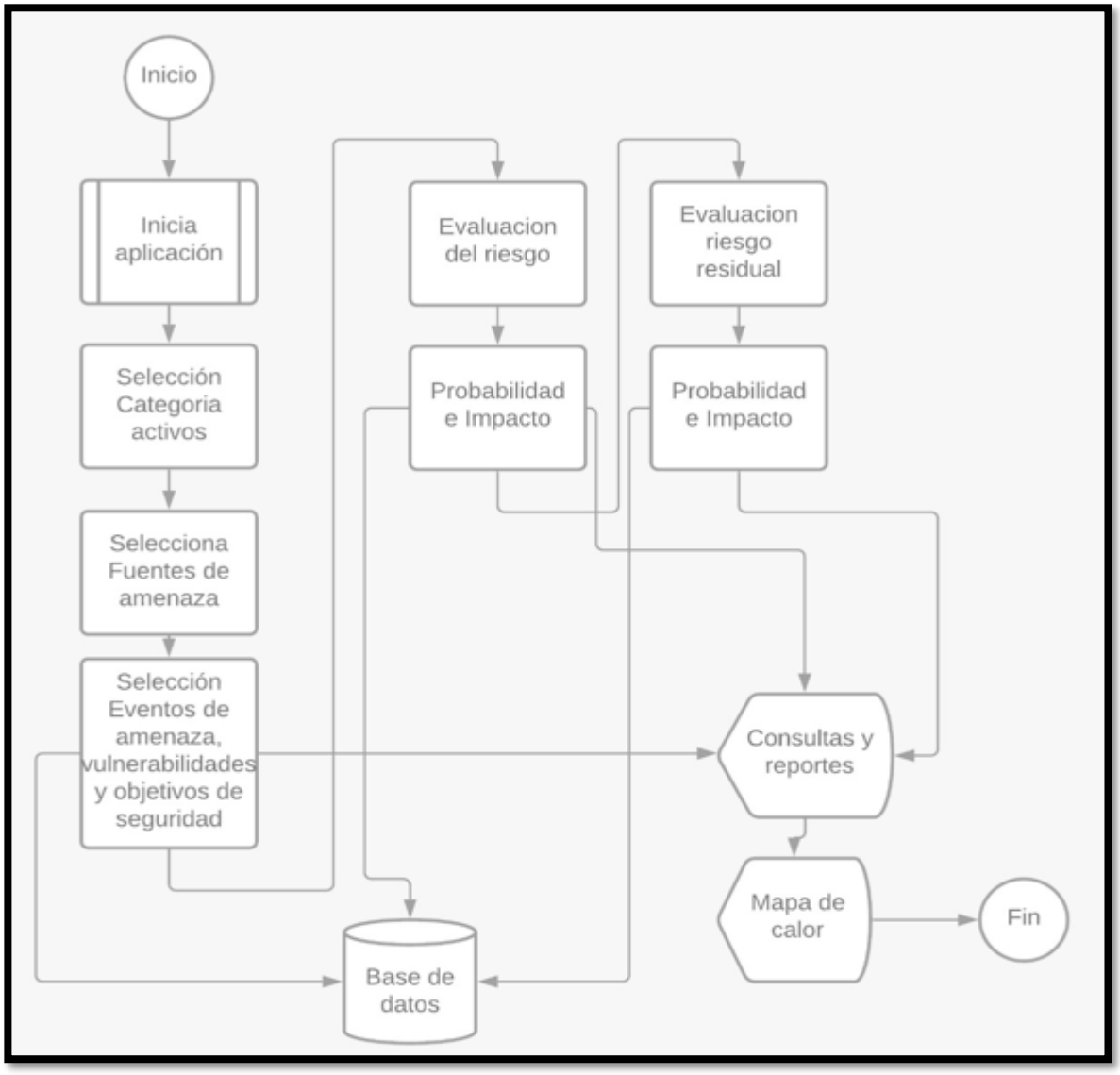
Figura 30. Diagrama de flujo de Autenticación en el Prototipo.



Fuente: Autores de la Investigación.

En la figura 31 se muestra el diagrama de flujo del comportamiento que tiene el actor en el prototipo. En este se refleja la implementación del CSF NIST, el cual muestra como a medida que el actor ingresa la información requerida por el sistema, es almacenada, analizada y como resultado final entrega controles sugeridos para su implementación.

Figura 31. Diagrama de flujo de Negocio.



Fuente: Autores de la Investigación.

9.2 BASE DE DATOS

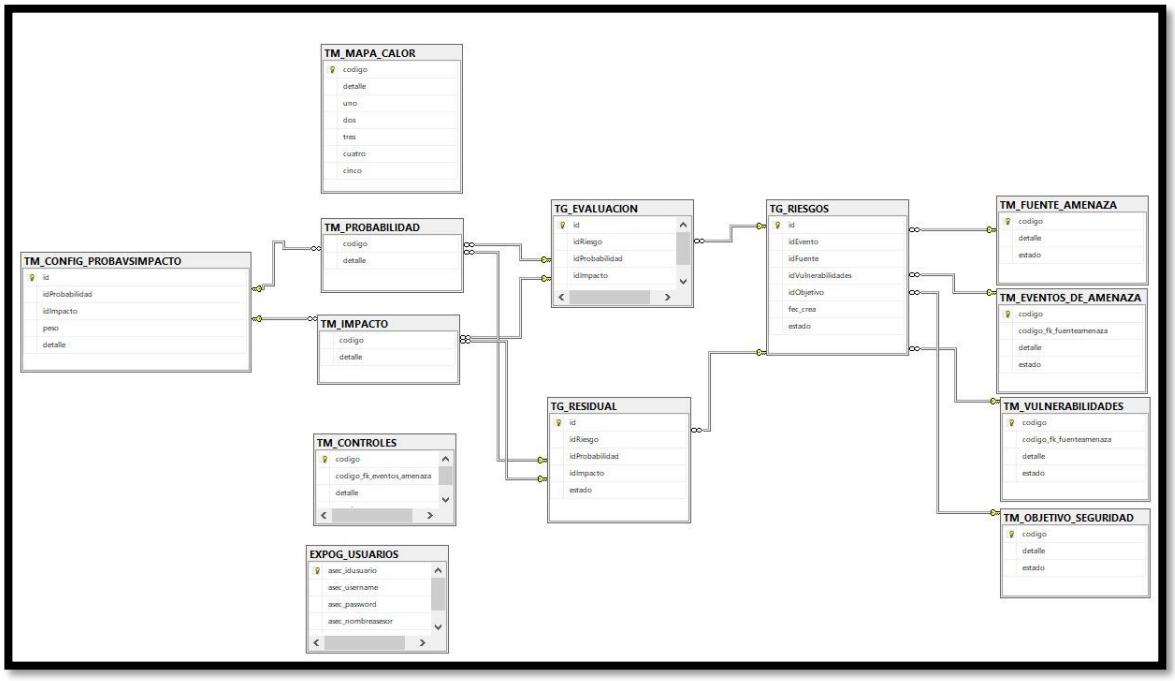
En la figura 33 se muestra el *SQL Server Management Studio* y se presenta la estructura de las tablas, las cuales son usadas por el prototipo, y tienen los siguientes prefijos al inicio de estas

- TM: tabla maestra que contiene la configuración de negocio usada en la aplicación.
- TG: tabla de gestión en la cual los datos son manipulados de acuerdo con la necesidad de negocio.
- EXPOG: contienen la configuración básica de la aplicación.

También contiene los procedimientos almacenados los cuales gestionan la entrega de los datos a el prototipo. Estos inician con el prefijo “SP_” seguido del detalle indicando lo que hace.

