PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTC ISO/IEC 27001:2022 PARA EL GRUPO EMPRESARIAL ASERTEMPO – POLIFUNCIONALES

TRABAJO DE GRADO PARA OPTAR AL TITULO DE ESPECIALISTA EN SISTEMAS DE GESTIÓN INTEGRADAS DE LA CALIDAD, MEDIO AMBIENTE Y PREVENCIÓN DE RIESGOS LABORALES

FUNDACIÓN UNIVERSITARIA AGRARIA DE COLOMBIA

FACULTAD DE CIENCIAS ECONOMICAS, ADMINISTRATIVAS Y CONTABLES

ESPECIALIZACIÓN EN SISTEMAS DE GESTIÓN INTEGRADAS DE LA CALIDAD, MEDIO AMBIENTE Y PREVENCIÓN DE RIESGOS LABORALES

BOGOTÁ D.C.

2024

PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTC ISO IEC 27001:2022 PARA EL GRUPO EMPRESARIAL ASERTEMPO – POLIFUNCIONALES

Stefany Jamaica Rojas

Estudiante del Programa de Especialización En Sistemas De Gestión Integradas De La Calidad, Medio Ambiente Y Prevención De Riesgos Laborales

JAMAICA.STEFANY@uniagraria.edu.co

Director: Germán Andrés Sánchez Ortegón

gsanchez@escae.com.co

Modalidad: TRABAJO DE GRADO

FUNDACIÓN UNIVERSITARIA AGRARIA DE COLOMBIA

FACULTAD DE CIENCIAS ECONOMICAS, ADMINISTRATIVAS Y CONTABLES

ESPECIALIZACIÓN EN SISTEMAS DE GESTIÓN INTEGRADAS DE LA CALIDAD, MEDIO AMBIENTE Y PREVENCIÓN DE RIESGOS LABORALES

BOGOTÁ D.C.

2024

Contenido

Tabla De Contenido

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

1. ANTECEDENTES

Con el fin de investigar los avances obtenidos en las cuestiones internas y externas que puedan afectar de alguna manera la seguridad de la información basada en la NTC ISO/IEC 27001:2022 se relaciona de manera cronológica la presente norma; iniciando desde el año 1995 con su versión inicial, redactada por el Departamento de Comercio e Industria (DTI), desde el Reino Unido, en el año 1999 se generan nuevos estándares encaminados a las buenas experiencias en gestión de seguridad y normas para la gestión de riesgos (Rodríguez, Cruzado, Mejía, & Alarcón, 2020).

A finales de la década pasada la norma fue actualizada y complementada, lo cual modificó y estableció las recomendaciones para evaluar y certificar el sistema de gestión de seguridad de la información, convirtiéndola de la NTC ISO 17999 de diciembre de 2000, en donde se evidencian las directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económico) en materia de privacidad, seguridad de la información y Criptología, a partir del año 2002, la norma adquiere una nueva denominación, NTC ISO/IEC 27001:2022 (Velasco, 2008).

Entre los años 2001 al 2004 se revisaron y actualizaron las NTC ISO/IEC las que se difundieron en el año 2005, generando un impacto de la vulnerabilidad de la información perteneciente a la empresa, años posteriores a través de un estudio enfocado en la mejora de los procesos a través de la NTC ISO IEC 27001:2022 se determinó que, ante factores de riesgo existente, los planes de mejora garantizan los aspectos de integridad, disponibilidad y accesibilidad, a partir de esta investigación se logró disminuir los niveles de riesgo y se empleó la NTC ISO/IEC 27001:2013 (Rodríguez, Cruzado,

Mejía, & Alarcón, 2020).

En la actualidad existe la NTC ISO/IEC 27001:2022, la cual tiene como objeto y campo de aplicación, especificar los requisitos para el establecer, implementar, mantener y mejorar continua de un sistema de gestión de la seguridad de la información en el contexto de la organización (ISO, 2022).

Además de ello, también es importante identificar el enfoque que ha tenido esta norma, desde la NTC ISO/IEC 27001, la cual establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI) y es aquella que define los requisitos para establecer una política de seguridad, realizar una evaluación de riesgos, y definir controles para proteger la información, por otro lado está la NTC ISO/IEC 27002, la cual es la que proporciona las directrices o guía para la implementación de controles de seguridad de la información, además de contener el catálogo de buenas prácticas para los controles de seguridad.

En igual firma, se puede evidenciar la NTC ISO/IEC 27003, la cual proporciona recomendaciones prácticas y enfoques para la puesta en marcha de un SGSI y se puede ver como una guía de apoyo para las organizaciones, en cómo ponerla en práctica la NTC ISO/IEC 27001 y entender mejor el proceso de implementación.

Con respecto a la NTC ISO/IEC 27004, se centra en el seguimiento, medición, análisis y evaluación del SGSI, la proporciona directrices sobre cómo monitorear y evaluar la efectividad de este, para asegurar que se mantenga y mejore adecuadamente.

Y finalmente se encuentra la NTC ISO/IEC 27005, la cual indica las directrices

para la gestión de riesgos en el contexto de la seguridad de la información, adicionalmente se detalla el proceso estructurado para la identificación, evaluación y tratamiento de los riesgos relacionados con la seguridad de la información, se centra en la gestión de riesgos, complementando la NTC ISO/IEC 27001 en términos de análisis y tratamiento de riesgos.

Cada una de estas normas tiene un enfoque específico y se complementan entre sí para proporcionar una visión integral de la gestión de la seguridad de la información.

Así mismo es de gran importancia mencionar el Comité 1 SC 27 de la ISO, el cual se enfoca en el desarrollo de estándares para la seguridad de la información, ciberseguridad y protección de la privacidad. Este comité trabaja en la creación de métodos, técnicas y directrices para abordar tanto los aspectos de seguridad como de privacidad en la gestión de la información y las tecnologías de la información y comunicación (TICS).

Dentro del comité, se manejan diferentes áreas de Trabajo del SC 27, como lo es:

El sistema de Gestión de Seguridad de la Información (SGSI), a partir del Desarrollo de estándares como NTC ISO/IEC 27001, que especifica los requisitos para establecer, implementar, mantener y mejorar un SGSI.

Criptografía y Mecanismos de Seguridad: Se establecen los estándares relacionados con la protección de la confidencialidad, integridad y disponibilidad de la información mediante técnicas criptográficas.

Evaluación y Pruebas de Seguridad: Métodos y criterios para la evaluación y certificación de la seguridad de productos y sistemas de TI.

Controles y Servicios de Seguridad: Directrices para la implementación de

controles de seguridad y servicios de gestión de la seguridad.

Gestión de Identidad y Tecnologías de Privacidad: Estándares para la gestión de identidades y la protección de datos personales.

Por ende, el trabajo del SC 27 es crucial para asegurar que las organizaciones de todo el mundo puedan gestionar sus riesgos de seguridad de la información de manera efectiva, cumpliendo con las normativas y protegiendo la privacidad de los datos en un entorno digital en constante evolución.

2. FORMULACIÓN DEL PROBLEMA

2.1. Descripción del problema

En la actualidad el Grupo empresarial Asertempo – Polifuncionales, es una empresa EST (Empresas de Servicios Temporales), que presenta servicios de administración de personal temporal, desde la selección y contratación, estudios de seguridad, nómina y servicios de Outsourcing de Seguridad Y Salud en el Trabajo.

A partir de los servicios anteriormente mencionados, se puede identificar que el uso de la tecnología de la información y comunicaciones (TIC) es alta, lo cual supone que la información que maneja la compañía es de carácter confidencial y la cual debería llevar un control específico o generar un ciclo de vida, desde la creación de la información, identificación de su valor y también a los riesgos a los que están expuestos, los cuales deben gestionarse de manera prudente y con medidas de seguridad que permitan ganar y mantener la confianza de los usuarios en el servicio.

Adicionalmente, en la actualidad la empresa está certificada en ISO 9001:2015, la cual exige garantías de calidad a sus proveedores, motivo por el cual la compañía

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

busca estandarizar sus procesos, garantizar la seguridad de los mismos, asegurar la confidencialidad, integridad y disponibilidad de todos sus recursos frente al cliente.