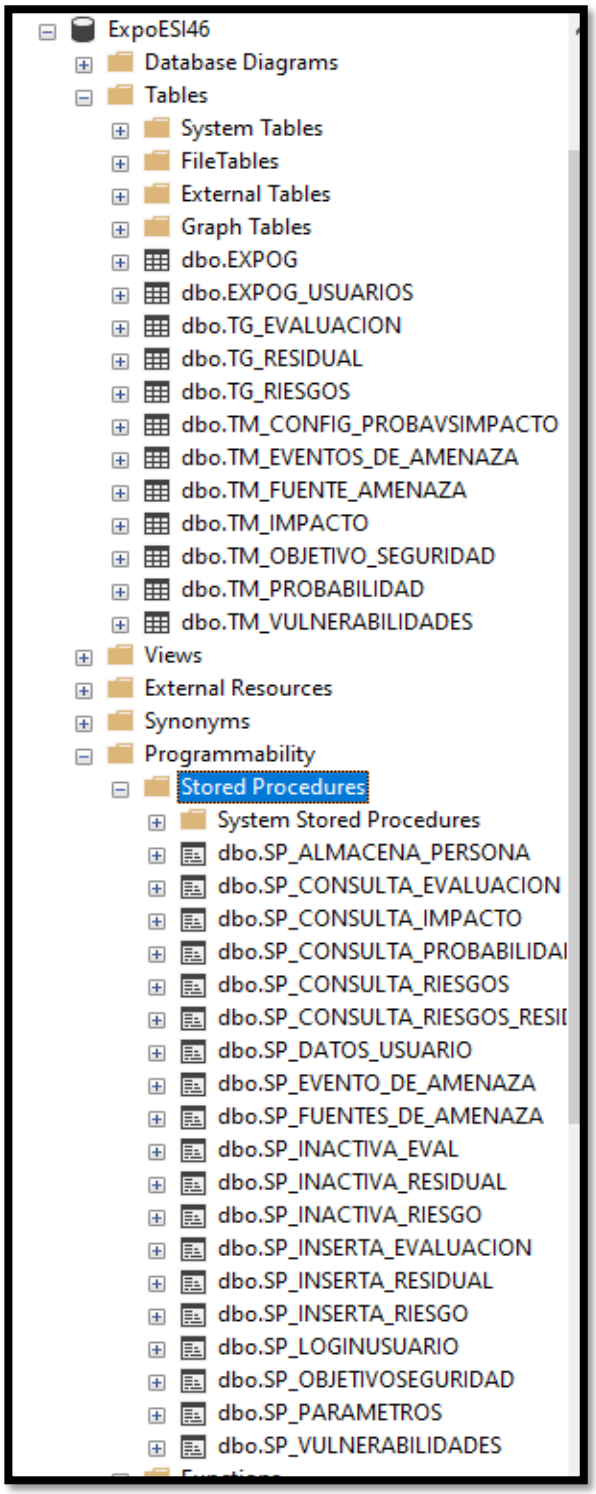
En la figura 32 y 33 se muestra el modelo entidad relación del prototipo propuesto en donde se puede evidenciar el conjunto de tablas maestras y las relaciones que hay entre ellas. Por otra parte, se muestran las llaves principales y las foráneas.

Figura 32. Modelo Entidad Relación.



Fuente: Autores de la Investigación.

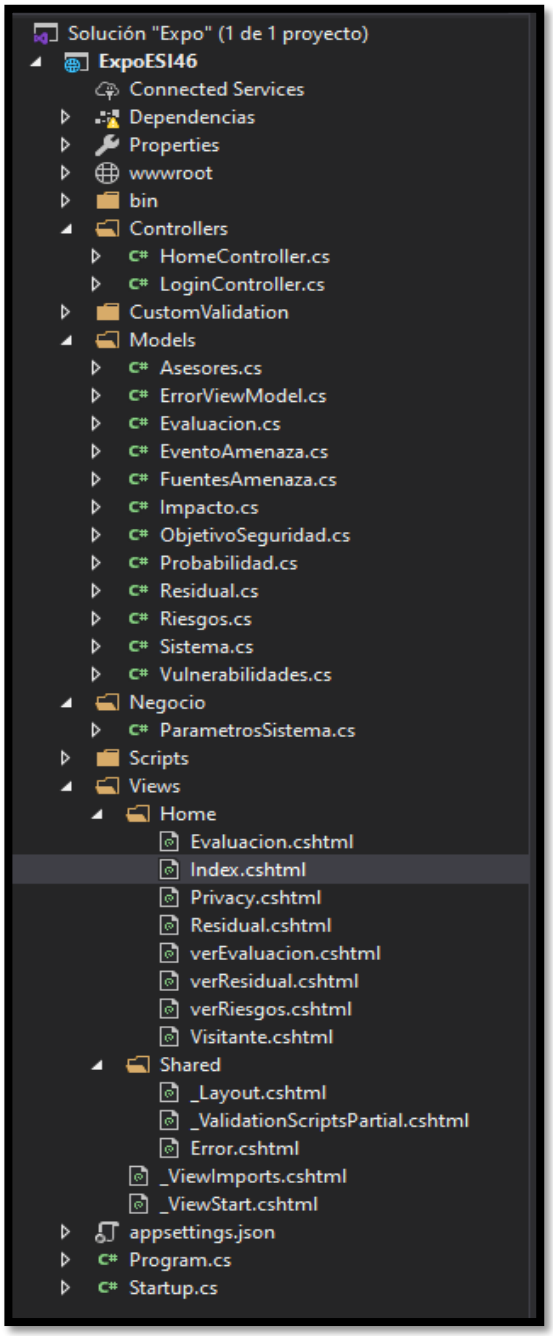
Figura 33. Bases de Datos.



Fuente: Prototipo web.

En la figura 34 se muestra claramente cómo está diseñado el prototipo con la arquitectura modelo vista controlador (MVC).

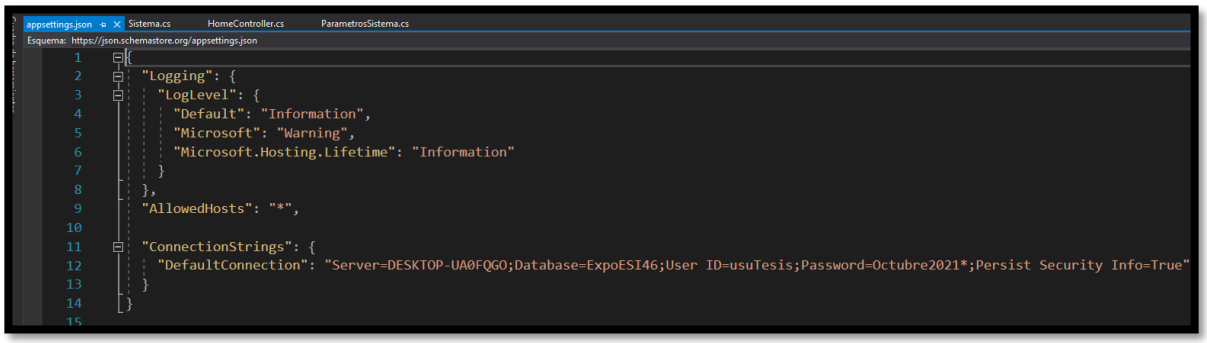
Figura 34. Explorador de soluciones en visual .net.



Fuente: Prototipo web.

En la figura 35 se muestra el archivo que permite configurar los parámetros necesarios para que la capa de conexión a la base de datos gestione el acceso a estos, la llave usada para esto es la llamada *ConnectionStrings.*

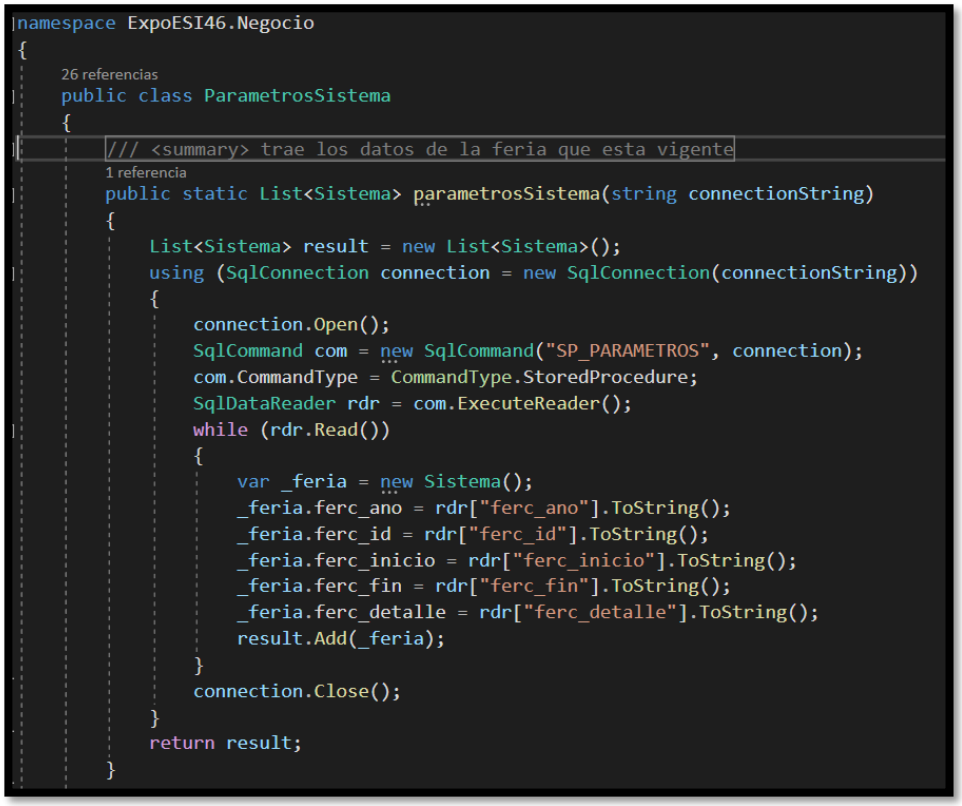
Figura 35. Archivo de configuración con cadena de conexión a la base de datos.