De esta manera, como no se evidencia dichos controles o manejo de la información, se tiene un riesgo en situaciones futuras, generando violación de la seguridad de la información, eventos de seguridad de la información, incidentes en cuanto a la seguridad de la información, sanciones económicas, pérdida de información sensible, a partir de ataques cibernéticos tanto del personal de administrativo, como del personal en misión, cliente, contratistas y demás partes interesadas de la empresa.

Y se pretende que con la implementación del SGSI, generar sentido de pertenencia y compromiso de todos los involucrados a la seguridad de la información, ciberseguridad y protección de la privacidad.

2.2. Pregunta de investigación

¿Cómo implementar un Sistema De Gestión De Seguridad De La Información conforme a los requisitos de la NTC ISO/IEC 27001:2022 en el Grupo Empresarial Asertempo – Polifuncionales para garantizar la protección de la información y activos relacionado de la organización?

3. JUSTIFICACIÓN

Al establecer un Sistema de Gestión de Seguridad de la Información (SGSI), le permitirá al Grupo Empresarial Asertempo – Polifuncionales, implementar los controles adecuados sobre la confidencialidad, disponibilidad e integridad de la información, protegiendo de esta manera la información de todas las partes interesadas, además del cumplimento en la NTC ISO/IEC 27001, lo cual permitirá darle un plus a sus clientes, en

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

cuanto a la seguridad de la información, siendo la base para la gestión de riesgos de seguridad y así mismo la determinación de los niveles de protección que se requiere.

A través de la presente investigación se podrá identificar la cantidad de información que tiene la organización, la naturaleza de la misma, el tipo de incertidumbre que puede afectar los resultados y objetivos tangibles como intangibles, la forma de definirla, predecir y medirla según las consecuencias que puede tener. Además de ello, determinar el nivel de riesgo, la probabilidad de ocurrencia y la capacidad que tiene la organización frente a este tipo de criterios de la seguridad de la información.

Es de gran importancia para la organización identificar los criterios de valoración de los riesgos, dado que a partir de ello es cómo se determina la importancia de estos, en términos de sus consecuencias, probabilidad y nivel de riesgo y posteriormente se podría desarrollar y especificar en términos de magnitud del daño o pérdida de confidencialidad, integridad y disponibilidad de la información para la organización.

De esta manera, la comunidad beneficiada en específico con este proyecto toda vez se realice, sería el Grupo empresarial Asertempo – Polifuncionales, incluyendo personal de planta y en misión, desde el riesgo del tráfico de datos personales, generando técnicas de ingeniería social de diferentes vías (telefónica, digital, entre otros), con el fin de tener acceso a la información personal, financiera o datos sensibles para lucrarse económicamente.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

4. OBJETIVOS

4.1. Objetivo General

Elaborar un plan de Implementación del Sistema de Gestión de Seguridad de la Información basado en la NTC ISO/IEC 27001:2022 para el Grupo Empresarial Asertempo – Polifuncionales.

4.2. Objetivos Específicos

1. Realizar un diagnóstico del estado actual, en cuanto al cumplimiento de la NTC- ISO/IEC 27001:2022 en el Grupo empresarial Asertempo – Polifuncionales.
2. Identificar las prácticas y controles de seguridad de la información definidos en la NTC- ISO/IEC 27001:2022, que sean aplicables y relevantes para el contexto específico del Grupo empresarial Asertempo – Polifuncionales.
3. Formular las acciones de mejora para la implementación de la NTC-ISO/IEC 27001:2022, del SGI en el Grupo empresarial Asertempo – Polifuncionales.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5. MARCO DE REFERENCIA

Actualmente en las empresas, no solamente depende la calidad de los servicios que se presenta, sino que también es un factor determinante en la competencia en el mercado, la adaptación que se tiene a las nuevas tecnologías y a adquirir nuevos métodos de seleccionar, contratar, prestar el servicio o incluso el manejo del área de Seguridad y salud en el trabajo, que en muchas ocasiones se maneja de manera tangibles o intangibles, y se adquiere información desde los diferentes procesos, como los siguientes:

TIPO DE ACTIVOS	DESCRIPCIÓN	PROCESOS	USO
Bases de Datos	Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.	Selección Nomina Proveedores Financiera	Bases de datos con información personal o con datos relevante, bases de datos de nóminas, Base de datos Aprendices, Listado de proveedores, estados financieros

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Datos / Información	Información vital para la ejecución de la misión de la organización, así mismo puede ser información personal definida específicamente en el sentido de las leyes nacionales relacionadas con la privacidad o incluso información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exige un largo tiempo.	Calidad TI Seguridad y salud en el trabajo Contratación Financiera	Copias de Respaldo, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad, Matrices de Roles y Responsabilidades , Datos de Prueba, Contratos, acuerdos de confidencialidad, manuales de usuario,

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

	procedimientos administrativos, operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, formatos o formularios físicos o digitales, registro de clientes, entre otros

Hardware / Infraestructura	Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.	TI	Servidores, Equipos de Escritorio (Pc), Equipos Portátiles, Dispositivos Móviles, Equipos de Respaldo, Dispositivos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Soporte de la Red, Módems, Conmutadores Central Telefónica, Telefonía IP.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Software	Consiste en todos los programas que contribuyen al funcionamiento en conjunto de procesamiento de datos	Nomina Servicio Seguridad Seguridad y salud en el trabajo	Software de contabilidad, Software de nómina, Software para la gestión de competencias del personal, Software de tiempo trabajado y tiempo muerto, Software teletrabajo, Software de estudios de seguridad, Software de aplicación de Riesgo Psicosocial
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.		Ambiente externo: Domicilio del personal, instalaciones de otras organizaciones.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

			Instalaciones: Edificación de la organización.
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.	Servicio Selección Contratación Nomina Seguridad y salud en el trabajo	Personal a cargo de la toma de decisiones: Alta gerencia y lideres de procesos. Usuarios, personal de operación/ mantenimiento: Gestión de servicios, Gestión de TI.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Red	Tipos de red, la cual consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios sistemas de información	Red Telefónica, Red Inalámbrica, Telefonía Móvil, Red Local (LAN), Internet.
Soportes de Información	Dispositivos físicos o electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo y que posteriormente permiten recuperar la información contenida en ellos.	Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.

Tabla 1: Procesos del grupo empresarial Asertempo – Polifuncionales (Creación propia)

De acuerdo con lo anterior, se debe tener en cuenta lo siguiente; la información la tienen diferentes procesos en el transcurso del servicio, para ello es importante tener ciertos parámetros de seguridad establecidos, para que no se materialice un

riesgos ante la organización o sus partes interesada, teniendo en cuenta este panorama es importante aclarar el término información, entendiéndolo como, aquel conjunto de datos ordenados que cumplen con ciertas características, tales como: pertinente, relevante, oportuna, precisa y accesible (Martínez, 2019).

Ahora bien, frente a esa información de los diferentes procesos, se debe tener presente el término seguridad de la información, entendiéndolo como conjunto de técnicas que se requieren para proteger y salvaguardar la información que de alguna manera es importante para la función de la organización (Martínez, 2019).

Además de tener como objetivo principal la protección de los datos con el fin de evitar la pérdida, modificación o divulgación no autorizada de la información, dado que aquellos sucesos ocasionan pérdidas significativas en las organizaciones en los procesos administrativos, operativos, afectando directamente la economía de las organizaciones (Restrepo, 2017).

Y, por otro lado, la seguridad de la información se encarga del diseño de normas, procedimiento, método y técnicas, consiguiendo de esta forma un sistema de información seguro y confiable (Moyano & Suarez, 2017).

Para establecer un Sistema de Seguridad de la información es necesario establecer cierto puntos como lo son: Los elementos que componen el sistema, los peligros que afectan al sistema y cuales son la medidas que se debería acoger para lograr conocer y prevenir los riesgo potenciales, así mismo identificar quien el personal idóneo para obtener el acceso y la modificación a cierta información y poder considerar este sistema cuando tenga los tres elementos importante, que son (Moyano & Suarez, 2017):

1. Integridad: Por medio de ella se garantiza que los datos no

han sido alterados o destruidos de modo no autorizado, es decir que se garantice la autenticidad de la información y sin importar el momento.