Fuente: Prototipo web.

En la figura 36 se muestra cómo se hace el manejo de conexión a la base de datos y solicitud de estos para su posterior uso del controlador y entrega a la capa de la vista.

Figura 36. Capa adicional conexión a la base de datos donde se obtiene los parámetros iniciales para el uso de la aplicación.

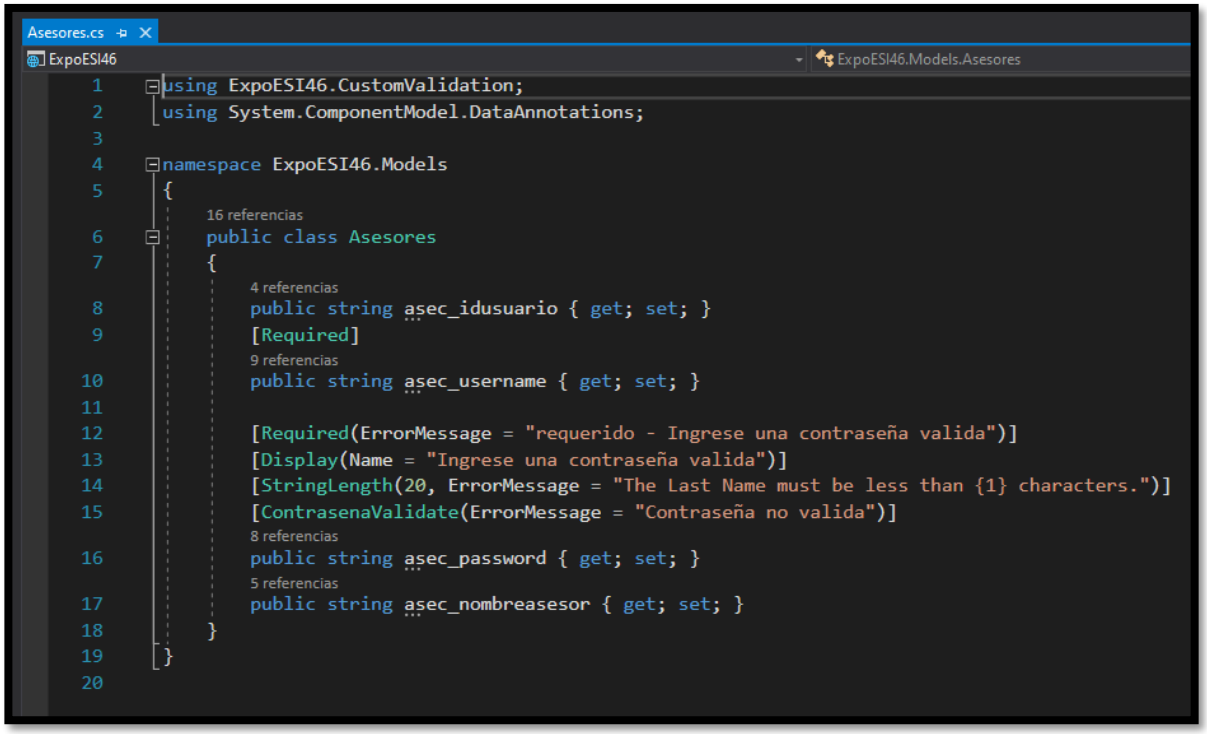


```
namespace ExpoESI46.Negocio
{
    26 referencias
    public class ParametrosSistema
    {
        /// <summary> trae los datos de la feria que esta vigente
        1 referencia
        public static List<Sistema> parametrosSistema(string connectionString)
        {
            List<Sistema> result = new List<Sistema>();
            using (SqlConnection connection = new SqlConnection(connectionString))
            {
                connection.Open();
                SqlCommand com = new SqlCommand("SP_PARAMETROS", connection);
                com.CommandType = CommandType.StoredProcedure;
                SqlDataReader rdr = com.ExecuteReader();
                while (rdr.Read())
                {
                    var _feria = new Sistema();
                    _feria.ferc_ano = rdr["ferc_ano"].ToString();
                    _feria.ferc_id = rdr["ferc_id"].ToString();
                    _feria.ferc_inicio = rdr["ferc_inicio"].ToString();
                    _feria.ferc_fin = rdr["ferc_fin"].ToString();
                    _feria.ferc_detalle = rdr["ferc_detalle"].ToString();
                    result.Add(_feria);
                }
                connection.Close();
            }
            return result;
        }
```

Fuente: Prototipo web.

En la figura 37 se evidencia la estructura que se plantea en el modelo para el manejo de los datos del usuario que se autenticara en el prototipo.

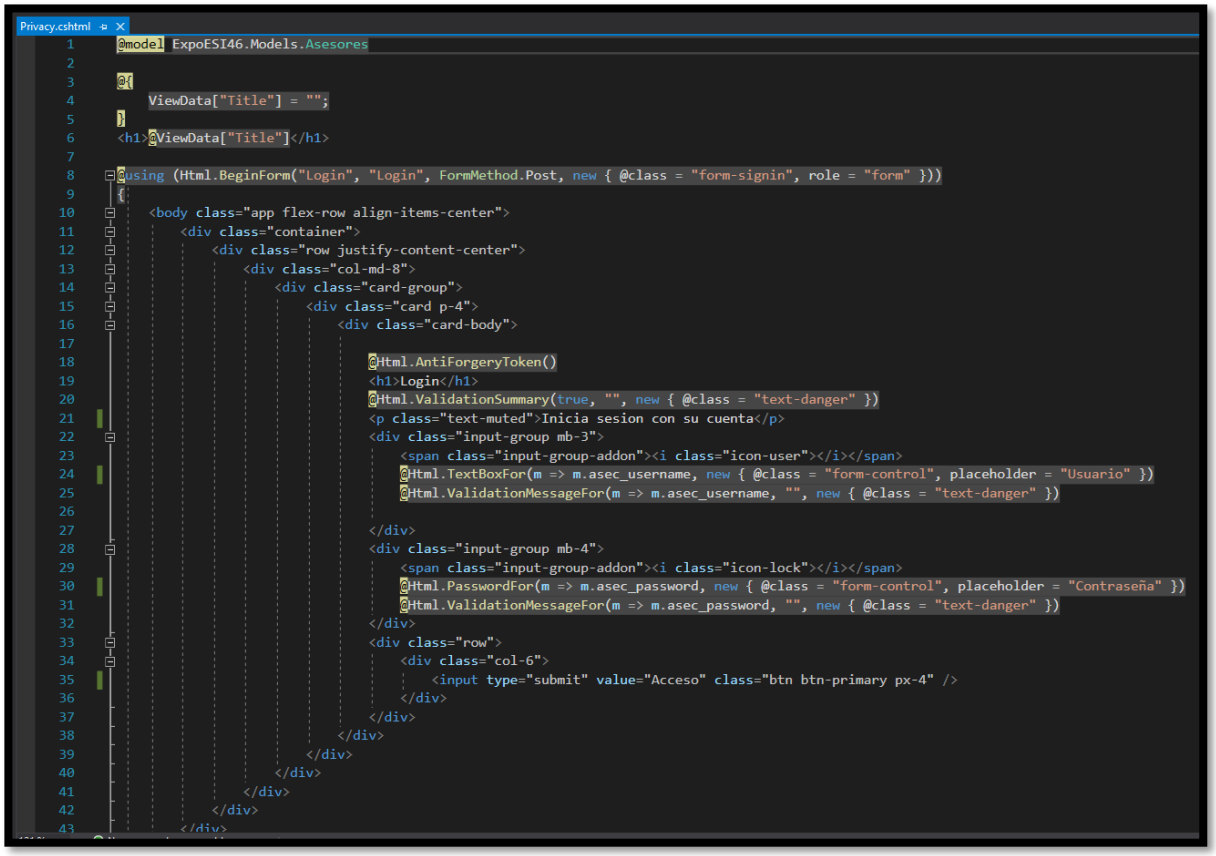
Figura 37. Modelo de usuario que se conectaran al prototipo.



Fuente: Prototipo web.

En la figura 38 se evidencia cómo se entregan y capturan los datos en la capa la vista, permitiendo validar si este tiene permisos para ingresar al prototipo.

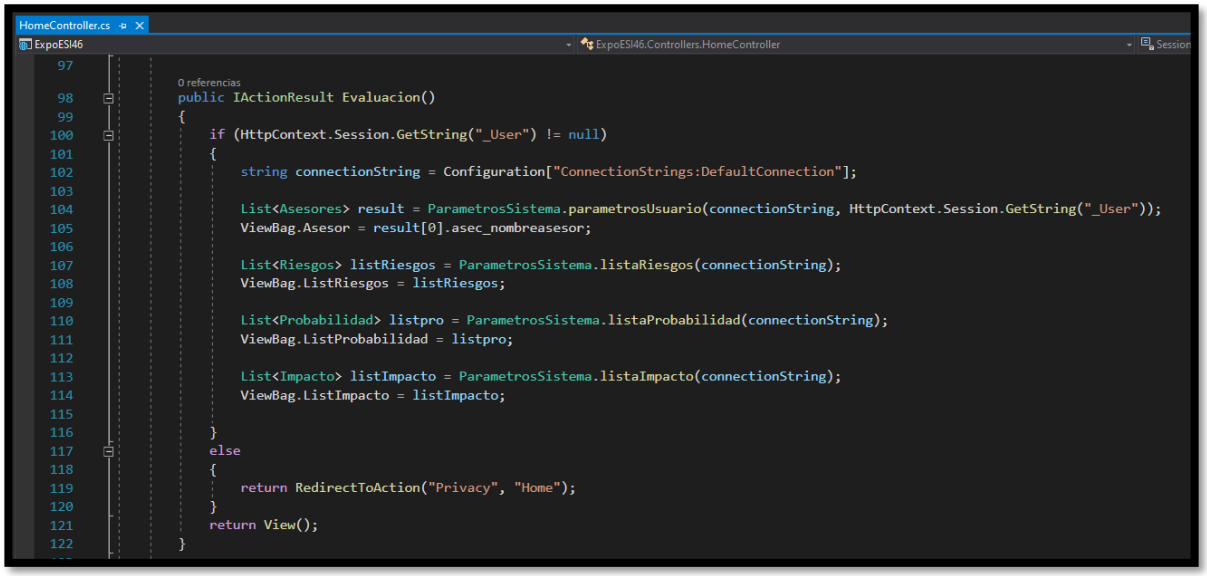
Figura 38. Vista.



Fuente: Prototipo web.

En la figura 39 se muestra como el controlador solicita a la capa de acceso a los datos peticiones para cargar las listas desplegables y los *textbox* creados en las vistas. Esto le permite al controlador manipular los datos entregados y de acuerdo a las necesidades del negocio mostrar en la vista lo que sea necesario.

Figura 39. Controlador.



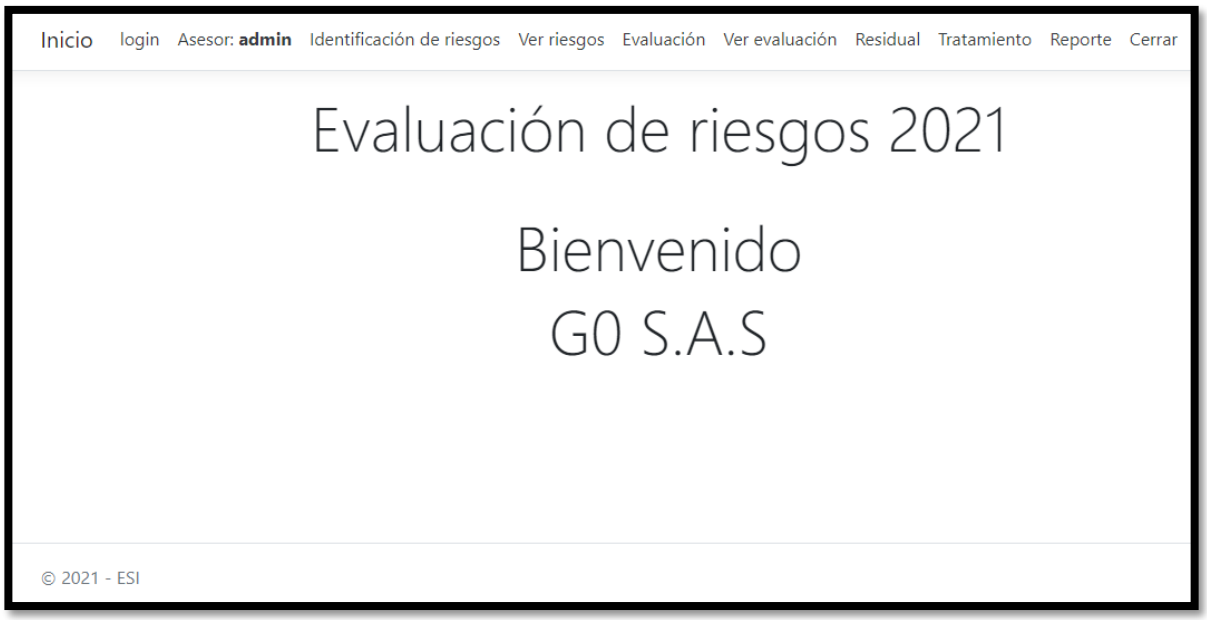
Fuente: Prototipo web.

9.3 VALORACIÓN DEL PROTOTIPO

En las imágenes siguientes se muestra como el prototipo busca de una manera fácil y amigable permitirle al usuario poder identificar los riesgos, hacer la evaluación de estos y como resultado final, obtener unos controles sugeridos que le permitan tener mayor conocimiento en seguridad de la información y poder posteriormente aplicar los controles que más se ajusten a sus necesidades.

En la figura 40 se muestra la vista de bienvenida a adecuar en el prototipo presentado, de acuerdo con las necesidades de G0 S.AS.

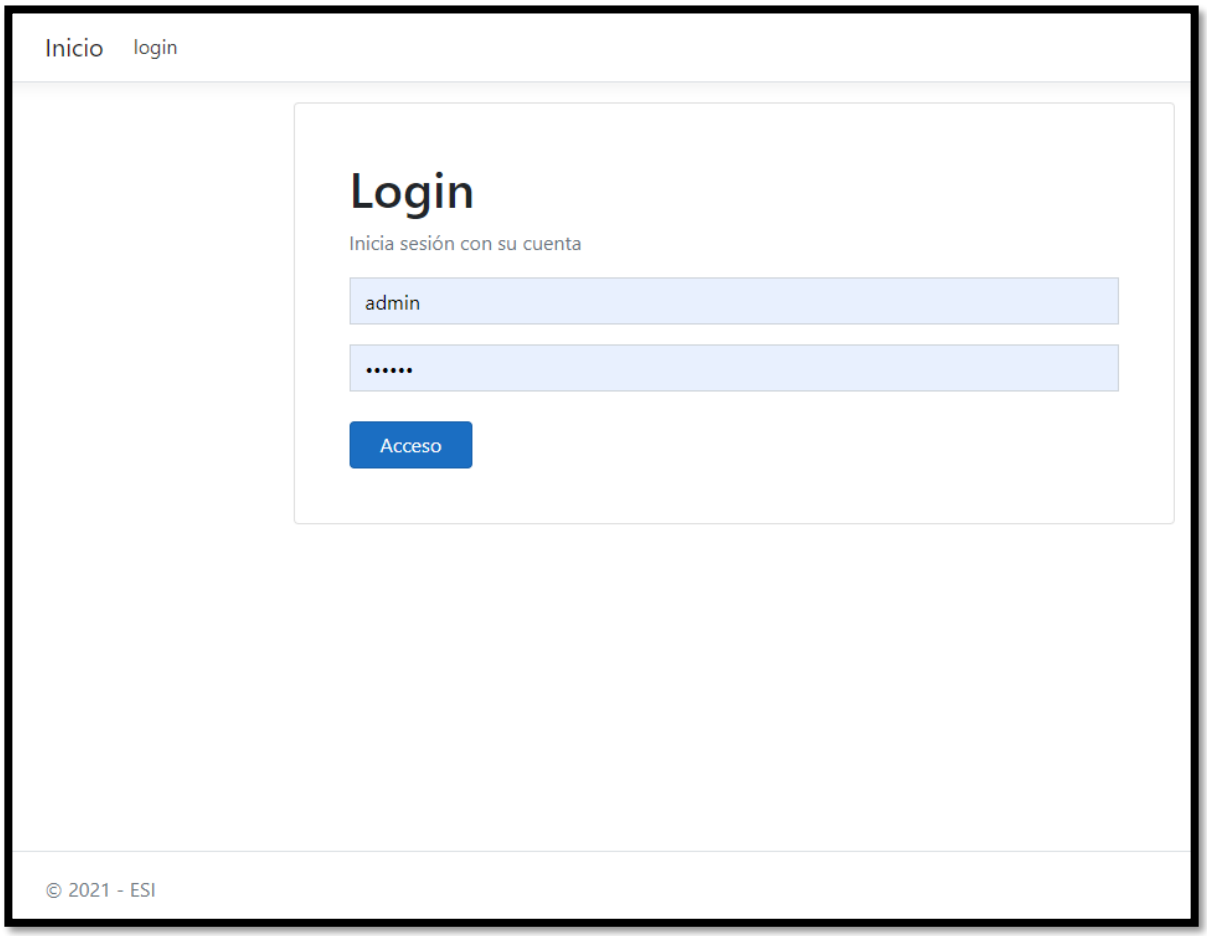
Figura 40. Pantalla de bienvenida.