2. Confidencialidad: Se refiere al atributo que debe tener los datos o la información, al encontrarse únicamente al alcance de las personas o las entidades autorizadas.

3. Disponibilidad: Se debe garantizar que la información se encuentre disponible para los usuarios siempre que se necesite (Moyano & Suarez, 2017).

5.1. Estado del Arte:

En la actualidad en las empresas en Colombia se han generado diferentes cambios de gran importancia en cuanto a los procesos de vinculación formal de los trabajadores, esto se puede ver reflejado en la forma de contratación que actualmente están adoptando las organizaciones, apoyándose en las empresas de servicio temporal para recibir a los empleados que cubrirán las vacantes ofertadas, de acuerdo con la definición de la ley número 50 del 28 de diciembre de 1990: “Las Empresas de Servicios Temporales (EST) son aquellas que prestan un servicio para ayudar de forma temporal en el desarrollo de actividades a una empresa. El servicio se ejecuta mediante el envío de trabajadores en misión” (Congreso de la República, 1990).

Dentro del proceso de estas compañías se identifica una rotación constante, en donde el 60% de los ex empleados al momento de su salida se llevan los datos sensibles de la empresa, los cuales pueden ser publicados de manera inescrupulosa, poniendo en gran riesgo dicha información confidencial, por esta razón es importante que al momento de incorporar un empleado se deben evaluar de manera imparcial los componentes éticos

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

que influyan en sentido positivo para la seguridad de la información, tomando como premisa esta como una cultura organizacional (Martínez, 2019).

Ante la situación anteriormente mencionada e identificando otras situaciones externas que puede afectar a la empresa, la seguridad de la información es una estrategia, para apoyar en el proceso de mitigar los riesgos a los cuáles están expuestos y evitar sanciones legales, en Colombia el respaldo legislativo promulgó con la Ley 1273 de 2009, la cual tiene como objetivo modificar el Código Penal, para crea un nuevo bien jurídico tutelado denominado, la Protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Congreso de Colombia, 2009).

Estudio anteriores han identificado la importancia de la seguridad de la información en diferentes entidades, como es el caso del autor Oscar Zaque (2018), el cual realizó un proyecto para la implementación del SGSI, teniendo como objetivo que la empresa responda de la manera más eficiente y minimice los riesgos que se presenten ante las amenazas, el enfoque utilizado es basado en procesos para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el Modelo de Seguridad de la Información y estar orientado a todos los actores y entidades involucradas que permite mantener un proceso de mejora continua brindando una seguridad razonable para la proyección financiera y tecnológica.

Por otro lado se encuentra la investigación de los autores Guzmán y Taborda (2015), denominada “Diseño de una sistema de gestión de la seguridad informática - SGSI - para empresas del área textil en la ciudad de Itagüí, Medellín y Bogotá D.C, a través de la auditoría”, en donde se indican las prácticas apropiadas para el desarrollo e

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

implementación de cada uno de sus componentes, estableciendo las fases, documentación, procedimientos requeridos y exigidos de acuerdo a la NTC ISO/IEC 27001:2015, en donde se concluye en aspectos importantes; la cual involucra los recursos económicos limitados que tienen este tipo de organizaciones (Pymes), razón por la cual no pueden establecer y/o mantener un sistema de seguridad robusto y por ende lo que se deba implementar debe satisfacer las necesitas de las pequeñas empresas, en el cual cada uno de los componentes informáticos, juegan un papel de gran importancia para permanecer en el mercado, así mismo se debe proporcional metodología sencilla, muy completa para proteger cada uno de los activos informáticos.

De acuerdo con esta investigación se puede inferir que, para realizar una implementación de un SGSI, se debe tener en cuenta el tamaño de la organización, los procesos a incluir dentro del alcance del sistema, la criticidad de la información que se maneja, la tecnología utilizada y que se dispone dentro de la organización y las disposiciones legales a enfrentar.

5.2. Marco Histórico

Dentro del grupo empresarial, actualmente se cuenta con la certificación de ISO 9001:2015, lo cual hace que se tenga la política de calidad, la cual hace referencia a cumplir con el compromiso empresaria, garantizar a los clientes calidad y oportunidad en el servicio, medir, controlar y hacer rentable todos sus procesos, pero adicionalmente se tiene un objetivo desde el proceso de seguridad, queriendo establecer tecnología de punta en sus principales procesos, seguridad para todos los involucrados en el grupo y minimizando los riesgos y peligro con respecto a la seguridad de la información (Asertempo Colombia S.A, 2023).

En el presente año, se identificó que esta actividad se intentó implementar anteriormente en la compañía, pero no fue exitosa, dado que no se contaba con la persona experta, ni con la identificación de la norma para encontrar diversas metodologías y normas con las cuales se pueda implementar un SGSI, tales como la norma técnica NTC ISO/IEC 27001:2022, la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2022), entre otras.

Para conocer el estado actual del Grupo empresarial Asertempo – Polifuncionales, se realizará un diagnóstico base, a la implementación del Anexo A de la NTC- ISO/IEC 27001:2022 por parte de la empresa; de tal forma que se pueda definir el estado actual y el resultado esperado tras la propuesta de implementación del SGSI que plantea este trabajo.

Estrategia Desarrollada

De acuerdo con las metodologías seleccionadas, se establecer el modelo de PDCA (Plan- Do- Check- Act), propuesto por Deming (1986), siendo una estrategia de mejora continua de la calidad en cuatro pasos,

1. PLAN (Planificar): Establecer los objetivos y procesos necesarios para obtener los resultados de acuerdo con el resultado esperado. Al tomar como foco el resultado esperado, difiere de otras técnicas en las que el logro o la precisión de la especificación es también parte de la mejora.
2. DO (Hacer). Implementar los nuevos procesos. Si es posible, en una pequeña escala.
3. CHECK (Verificar): Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora esperada y Documentar las conclusiones.

4. ACT (Actuar): Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario. Aplicar nuevas mejoras, si se han detectado errores en el paso anterior y documentar el proceso.

A partir de lo anterior, la información se debe construir con base en metodologías existentes que puedan ser aplicadas a las organizaciones, para ello se hace referencia a los aspectos de las NTC ISO/IEC 27001:2022, Sistema de Gestión de Seguridad de la Información, a través de un análisis de brechas GAP, entiendo como un método para evaluar las diferencias de rendimiento entre los sistemas de información de una empresa o las aplicaciones de software para determinar si se cumplen los requisitos de un SGSI en la organización (ISO, 2022).

5.3. Marco Teórico:

El desarrollo del presente proyecto no tiene como objetivo establecer nuevas bases teóricas, dado que se apoya en ciertos conceptos que permiten el avance hacia el objetivo propuesto: Elaborar un plan de Implementación del Sistema de Gestión de Seguridad de la Información basado en la NTC ISO/IEC 27001:2022 para el Grupo Empresarial Asertempo – Polifuncionales. Para ello, en el desarrollo del proyecto se destacan diferentes términos como lo son:

- Activo: Es un recurso del sistema de información, necesario para garantizar el correcto funcionamiento de los procesos de la organización. También son fundamentales para lograr los objetivos definidos por la organización y

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

requieren de una especial protección.

- Vulnerabilidad: Es la probabilidad de que una amenaza se materialice sobre un activo. Para identificar y estimar una vulnerabilidad, es necesario conocer los distintos activos del sistema de información y las amenazas y riesgos que puede sufrir.
- Riesgo: Permite estimar las probabilidades de que una amenaza se materialice sobre los activos de la organización, causando efectos negativos o pérdidas (económicas, reputacionales, etc.).
- Gestión de Riesgos: Según el nivel del riesgo al que se someten los activos de una organización, se encuentran diferentes alternativas para su gestión. La política de gestión de riesgos decide qué tipo de control se implementa en el sistema de información.
- Información confidencial: Entendido como la información que no se pretende poner a disposición o divulgar a personas o entidades o procesos no autorizados.

Con el fin de investigar los avances obtenidos en la seguridad informática basada en la NTC ISO/IEC 27001:2022 se consultó en diferentes proyectos que permiten visualizar y contextualizar la seguridad de la información, en empresas de servicios temporales (EST), de acuerdo con los resultados obtenidos en los siguientes proyectos:

De acuerdo a la investigación de los autores Matiz y Rueda (2020), que tuvo como objetivo el diseño de un modelo de seguridad y privacidad de la información enfocado en las empresas de empleo temporal, se puede identificar qué información a nivel de seguridad informática, se manejan a nivel interno en las EST, siendo este el primer pasó que se debe realizar, para que se pueda identificar; quien maneja la información

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

importante, realizar el análisis de qué riesgos tiene o se está expuesto en la empresa e identificar el nivel de madurez que permitirá medir las capacidades de la empresa con el objetivo de buscar las formas de conseguir una mejora

Por otro lado, cabe resaltar que adoptar estándares de seguridad de información es un factor clave para gestionar los intereses de las organizaciones, construyendo una cultura de seguridad y continuidad del negocio, a partir del estándar ideal para implementar un Sistema de Gestión de la Seguridad de la información (SGSI) , el cual proporciona elementos para alcanzar y mantener buenos niveles de seguridad en la información , aumentando los niveles de productividad para conseguir una ventaja competitiva frente a las demás empresas (Martínez, 2019).

Y al mismo tiempo, se puede identificar que hoy en día es uno de los muchos riesgos que se evidencian dentro de las compañías, como los que presentarán a continuación:

El ransomware es una forma de ataque cibernético que encripta los datos del usuario y exige un pago para proporcionar la clave de descifrado. Es una de las amenazas más disruptivas y costosas en la actualidad (Anderson, 2020).

SQL Injection es una vulnerabilidad que permite a los atacantes ejecutar comandos SQL maliciosos en una base de datos, lo que puede llevar al acceso no autorizado a datos sensibles o a la corrupción de datos (Halfond, Viegas & Orso, 2006).

Insider Threats, amenaza que proviene de individuos dentro de la organización, ya sea empleados, contratistas o socios, que abusan de su acceso a los sistemas para causar daño o robar información, estas amenazas internas representan un riesgo significativo para la seguridad de la información, ya que los empleados y otros individuos con acceso legítimo pueden abusar de su posición para comprometer la integridad de los

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

sistemas y datos (Chaudhary, Vasileios & Katsikas,2023).

Así mismo una acción que últimamente es recurrente, son fraudes por falso WhatsApp, en donde las personas inescrupulosas duplican perfiles, utilizan datos públicos de publicaciones anteriores, solicitan dinero por actividades relacionadas a las empresas y con esta información cometen delitos vinculados a la afectación de la reputación de las personas, estafas, extorsión, entre otros.

Por otro lado, se evidencia fugas de información de cualquier índole que pueden generar implicaciones jurídicas y económicas, dado que existe un tratado internacional que proporciona un marco legal para combatir el cibercrimen, el cual establece directrices para la cooperación internacional, la recopilación de pruebas y la penalización de delitos informático (Seger, 2012).

En Colombia existe normatividad legal vigente, la cual apoya a minimizar estos actos, como lo es la Ley 1273 de 2009, la cual representa un avance significativo en la legislación colombiana para combatir los delitos informáticos, alineando las penas con la gravedad de los actos y proporcionando un marco para la protección de sistemas informáticos, en cuanto a las implicaciones penales reglamenta que “penas de prisión que pueden variar de 1 a 10 años, dependiendo de la gravedad del delito. Por ejemplo, el acceso no autorizado a sistemas puede ser castigado con prisión de 1 a 4 años” (Congreso de Colombia, 2011).

Así mismo se puede identificar la Ley 1732 de 2014, la cual refuerza el marco legal para el combate del fraude electrónico en Colombia, proporcionando sanciones específicas que abordan las nuevas formas de delitos financieros en el entorno digital (García, 2015).

5.4. Marco Conceptual:

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

De acuerdo con los autores Matiz y Rueda (2020), indican que existen cinco fases que componen el SGSI, y donde se permite que la seguridad y la privacidad de la información sea un sistema de gestión sostenible dentro de las EST, en primer lugar, se encuentra la fase del diagnóstico, seguido de la fase planificación, posteriormente la tercera fase de implementación, la cuarta fase de evaluación del desempeño y la quinta fase de mejora continua.

A partir de ello, en la primera fase de diagnóstico, se pretende identificar el estado actual de seguridad y privacidad de la información, para que, de acuerdo con este diagnóstico se pueda clasificar la organización en el esquema del nivel de madurez en el que se encuentran la empresa frente a su nuevo SGSI, de acuerdo con los siguientes niveles:

Ilustración 1. Niveles de Madurez frente al SGSI (Matiz & Rueda, 2020)

Entendiéndose los niveles de la siguiente manera:

- Nivel 0: Inexistente. Para este nivel no se desarrollaron procesos ya que lo que se busca es contar con un ambiente propicio para la implementación del modelo y en esta instancia aún no se ha iniciado la evaluación como tal.
- Nivel 1: Inicial. Los resultados de calidad obtenidos en el proceso son impredecibles, sin control, reactivo y son consecuencia de las personas y de las herramientas que emplean. Este nivel no depende de los procesos previamente definidos por la organización, ya que estos no existen o no son utilizados
- Nivel 2: Gestionado. Se considera cuando se llevan a cabo prácticas básicas de gestión de proyectos (costos, cronograma, funcionalidad), de gestión de requisitos, control de versiones y de los trabajos realizados por subcontratistas. Los equipos de los proyectos pueden aprovechar las prácticas realizadas para aplicarlas en nuevos proyectos.
- Nivel 3: Definido. Los procesos comunes para desarrollo y mantenimiento del software están documentados de manera suficiente en una biblioteca accesible a los equipos de desarrollo. Las personas han recibido la formación necesaria para comprender los procesos.
- Nivel 4: Gestionado cuantitativamente. La organización mide la calidad del producto y del proceso de forma cuantitativa con base en métricas establecidas. La capacidad de los procesos empleados es previsible, y el sistema de medición permite detectar si las variaciones de capacidad exceden los rangos aceptables para adoptar medidas correctivas.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

- Nivel 5, integración de los componentes certificados en sistemas compuestos y su certificación (Henao & Lopera, 2007).

En su segunda fase, empleando los resultados de la fase anterior, se procederá a elaborar un plan de seguridad de la información con el propósito de definir las acciones a implementar y definir los límites sobre los cuales se implementará en SGSI, se realizará la revisión de contexto de la organización, necesidades y expectativas, por otro lado se busca identificar el liderazgo de la compañía, las responsabilidades y autoridades para la implementación de este sistema de gestión, posteriormente se realizará un cronograma de los objetivos, planes a desarrollar y acciones para abordar las responsabilidades y finalmente en esta fase se revisarán los soportes de recursos, competencias, comunicación y documentación (Matiz & Rueda, 2020).

Continuando con la tercera fase de planeación, la empresa determinara que información documental requiere en la medida necesaria para tener la confianza que todos sus procesos, personas involucradas y los servicios, se han llevado a cabo según lo planificado, además de llevar el control de cambios que permitan tomar acciones para mitigar efectos adversos cuando sea necesario (Matiz & Rueda, 2020).

A partir de lo anterior, se prosigue a la cuarta fase de desempeño, donde se deberá crear un plan que contemple actividades como: monitoreo, medición, análisis, evaluación del sistema de gestión de seguridad de la información, auditoria del mismo y la revisión por la alta dirección, dando continuidad a la quinta fase donde se procura consolidar los resultados obtenidos de la fase anterior, para diseñar el plan de mejoramiento continuo del SGSI, tomando las acciones oportunas para mitigar las debilidades identificadas (Matiz & Rueda, 2020).