Fuente: Prototipo web.

En la figura 41 se muestra la vista que permite realizar un control de seguridad antes de que la persona indicada pueda acceder a el prototipo y realizar las actividades de gestión de los riesgos.

Figura 41. Formulario de autenticación del prototipo.



Fuente: Prototipo web.

En la figura 42 se muestra la vista de identificación de los riesgos, que permite al actor seleccionar su categoría de activo, las fuentes de amenaza. Una vez seleccionado este campo, se precargarán las listas desplegables de eventos de amenaza y vulnerabilidades evidenciando como se integra el CSF NIST 800-30 en el prototipo; usando este marco NIST se realiza la evaluación del riesgo. Luego de esto, por medio del análisis y de la lógica de programación se implementa el CSF NIST 800-53 para entregar los controles sugeridos para el tratamiento de los riesgos.

Figura 42. Selección y almacenamiento de los riesgos.

Fuente: Prototipo web.

En la figura 43 se muestra la lista desplegable con las posibles opciones a seleccionar.

Figura 43. Categoría de Activo.

Fuente: Prototipo web.

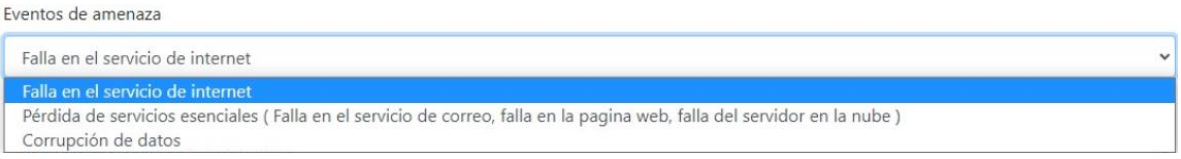
En la figura 44 se muestra la lista desplegable con las posibles opciones a seleccionar.

Figura 44. Lista Fuentes de Amenaza.

Fuente: Prototipo web.

En la figura 45 se muestra la lista desplegable con las posibles opciones a seleccionar

Figura 45. Lista Eventos de Amenaza.



Fuente: Prototipo web.

En la figura 46 se muestra la lista desplegable con las posibles opciones a seleccionar.

Figura 46. Lista de Vulnerabilidades.

Fuente: Prototipo web.

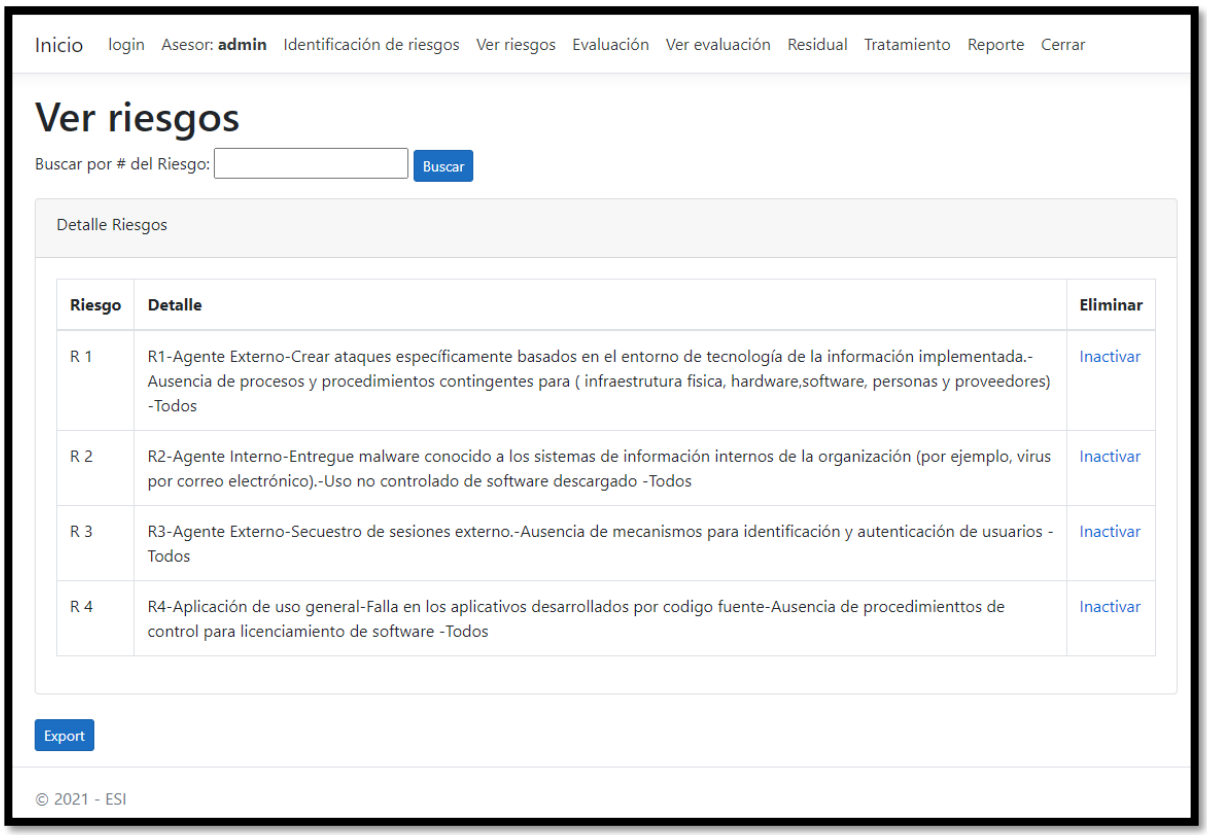
En la figura 47 se muestra la lista desplegable con las posibles opciones a seleccionar.

Figura 47. Lista de Objetivos de Seguridad.

Fuente: Prototipo web.

En la figura 48, se muestra los diferentes datos almacenados en la vista de identificación del riesgo. Esta vista tiene las opciones de realizar búsqueda por el número de identificación del riesgo, eliminación, y, por último, exportación a Excel permitiendo descargar los datos que se visualizan para su posterior análisis.

Figura 48. Consulta de los riesgos cargados en el prototipo.



Fuente: Prototipo web.

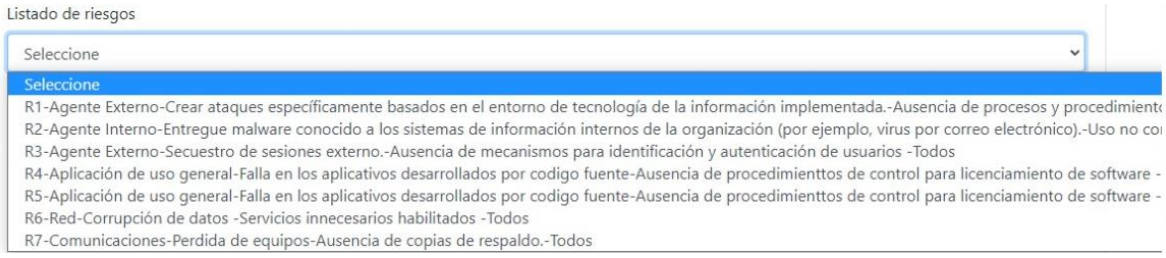
En la figura 49 se muestra en la lista desplegable cómo se van adicionando los riesgos a medida que el usuario los identifica en la vista de "identificación de los riesgos", esto le permite al usuario seleccionar el riesgo para ser evaluado con su probabilidad e impacto.

Figura 49. Selección y cargue para la evaluación de los riesgos.

Fuente: Prototipo web.

En la figura 50 se muestra la lista desplegable con las posibles opciones a seleccionar.