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.5. Marco Legal Normativo:

Norma	
Ley 50 de 1990	Artículo 71: hace referencia a las empresas de servicios temporales en Colombia, la cual indica que se deben cumplir una serie de requisitos, para poder desempeñar la actividad comercial para la cual están facultados. Esta ley hace énfasis en la garantía de los derechos de los trabajadores que son contratados y a su vez son cedidos a las empresas contratantes, asegurando que exista transparencia en el funcionamiento.
Decreto 1530 de 1996	CAPITULO IV, ARTÍCULOS 10 Y 14: En donde se establece la figura de empresa de servicio temporal, el cual tiene como propósito tener a disposición trabajadores contratados de manera temporal cumpliendo con todos los requisitos legales y cederlos a una empresa contratante donde posteriormente el trabajador desempeñará las funciones asignadas por medio de un contrato autorizado.
Ley 1266 del 31 de diciembre del 2008	Habeas Data. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Esta ley desarrolla una regulación integral del derecho fundamental de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en banco de datos y en archivos de entidades públicas y privadas
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1581 de 2012.	La ley colombiana contempla como regulación fundamental la protección que tienen todas las personas naturales en autorizar la

	información personal que puede ser almacenada en alguna base de datos o en cualquier archivo. La cual también aplica para la empresa de servicios temporales, en la recolección de información de candidatos y trabajadores activos o retirados.
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
Decreto 1078 de 2015.	"Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
NTC ISO/IEC 27000:2013	Contiene los términos y definiciones que se emplean en toda la serie, hace referencia Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario; esta recoge los términos y conceptos relacionados con la seguridad de la información, dando una visión general de la familia de estándares de esta área, una introducción a los SGSI y una descripción del ciclo de mejora continua.
NTC ISO/IEC 27001:2013	Norma internacional que especifica los requisitos para un SGSI, proporcionando un marco de trabajo para proteger la información de manera efectiva a través de controles de seguridad.
NTC ISO/IEC 27001:2022.	Norma internacional regulada por la Organización Internacional de Normalización (ISO) y hace una descripción de la gestión que debe cumplir una empresa con respecto a la seguridad de la información.
NTC ISO/IEC 27002:2022	Proporciona directrices para la implementación de controles de seguridad de la información basados en las mejores prácticas
NTC ISO/IEC 27003:2022	Directrices para la implementación de un SGSI.
NTC ISO/IEC 27005:2022	Gestión de riesgos en seguridad de la información.

5.6. Marco contextual

El grupo empresarial Asertempo Colombia y Polifuncionales S.A.S, es una

organización que presta servicios de EST (Empresas de servicios temporales) con más de 12 años de trayectoria en el mercado de la administración del talento humano, cuyo objetivo es prestar servicios en oportunidades de trabajo en empresas clientes. Y, por otro lado, prestadores de servicios complementarios para los procesos de recursos humanos, nómina y Seguridad y salud en el trabajo.

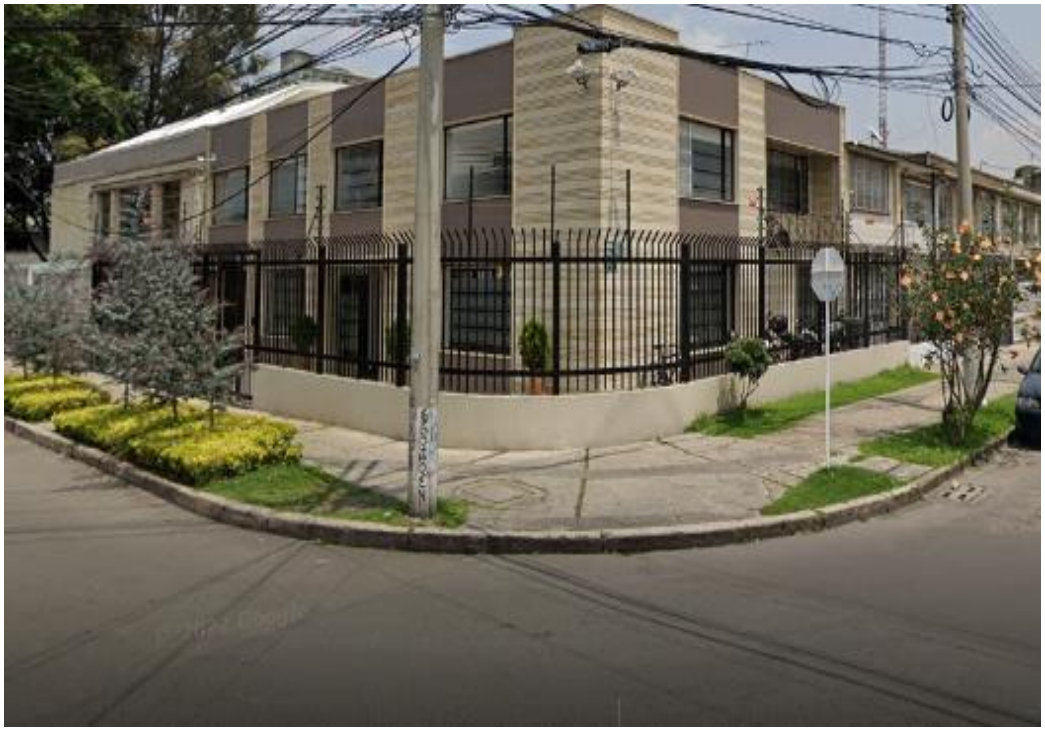
Su misión está establecida desde su experiencia, en el mercado de la administración del talento humano, cuyo objetivo es fomentar el desarrollo integral del empleado, generando una alternativa y oportunidad de trabajo, buscando siempre la satisfacción de las empresas usuarias, todo dentro del marco de la normatividad legal vigente (Asertempo Colombia S.A, 2023).

Actualmente el Grupo empresarial Asertempo Colombia y Polifuncionales S.A.S, es parte de la sociedad de Asociación Colombiana De Empresas De Servicios Temporales (Acoset), siendo un gremio sin ánimo de lucro, “es un gremio sin ánimo de lucro, encargado de fomentar la utilización y desarrollo de las Empresas de Servicios Temporales (EST), como medio de garantía para el empresario, el trabajador en misión, de sostenimiento del desarrollo económico de la nación y sus regiones, la promoción de servicios que benefician a sus trabajadores de planta, en misión y sus familias” (ACOSET, 2023).

Con una visión, de querer ser una empresa que garantice que todos sus procesos críticos cuenten con tecnología de punta, que se cumplan las metas comerciales que se establecieron desde la alta dirección, en las diferentes líneas de negocio, adicionalmente que sus trabajadores puedan desarrollar su labor desde cualquier lugar, con calidad y oportunidad, de forma que les permitan mantener los costos operativos y generar la rentabilidad esperada para el grupo empresarial (Asertempo Colombia S.A, 2023).

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Actualmente ubicada en Bogotá, en la Calle 72 # 22-06



Fuente: Google Maps.

6. DISEÑO METODOLÓGICO

6.1. Tipo de investigación.

Enfoque: El presente proyecto se basa en el análisis cuantitativo de la organización mediante el diagnóstico de la seguridad de la información aplicado en el Grupo empresarial de Asertempo - Polifuncionales, el análisis se basó en la NTC ISO/IEC 27001:2022, para la identificación de las amenazas, vulnerabilidades, controles y riesgos, la probabilidad de ocurrencia y el impacto en caso de materialización. Considerando aspecto de la profundización en el contexto de la organización y que, junto a las herramientas propias del estudio exploratorio, genera una posibilidad de examinar y evidenciar lo que se necesita en la

organización para realizar la implementación de un sistema de gestión de seguridad de la información (Sampieri, Fernández, & Baptista, 2010).

6.2. Método:

Se realizará un estudio con un método que incluyen las entrevistas en profundidad dentro de la organización y se implementará al análisis de contenido, dentro de lo que se revisará la información que tenga la organización, la cual se asocia con la investigación exploratoria (Sampieri, Fernández, & Baptista, 2010).

6.3. Alcance:

Plan de implementación del sistema de gestión de seguridad de la información basado en la NTC ISO/IEC 27001:2022, orientado hacia el grupo empresarial Asertempo y Polifuncionales, de la sede de Bogotá.

6.4. Diseño:

El diseño utilizado está orientado a mejorar la seguridad y la privacidad de la información grupo empresarial Asertempo y Polifuncionales de la ciudad de Bogotá D.C., tomando como guía los controles definidos en la NTC ISO/IEC 27001:2022 y a través de un diagnóstico que lleve a la implementación de los temas que la empresa considere pertinentes y relevantes para aplicar.

Para ello se dispone a dar inicio con el diagnóstico del estado actual de la empresa basadas en los componentes de la NTC ISO/IEC 27001:2022, en su Anexo A, seguido de realizar un análisis de los controles establecidos en la norma y los implementados en las empresas, posteriormente lograr diseñar un plan para a la implementación y finalmente lograr el nivel de madurez en el que se encuentra la empresa.

6.5. Materiales y métodos

El presente proyecto se basa en las siguientes fases:

Etapa	Método
1. Análisis de la situación actual del grupo empresarial Asertempo - Polifuncionales	Consultar la documentación existente en el área de informática, respecto a la seguridad de la información. Poder establecer contacto con el personal encargado del aseguramiento de la información para indagar sobre los procesos, políticas y procedimientos existentes en la protección de la información. Determinar a nivel documental que tiene la compañía en cuanto a contexto de la organización, manejo de liderazgo y compromiso de la organización.
2. Análisis de control y riesgo	Identificar, validar y clasificar los soportes que tiene la organización en materia de recurso, competencias, toma de conciencia, comunicación e información documentada. Y así poder determinar el estado actual de la infraestructura tecnológica de la entidad.
3. Declaración de aplicabilidad	Para determinar la declaración de aplicabilidad, se realizará una

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

	identificación de los riesgos y controles que han sido identificados y analizados en la compañía. El desarrollo de la declaración de aplicabilidad será donde se registran los controles de seguridad que son aplicables según el tratamiento de riesgos, usando como referencia el Anexo A del estándar NTC ISO/IEC 27001 que contiene los controles de seguridad.
4. Propuesta de implementación	Con base a los resultados en el análisis de la situación actual y de la declaración de aplicabilidad de la organización y validando las necesidades que esta requiere se procede a realizar un análisis de seguridad del estado actual de la entidad con respecto a los requisitos de la NTC ISO/IEC 27001-2022. Y posteriormente se realizará la propuesta de implementación y documentación del SGSI.

6.6. **Procedimient**os**:**

Fase 1: Consultar la documentación existente en el área de informática, respecto a la seguridad de la información, así mismo establecer contacto con el personal encargado de la protección de la información de la organización para indagar sobre la política, objetivos, procesos y procedimientos del SGSI relevantes

para gestionar el riesgo y mejorar la seguridad de la información.

Fase 2: identificar y documentar el inventario de activos existente en el área de tecnología, con base a los dominios identificados en la NTC ISO/IEC 27001.

Fase 3: Se realizará una declaración de aplicabilidad, en donde se seleccionarán y se establecerán los controles necesarios según la organización y su actividad económica, en donde se realizará la evaluación de riesgos, requisitos legales, obligaciones adquiridas, mejores prácticas, entre otros, con el apoyo del personal del área tecnológico para la documentación y justificación de la declaración de aplicabilidad.

Fase 4: Realizar un análisis de seguridad del estado actual de la entidad con respecto a los requisitos de la norma ISO/IEC 27001: 2022 y establecer una guía de implementación de la norma para la presente compañía con base a las fases anteriores.

6.7. Población y muestra.

El proyecto se llevará a cabo en la ciudad de Bogotá, la población será el Grupo Empresarial Asertempo y Polifuncionales, ubicados en la carrera 73 No. 22-06. Respecto a la muestra serán basados en el personal que apoyará directamente las diferentes fases del proyecto, dentro de ellas, se encuentra la gerencia, lideres de procesos y toda el área de TI de la compañía.

Análisis estadístico. De acuerdo con la propuesta de Plan de implementación del sistema de gestión de seguridad de la información basado en la NTC- ISO/IEC 27001:2022 para el grupo empresarial Asertempo – Polifuncionales, se hará uso de análisis estadístico exploratorio, el cual consiste en un conjunto de técnicas estadísticas

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

cuya finalidad es entender los datos, detectando aquellas características importantes, como inesperadas y valores atípicos (Figueras & Gargallo, 2003).

7. RESULTADOS

Para el presente proyecto se estuvo orientado al cumplimiento del objetivo general del mismo, conjuntamente con los objetivos específicos, para lo cual, se consideró dividirlo en cuatro fases con sus respectivas actividades, las cuales se han cumplido de forma metódica y optimizada, a continuación, se detalla el desarrollo de cada una de ella:

En la primera fase, se tenía el análisis de la situación actual del grupo empresarial Asertempo – Polifuncionales, el cual se desarrolló a partir de los numérales de la NTC ISO/IEC 27001: 2022, desde el numeral 4 al 10, clasificándolos de acuerdo con lo que tiene en la compañía actualmente; en una escala de criterio determinada de la siguiente manera:

Criterio	Calificación	Porcentaje
No Existe	0	0%
Muy Insuficiente	1	20%
Insuficiente	2	40%
Adecuado	3	60%
Bueno	4	80%
Excelente	5	100%

Tabla 2: Criterio de evaluación para el análisis inicial

En donde se pueden observar los resultados que se obtuvieron a la siguiente tabla:

Numeral	Nombre	Resultado
4	Contexto de la organización	50%
5	Liderazgo	60%
6	Planificación	20%
7	Apoyo	35%

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8	Operación	40%
9	Evaluación del desempeño	13%
10	Mejora	0%
	TOTAL	**31%**

Tabla 3: Análisis de la situación actual de la organización

Dentro de este orden de ideas se puede evidenciar que actualmente la compañía tiene un nivel de cumplimiento del 31% dentro de lo que pide la norma para su implementación, debe señarle que es una empresa que tiene proyectado implementar su SGSI e intento implementarla hace unos años y la cual fracaso, dado que no contaba con un experto en el tema y por temas financieros no podía subsidiar a uno. Para ver los resultados generales dirigirse al Anexo A.

Se plantea así el nivel de madurez que tiene la organización, estando en un nivel 2, en donde se caracteriza por que la organización ha comenzado a implementar procesos y políticas básicas de seguridad de la información, pero estos aún no están completamente definidos ni documentados de manera formal, así mismo se pueden identificar características como lo son:

a. Conocimiento Inconsistente: El conocimiento y manejo de los riesgos clave de la organización es inconsistente, algunas de las capacidades para gestionar los riesgos son limitadas y la información sobre este proceso es informal.
b. Procesos Básicos: Existen algunos procesos básicos de seguridad de la información, pero no están completamente integrados ni formalizados en toda la organización.
c. Documentación Inicial: Se tiene un inicio de la parte documental, algunos procedimientos y políticas, pero esta documentación no es exhaustiva ni

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

está completamente alineada con los estándares internacionales, además la organización cuenta con un desconocimiento a nivel general de estas políticas o los procedimientos ya establecidas.

d. Cumplimiento Parcial: La organización cumple parcialmente con las normativas y estándares de seguridad de la información, pero aún tiene áreas significativas de mejora.
e. Evaluación de desempeño: No se tiene establecidos una forma de realizar un seguimiento, medición análisis y evaluación de lo implementado en el SGSI e incluyendo acciones de mejor.

En cuanto a la segunda fase, del análisis de control y riesgo, se realiza una identificación de los riesgos principales que tiene la compañía en materia de Seguridad de la Información, en primera medida se identifica el control según la norma, en el Anexo A, la descripción, el riesgo asociado y la medida de control, dentro de ello se identificaron los siguientes riesgos

Categoría de Control	Control	Descripción	Riesgo Asociado	Medida de Control
A.5 Políticas de Seguridad de la Información	A.5.1.1	Políticas para la seguridad de la información	Falta de políticas claras puede llevar a incumplimientos y brechas de seguridad.	Desarrollo y comunicación de políticas de seguridad de la información.
A.6 Organización de la Seguridad de la Información	A.6.1.1	Roles y responsabilidades de seguridad de la información	Confusión en roles y responsabilidades puede resultar en fallos de seguridad.	Definición clara de roles y responsabilidades.
A.7 Seguridad de Recursos Humanos	A.7.2.2	Concienciación, educación y formación en seguridad de la información	Falta de formación puede llevar a errores humanos y brechas de seguridad.	Programas de formación y concienciación continuos.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