Figura 50. Lista desplegable de Riesgos.



Fuente: Prototipo web.

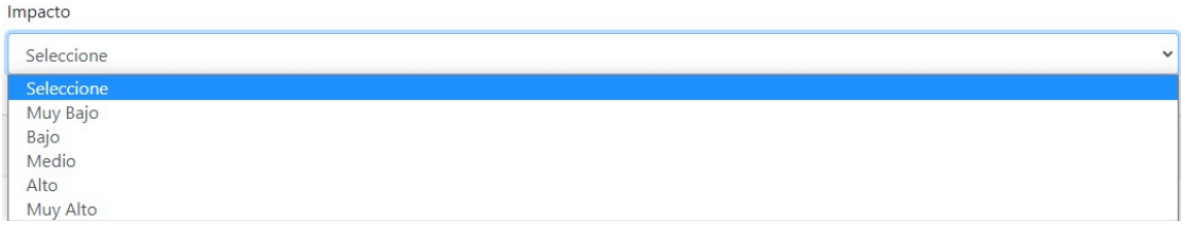
En la figura 51 se muestra la lista desplegable con las posibles opciones a seleccionar.

Figura 51. Lista de valores de Probabilidad.

Fuente: Prototipo web.

En la figura 52 se muestra la lista desplegable con las posibles opciones a seleccionar.

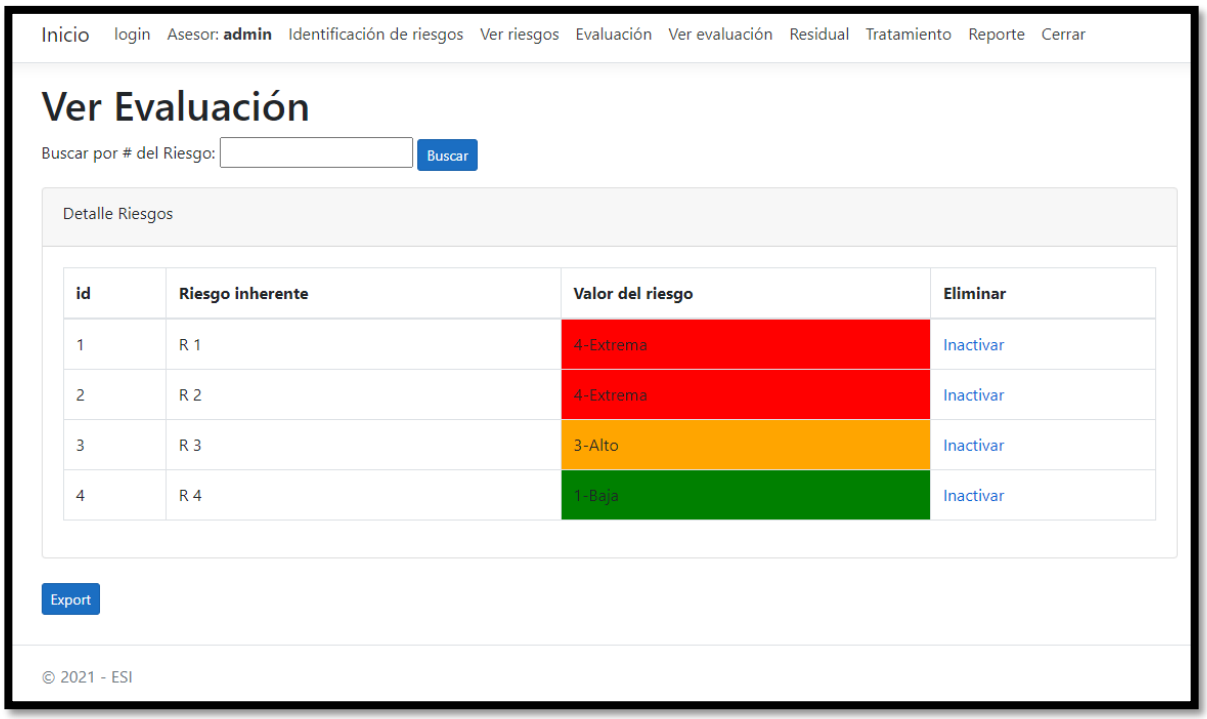
Figura 52. Lista de valores de Impacto.



Fuente: Prototipo web.

En la figura 53 se muestra los diferentes datos almacenados en la vista de evaluación del riesgo junto con sus respectivos valores de clasificación identificadas …en la sección 7.3.2.1 y 7.3.2.2. … Esta vista tiene las opciones de realizar búsqueda por el número de identificación del riesgo, eliminación y por último, exportación a Excel, permitiendo descargar los datos que se visualizan para su posterior análisis.

Figura 53. Consulta de la evaluación de los riesgos cargados.



Fuente: Prototipo web.

En la figura 54 se muestra la lista desplegable como se van adicionando los riesgos a medida que el usuario los identifica en la vista de "identificación de los riesgos", esto le permite al usuario seleccionar el riesgo para ser evaluado con su probabilidad e impacto residuales.

Figura 54. Selección y cargue de los riesgos residuales en el prototipo.

Fuente: Prototipo web.

En la figura 55 se muestra la lista desplegable con las posibles opciones a seleccionar.

Figura 55. Lista de valores de Probabilidad Residual.

Fuente: Prototipo web.

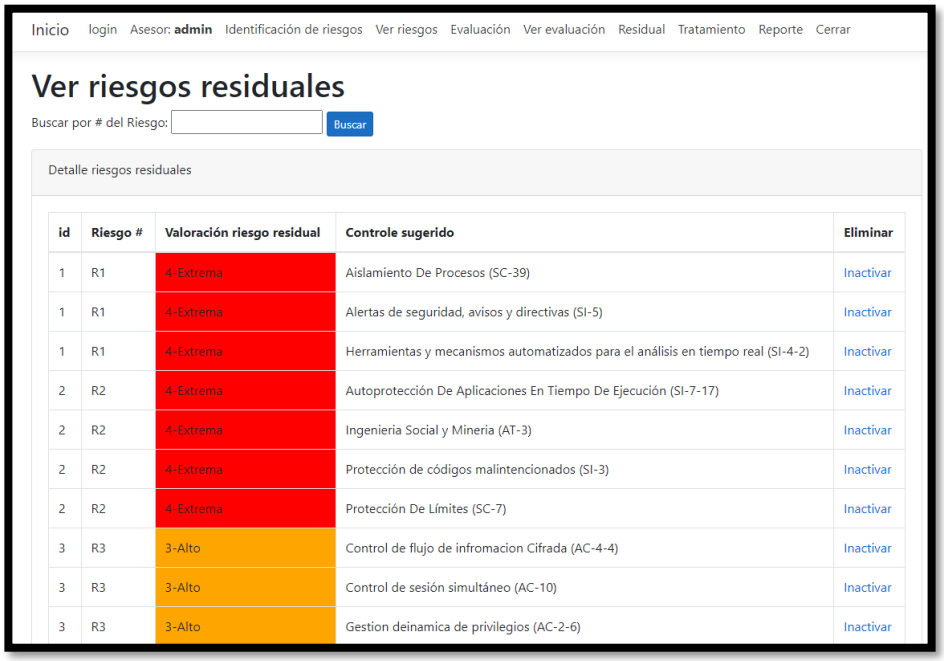
En la figura 56 se muestra la lista desplegable con las posibles opciones a seleccionar

Figura 56. Lista de valores de Impacto Residual.

Fuente: Prototipo web.

En la figura 57 se muestra los diferentes datos almacenados en la vista de evaluación del riesgo residual, junto con sus respectivos valores de clasificación identificadas …en la sección 7.3.2.1 y 7.3.2.2. … Esta vista tiene las opciones de realizar búsqueda por el número de identificación del riesgo, eliminación y por último, exportación a Excel permitiendo descargar los datos que se visualizan para su posterior análisis.

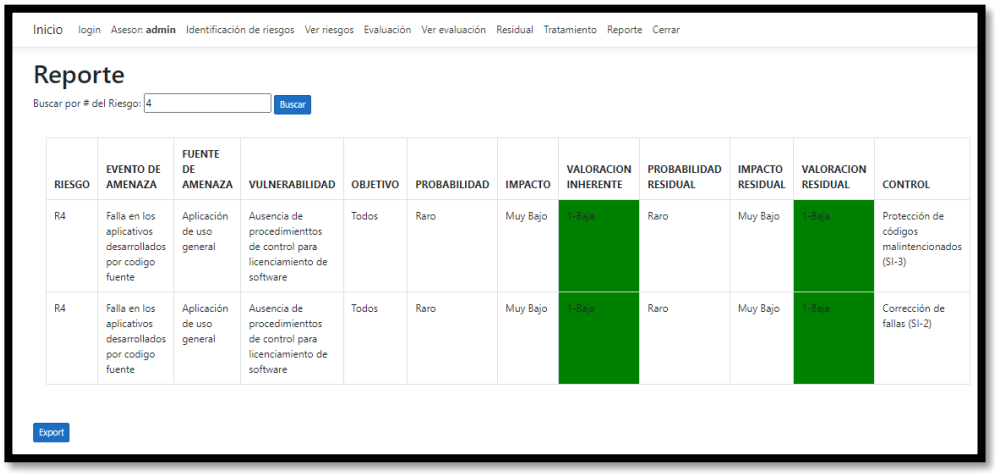
Figura 57. Consulta de los riesgos residuales.



Fuente: Prototipo web.

En la figura 58 se muestran todo el ecosistema cargado relacionadas con la evaluación de riesgos, junto con sus respectivos valores de clasificación identificadas …en la sección 7.3.2.1 y 7.3.2.2. …Esta vista tiene las opciones de realizar búsqueda por el número de identificación del riesgo e exportación a Excel permitiendo descargar los datos que se visualizan para su posterior análisis, sirviendo como insumo para el informe ejecutivo a socializar con la alta gerencia, asociando el riesgo evaluado con los controles sugeridos.

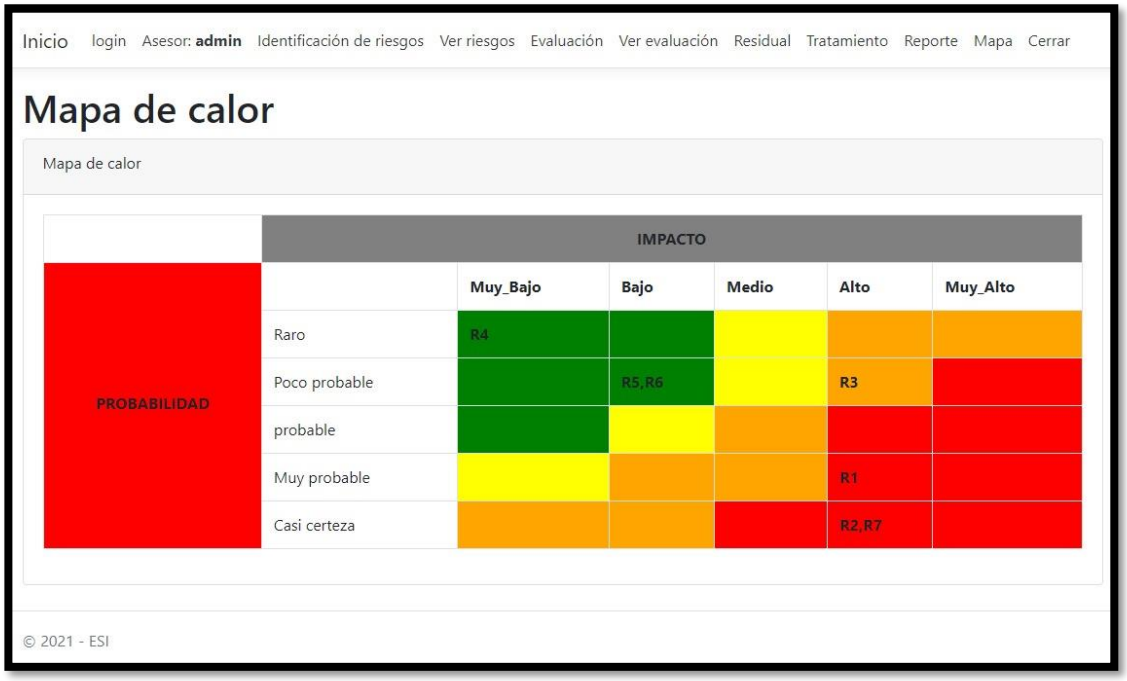
Figura 58. Reporte final ejecutivo.



Fuente: Prototipo web.

En la figura 59 se muestra cómo se van ubicando los riesgos identificados y evaluándose en el mapa de calor dentro de su zona de criticidad, para así visualizar que riesgos son los de mayor prioridad a tratar en la toma de decisiones de la alta gerencia.

Figura 59. Mapa de calor.



Fuente: Prototipo web.

10. RESULTADOS

¿Qué controles de seguridad y privacidad debe implementar la empresa G0 S.A.S, para mitigar los riesgos y proteger los datos informáticos registrados en su infraestructura tecnológica?

Para establecer la integridad, disponibilidad y confidencialidad de la información en la infraestructura tecnológica de G0 S.A.S, la cual ofrece al mercado un modelo de negocio orientado a la prestación de servicios tecnológicos, y para cumplir su meta descrita en la visión de la empresa, se deben implementar los controles referenciados en el marco CSF NIST 800-53, realizando previamente una evaluación de riesgos basado en el marco CSF NIST 800-30. De esta forma, se buscó entregarle a G0 S.A.S una adecuada gestión de los riesgos, acertada a sus necesidades y acotada a su capacidad económica.

A través de la evaluación de riesgos basados en el marco CSF NIST SP800-30, realizados a la infraestructura tecnológica e identificando los diferentes escenarios de riesgos en cada uno de los procesos de la empresa G0 S.A.S, se determinaron las posibles fuentes y eventos de amenazas asociadas con las vulnerabilidades para evitar que se materialicen los riesgos encontrados. Con los resultados obtenidos, se sugiere a la alta gerencia promover las mejores prácticas implementado los controles en los procesos más críticos para su debido tratamiento, fomentando de esta forma, un ambiente de cultura de seguridad de la información.

Pensando en facilitar anualmente la evaluación de los riesgos para una empresa como G0 S.A.S, se presenta el diseño de un prototipo que le permitirá poder realizar una evaluación y mitigación de los riesgos haciendo uso del marco CSF NIST SP800-30 y CSF NIST SP800-53. Como resultado de este proceso se obtienen los controles sugeridos junto con el mapa de calor que será analizado por la junta directiva para definir su hoja de ruta. Con esto se busca mantener la integridad, disponibilidad y confidencialidad de la información en la infraestructura tecnológica de G0 S.A.S.

Como parte de los retos del proyecto al entregar un prototipo web de uso fácil e intuitivo para los usuarios, el diseño entregado a G0 S.A.S no solo fue hecho a la medida y acorde a las necesidades, sino que demostró su capacidad de adaptación en la etapa inicial de implementación por no presentar funcionalidades extensas y complejas para conocimiento de los usuarios e integración en los procesos actuales de la organización.

Así mismo, como parte del diseño se usó .net Core 5 para primero realizar un despliegue rápido y fácil, ya sea en servidores Windows o Azure, y segundo, asegurar el cumplimiento de presupuesto por los costes de mantenimiento que esté

presenta para así incluir el análisis de riesgo como proceso fundamental en la empresa.

Por otra parte, para lograr tener un mejor entendimiento de la criticidad de los riesgos a los que se enfrentan los diferentes procesos de G0 S.A.S, se propusieron dos reportes los cuales permiten rápidamente identificar cuáles de estos se deben atender de forma inmediata. A solicitud de los procesos de G0 SAS, se creó el reporte histórico que muestra toda la trazabilidad desde sus fuentes de amenaza del riesgo, hasta la valoración residual. Para finalizar, el mapa de calor imprime los resultados de la evaluación de los riesgos, y muestra su ponderación en la criticidad de la matriz indicando su probabilidad e impacto.

Por último, el diseño entregado le permitió a G0 S.A.S establecer una hoja ruta definida bajo la metodología NIST con la finalidad de adoptar las buenas prácticas y asegurar las acciones que deben realizar para salvaguardar su información y poder así, proyectarse en el mercado como una empresa pyme líder en el desarrollo tecnológico.

11. CONCLUSIONES

- Las pequeñas empresas como G0 S.A.S, se enfrentan a riesgos no deseados que pueden generar daños reputacionales y económicos irreparables en el desarrollo de las actividades de la organización. Con la ayuda del marco de referencia NIST SP 800-30, se establecieron mejores mecanismos para la protección de la infraestructura tecnológica de G0 S.A.S, las cuales permitirán tomar acciones para asegurar la continuidad de negocio en cada uno de sus procesos.

- Para la evaluación del riesgo en la empresa G0 S.A.S se contó con la participación de los procesos críticos para su operación. Con esto se busca que en sus grupos de interés, se genere confianza entre las partes en el uso de las buenas prácticas para la protección de la infraestructura tecnológica.