A.8 Gestión de Activos	A.8.1.1	Inventario de activos	Pérdida o mal uso de activos de información.	Mantenimiento de un inventario actualizado de activos.
A.9 Control de Acceso	A.9.2.1	Gestión de acceso de usuarios	Acceso no autorizado a información sensible.	Implementación de controles de acceso basados en roles.
A.10 Criptografía	A.10.1.1	Política de uso de controles criptográficos	Falta de cifrado puede exponer datos sensibles.	Uso de cifrado para proteger datos sensibles.
A.11 Seguridad Física y del Entorno	A.11.1.1	Controles de seguridad física	Acceso físico no autorizado a instalaciones.	Implementación de controles de acceso físico.
A.12 Seguridad en las Operaciones	A.12.4.1	Registro y monitoreo de eventos	Falta de monitoreo puede permitir actividades maliciosas no detectadas.	Implementación de sistemas de monitoreo y registro de eventos.
A.13 Seguridad en las Comunicaciones	A.13.1.1	Gestión de redes	Interceptación de datos durante la transmisión.	Uso de protocolos seguros para la transmisión de datos.
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.2.1	Requisitos de seguridad de los sistemas de información	Vulnerabilidades en sistemas desarrollados internamente.	Integración de requisitos de seguridad en el ciclo de vida del desarrollo de sistemas.
A.15 Relaciones con Proveedores	A.15.1.1	Política de seguridad de la información para proveedores	Riesgos asociados con proveedores no seguros.	Evaluación y monitoreo de la seguridad de los proveedores.
A.16 Gestión de Incidentes de Seguridad de la Información	A.16.1.1	Responsabilidades y procedimientos de gestión de incidentes	Respuesta inadecuada a incidentes de seguridad.	Establecimiento de procedimientos de gestión de incidentes.
A.17 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	A.17.1.1	Planificación de la continuidad del negocio	Interrupciones en el negocio debido a incidentes de seguridad.	Desarrollo y prueba de planes de continuidad del negocio.
A.18 Cumplimiento	A.18.1.1	Identificación de requisitos legales y contractuales	Incumplimiento de leyes y regulaciones.	Monitoreo y cumplimiento de requisitos legales y contractuales.

Tabla 4: Análisis de control y riesgos de la compañía.

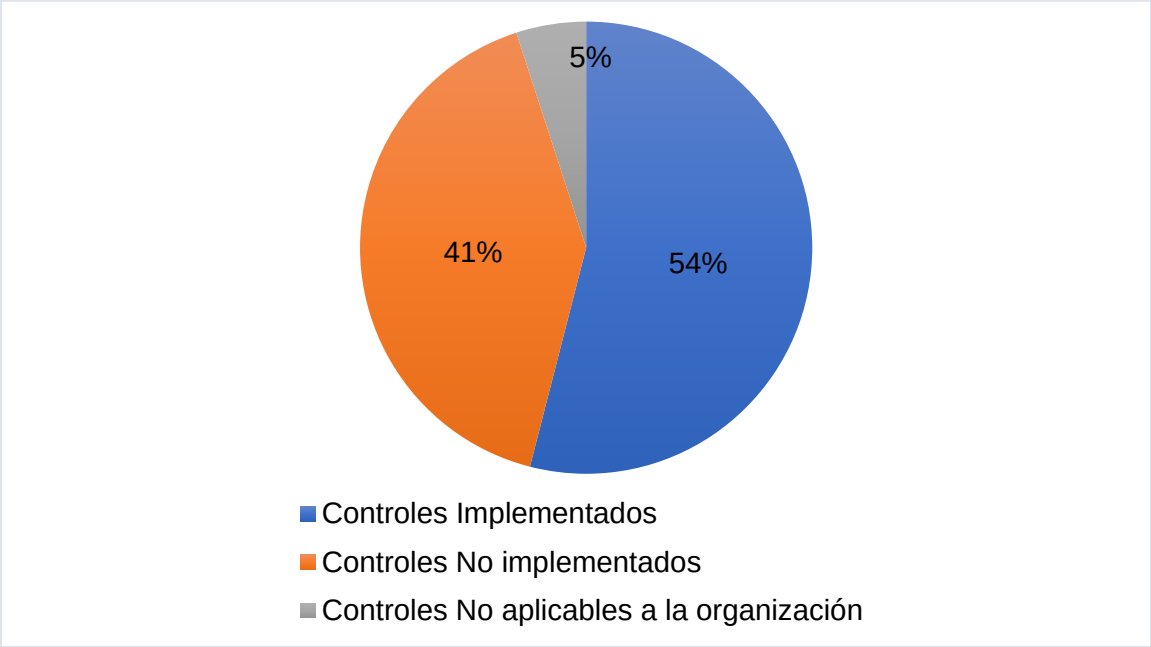
Dando continuidad al proyecto, se realiza la Declaración de aplicabilidad, la cual consiste en realizar una valoración de todos los controles, según el Anexo A de la NTC ISO/IEC 27001:2022, en donde se identifican los controles que solicita la norma, si ya están implementados en la compañía o no, el objetivo del control, la justificación de lo que se tiene o no se tiene en la organización actualmente y el control que debería tener según la norma, para posteriormente realizar la evaluación del cumplimiento y el porcentaje de cumplimiento de acuerdo con los siguientes criterios:

Calificación	Efectividad	Cumplimiento
0	**0%**	No está definido ningún tipo de control
1	**10%**	No existen controles efectivos – Deficiencias considerables con respecto a lo esperado para el requerimiento
2	**50%**	Controles Básicos – Deficiencias menores con respecto a lo esperado para el requerimiento
3	**90%**	El Requerimiento se Cumple en forma efectiva
4	**95%**	Controles Comprehensivos
5	**100%**	Optimizado – Implementación que mejora el estándar

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Tabla 5 Criterios para la de valoración de controles. ANEXO A -NTC ISO/IEC 27001:2022

Por consiguiente, se obtuvieron los siguientes resultados: En cuanto a la cantidad de controles implementados se tienen 58 controles implementados, siendo el 51% de los controles, existen 53 controles no implementados siendo el 47% de los controles y existen 2 controles que no le aplican a la compañía siendo el 2%; como se puede ver en la siguiente gráfica:



Grafica 1: Resultado de controles implementados; no implementados y no aplicables a la organización según el Anexo A de la NTC ISO/ IEC 27001:2022.

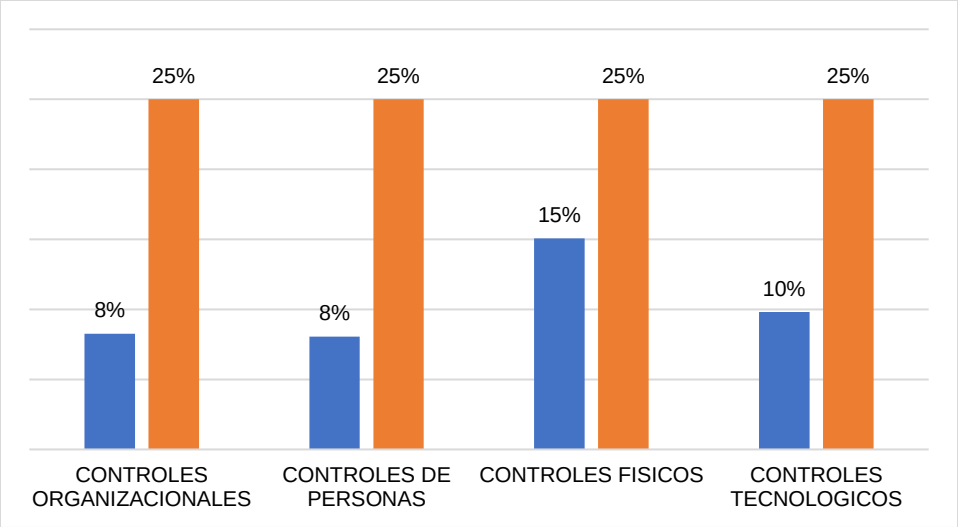
En donde se pudo evidenciar que por cada temática existen la siguiente cantidad de controles implementados y no implementados y el porcentaje de cumplimiento, como se puede ver en la siguiente tabla:

Temas	Implementados	No implementados	N/A	Porcentaje Cumplimiento

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

A.5	CONTROLES ORGANIZACIONALES	**23**	**0**	38%
A.6	CONTROLES DE PERSONAS	2	1	62%
A.7	CONTROLES FISICOS	2	1	78%
A.8	CONTROLES TECNOLOGICOS	21	0	38%
		% DE CUMPLIMIENTO TOTAL		**54%**