- La Seguridad de la Información es fundamental en los diferentes procesos manejados en la empresa G0 S.A.S; sin embargo, hasta la fecha esta no había tomado el tema de la seguridad de la información como factor esencial en su cultura organizacional. Por lo tanto, con la evaluación del riesgo, se ayudó a establecer los controles para generar buenas prácticas en el manejo óptimo en el desarrollo de las actividades de la empresa y así cumplir con los principios de la seguridad de la información.

- La evaluación de los riesgos contribuyó en la identificación de las amenazas a las que la organización está expuesta debido al desconocimiento de la seguridad de la información en sus procesos, lo que les permitió darse cuenta de los riesgos a los que están expuestos diariamente y el impacto que puede originar si se materializan alguno de ellos. Para los riesgos clasificados como muy altos o inaceptables en el mapa de calor, se proponen los controles para realizar acciones con el fin de mitigarlos y proteger los procesos en la organización.

- El prototipo propuesto además de integrar el marco CSF NIST se adapta a las necesidades de G0 S.A.S, permitiendo a este realizar la evaluación de los riesgos desde cualquier locación. Adicionalmente, los datos usados para la evaluación de los riesgos están disponibles y en línea, como resultado la junta directiva y los procesos podrán tener acceso a los datos y controles sugeridos en cualquier momento que se requieran. De esta forma, G0 SAS podrá tener a la mano la información necesaria para ser usada como su hoja de ruta, lo que le permitirá a

las personas encargadas de los procesos, estar al tanto de las actividades y buenas prácticas a implementar.

BIBLIOGRAFÍA

ALICANTE, U. d. (20 de 08 de 2012). si.ua.es. Obtenido de si.ua.es: https://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html.

BANCO INTERAMERICANO DE DESARROLLO. Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe [en línea]. Universidad de Oxford. 2020. 28-29 p. [Consultado: 31 de julio de 2021]. Disponible en: https://observatoriociberseguridad.org/#/home.

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Ciberseguridad en entornos cotidianos, estudio del cibercrimen 2020. [sitio web]. Bogotá: Wework. Diciembre 2020. [Consultado: 31 de julio de 2021]. Disponible en: https://www.ccit.org.co/estudios/ciberseguridad-en-entornos-cotidianos-estudio-del-cibercrimen-2020.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley estatutaria 1266 (31, diciembre, 2009). Por la cual se dictan disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales. [en línea], En: Diario Oficial. Bogotá, 2008. No.47219. p.1_10. [Consultado: 15 de agosto 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). Por 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 [en línea]. En: Diario Oficial. Bogotá, 2009. No.47223. p.1_3. [Consultado: 15 de agosto 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales [en línea]. En: Diario Oficial. Bogotá, 2012. 48587. p.1_8 [Consultado: 12 de julio de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981.

-------.------- Bogotá, 2012. 48587. p.1_8 [Consultado: 12 de julio de 2021]. Disponible en:. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 256 (18, enero, 1996). Por la cual se dictan normas sobre competencia desleal [en línea]. En: Diario Oficial. Bogotá, 1996. 42692. p.3. [Consultado: 17 de agosto de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0256_1996.html.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 527 (21, agosto 1999). Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. [en línea], En: Diario Oficial. Bogotá, 1999. No.43673. p.2. [Consultado: 18 de agosto 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html.

COLOMBIA, Constitución Política de la República de Colombia. (20, julio, 1991). Por la cual se decreta, sanciona y promulga la Constitución Política de Colombia [en línea]. En: Gaceta Constitucional. 1991. 116. p.4 [Consultado: 16 de agosto de 2021]. Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html.

CORDA, María Cecilia; VIÑAS, Mariela; CORIA, Marcela Karina. Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. En: Palabra Clave (La Plata) [en línea]. Universidad Nacional de La Plata Argentina: e032, octubre, 2017, vol. 7, nro. 1, p. 1-18. [Consultado el 29 de Julio del 2021]. Disponible en http://polux.unipiloto.edu.co:8080/00004422.pdf. E-ISSN: 1853-9912.

G0 S.A.S. [en línea]. [Consulta: 18 agosto 2021]. Disponible en: https://g0tech.com/es.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. Decálogo Ciberseguridad empresas: Una guía de aproximación para el empresario [en línea]. España.2017. 13 p. [Consultado: 29 de julio de 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf.

--------.-------- España.2017. 13 p. [Consultado: 31 de julio de 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias. (s.f.).

LÓPEZ DUQUE, Carlos Mario. Diferencia entre seguridad informática y ciberseguridad. En: Colecciones Especialización en Seguridad Informática [en línea]. Universidad Piloto de Colombia, 2018, p.1.[Consultado: 29 de julio de 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8600/Diferencia%20entre%20seguridad%20informatica%20y%20ciberseguridad.pdf?sequence=1&isAllowed=y.

NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-30: Guía para la realización Evaluaciones de riesgo [en línea]. Septiembre de 2012. 17 p. [Consultado: 29 de julio de 2021]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

NIST U.S. DEPARTMENT OF COMMERCE. Publicación Especial del NIST 800-53 Revisión 5: Controles de seguridad y privacidad para organizaciones y sistemas de información [en línea]. Septiembre de 2020. 29 p. [Consultado: 29 de julio de 2021]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (sgsi). Requisitos [en línea]. 22 de marzo de 2006. p10. [Consultado: 29 de agosto de 2021]. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (sgsi). Requisitos [en línea]. 22 de marzo de 2006. p.22.. [Consultado: 29 de agosto de 2021]. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

TEJENA MACÍA, Mayra A. Análisis de riesgos en seguridad de la información. En: Polo del Conocimiento [en línea]. Abril 2018, vol.3, nro.4, p.233-244. [Consultado:

31 de julio de 2021]. DOI 1023857/pc. v3i4.809. Disponible en: http://polodelconocimiento.com/ojs/index.php/es. E-ISSN:2550-682X.

UNIVERSIDAD DE SALAMANCA Departamento de Informática y Automática: Ingeniería de Software I [en línea]. 2020. 17 p. [Consultado: 29 de julio de 2021]. Disponible en: https://repositorio.grial.eu/bitstream/grial/1940/1/IS_I%20Tema%203%20-%20Modelos%20de%20Proceso.pdf.

XIII Seminario Iberoamericano de Seguridad en las Tecnologías de la Información) [en línea]. En:(17: 19-23, marzo 2018: La Habana, Cuba). Implementación del Marco de Trabajo para la Ciberseguridad NIST CSF desde la Perspectiva de Cobit 5. La Habana: GAE, 2018. 13 P. [Consultado: 2 de agosto de 2021]. Disponible en: https://scholar.google.com/scholar?hl=es&as_sdt=0%2C5&q=Implementaci%C3%B3n+del+Marco+de+Trabajo+para+la+Ciberseguridad+NIST+CSF+desde+la+Perspectiva+de+Cobit+5&btnG=.

ANEXOS

Anexos A. Acta de inventario de activos tecnológicos de G0 S.A.S.

SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION G0 S.A.S					
MEMORIA DE REUNION EXCLUSIVA PARA USO EXTERNO REUNIONES EXTERNAS					
CODIGO: SGSI-ID-0002	VERSION :2.0				
Fecha: dd/mm/aa	**02/02/2021**	**Horario Reunión:**	**10:00 am**	**Acta Número:**	**1**
Lugar:	Instalaciones de infraestructura de la empresa G0 S.A.S			**Hora Inicio / fin :**	**10:00 AM 13:00 PM**
ASUNTO DE LA REUNION					
Levantamiento e inventario de información a los activos tecnológicos de la organización.					
TEMAS TRATADOS					
1. Reconocimiento de todas las áreas de la organización 2. Presentación del presidente y gerencia general de G0 S.A.S junto al equipo de tecnología. 3. Entrevista a los coordinadores de cada área 4. Levantamiento de información de la infraestructura tecnológica. • Se hizo reconocimiento de todas las áreas para el levantamiento de información, identificando los activos tecnológicos y procesos que manejan que servirán como insumo para la evaluación de riesgos. • Mediante la presente Acta, el levantamiento de información recolectado es información confidencial recibido por la empresa G0 S.A.S y por lo tanto se hace un acuerdo de confidencialidad del tratamiento recolectado es para fines educativos y no podrá ser revelado a terceros o personas no autorizadas. • Se define la finalidad y el alcance que será considerado en la evaluación de riesgos.					
SEGUIMIENTO A COMPROMISOS ADQUIRIDOS					
• Las encuestas y entrevistas para la recolección de datos deben cumplir con el acuerdo de confidencialidad • Se comunicará los resultados arrojados en la evaluación de riesgos.					

Fuente: Autores de la Investigación