De lo cual se infiere que del 100% de los controles que debería tener la compañía, para la implementación de su SGIS, tiene actualmente un 54% de controles implementados, ahora bien, entendiendo que son 4 temáticas y se dará un peso del 25% cada una y se debe dividir por la cantidad de controles que tiene cada temática, por ende, se puede ilustrar de la siguiente manera:



Grafica 2: Resultados por controles de la compañía

Concluyendo las fases del presente proyecto está la propuesta de implementación, a continuación, se proporciona una guía de explicación para implementar la NTC ISO/IEC 27001:2022 en una empresa de servicios temporales, con un enfoque paso a paso y la

documentación requerida, con lo anteriormente realizado del diagnóstico y la identificación de controles y prácticas como lo pide la norma:

Paso 1: Contexto de la organización

Establecer una metodología para la identificación del contexto de la organización, esto con el objetivo de contemplar las Debilidades, Amenazas, Fortalezas y Oportunidades, y se puede identificar desde la matriz DOFA, elaborada de acuerdo con la planeación estratégica de la organización en la cual se analizan factores internos y externos como:

Factores Externos	Factores Internos
1.Físico (Clima)	1. Infraestructura
2.Económico	2. Personal.
3.Tecnológico	3. Metas, objetivos y cultura.
4.Sociocultural	4. Recursos Financieros.
5.Político – Jurídico	
6.Ético	

Tabla 6: Análisis de factores internos y externos

De igual forma se requiere identificar las partes interesadas en los resultados del sistema de gestión de la organización, esto se registra en la Matriz de partes interesadas de la compañía, según el instructivo definido para su diligenciamiento. Esta matriz debe ser actualizada anualmente.

- **Documento:** Matriz de partes interesadas.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Paso 2: Definir el Alcance del SGSI

De acuerdo con los factores internos y externos elaborados en la matriz DOFA, con cada uno de los lideres de proceso, se debe identificar los riesgos a los que está sometido de acuerdo con su proceso, para lo cual se pueden emplear algunos métodos de acuerdo con los lineamientos de la norma ISO 31000 (lluvia de ideas, aporte de experiencias propias y observaciones directas a procesos). Teniendo en cuenta los objetivos y metas que la organización ha identificado y técnicas básicas de análisis que permiten aclarar los criterios que definen los riesgos identificados.

Esto será el paso para determinar qué partes de la organización estarán cubiertas por el SGSI y poder determinar el alcance puede incluir áreas específicas, tipos de servicios, o si se aplicara a toda la empresa.

- **Documentación**: Alcance del SGSI, que debe estar documentado y aprobado.

Paso 3: Identificación de Activos

Se debe realizar una Matriz de Identificación y Valoración de Riesgos de Seguridad de la Información, en donde se deben registrar los ítems de Proceso responsable de gestionar el riesgo, el número de activo de la información y parte interesada.

Para describir el riesgo se debe plantear las preguntas ¿Qué puede suceder, donde y cuando? ¿Por qué y cómo puede suceder?, son algunas de las actividades que se realizan. La identificación incluye riesgos, que, aunque no estén bajo control de la empresa, pueden materializarse y afectar la operación y la imagen de la organización.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Estos activos de información son todo lo que la organización utiliza para gestionar y procesar la información, como equipos, software, datos y personal, y a partir de ello se realiza un inventario de activos.

- **Documentación**: Matriz de Identificación y Valoración de Riesgos de Seguridad de la Información y registro de activos de información.

Paso 4: Evaluación de Riesgos

La descripción de cada uno de los riesgos identificados se encuentra registrados en la "Matriz de Identificación y Valoración de Riesgos de Seguridad de la Información", de igual manera se determinan las consecuencias que implicarían a las partes interesadas la materialización del riesgo y las causas que lo generan o podrían generar. Esta matriz lleva un cuadro de control de cambios donde se registran los cambios que se implementen entre cada una de las versiones, debido a la revisión y actualización de la matriz.

Para cada uno de los riesgos se establecen los siguientes criterios de probabilidad

PROBABILIDAD		
Para cada uno de riesgos identificados, establezca la probabilidad de que cada uno de ellos ocurra usando la siguiente escala.		
CALIFICACIÓN	**DESCRIPCIÓN**	**ESCALA**
INMINENTE	Se espera que el evento ocurra en la mayoría de las circunstancias y/o está ocurriendo ahora.	**10**

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

	El evento de riesgo probablemente ocurrirá en la mayoría de las circunstancias	
ALTA	Se ha recibido una amenaza directa, creíble y/o ya ha ocurrido y/o hubiera ocurrido si no se hubiera impedido activamente varias veces con anterioridad durante el último año.	**7**
	Les ha ocurrido a empresas del sector en el último año.	
MEDIA	El evento de riesgo puede ocurrir en algún momento, pero generalmente solo bajo circunstancias específicas.	**5**
	Se han recibido amenazas indirectas.	
BAJA	El evento de riesgo podría ocurrir en algún momento, pero es muy baja	**3**
	Se han recibido amenazas indirectas.	
	Les ha ocurrido a compañías del sector, pero bajo circunstancias específicas.	
IMPROBABLE	El evento de riesgo podría ocurrir, pero es improbable.	**1**

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

	No se han recibido amenazas creíbles.	

Y de impacto:

CONSECUENCIA DEL RIESGO		
La siguiente parte de la evaluación involucra considerar las consecuencias para la empresa, o el impacto en el negocio si ocurriera el evento de riesgo. Puede haber una probabilidad muy alta de que el evento ocurra, pero si su impacto es muy bajo, no sería lógico gastar tiempo y recursos en manejarlo. Para cada uno de los riesgos incidentes identificados en la tabla "Matriz de riesgos ", determine el impacto potencial en el negocio utilizando esta tabla.		
CALIFICACIÓN	**DESCRIPCIÓN**	**ESCALA**
CRITICO	Pérdida financiera muy significativa. Mayor a 500SMLV. Suplantación de persona.	**10**
	Pérdida de ventaja competitiva e imagen a largo plazo.	
	Si se trata de riesgos de seguridad de la información y se asocia un activo de información cuya criticidad en cuanto a confidencialidad, integridad y disponibilidad es ***Muy Alta***	
ALTO	Perdidas graves cuando hay un siniestro sin recuperación.	**7**

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

	Pérdida financiera significativa superior a 320SMLV e inferior a 500 SMLV.	
	Si se asocia un activo de información cuya criticidad en cuanto a confidencialidad, integridad y disponibilidad es ***Alta.***	
MEDIO	Recuperación parcial	**5**
	Pérdida financiera menor entre 20SMLV e inferior a 320SMLV.	
	Si se asocia un activo de información cuya criticidad en cuanto a confidencialidad, integridad y disponibilidad es Media.	
BAJO	Siniestro con recuperación.	**3**
	Pérdida financiera menor entre 20SMLV e inferior a 200SMLV.	
	Si se asocia un activo de información cuya criticidad en cuanto a confidencialidad, integridad y disponibilidad es ***Baja***.	
	Desprestigio o daño a la imagen y reputación que impacte a las ventas a corto plazo.	

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

MENOR	Perdidas menores cuando los elementos afectados se puedan reparar.	**1**
	Pérdidas financieras mínima menor a 20SMLV.	
	Si se asocia un activo de información cuya criticidad en cuanto a confidencialidad, integridad y disponibilidad es ***Muy Baja***	

El nivel probable de riesgo se determinará aplicando la siguiente fórmula:

Probabilidad * Consecuencia = Nivel Probable de Riesgo (NPR)

Teniendo en cuenta que el máximo de calificación es 100 puntos, se establece la siguiente escala de nivel probable del riesgo:

CLASE	**NIVEL PROBABLE DE RIESGO**
Bajo	1 a 9
Medio	10 a 24
Alto	25 a 48
Muy Alto	49 a 100

Tabla 7: Criterios para determinar los niveles de probabilidad

Posteriormente se debe realizar el análisis de riesgos para identificar vulnerabilidades y amenazas que puedan afectar a los activos. Luego, se evalúa la probabilidad y el impacto de cada riesgo para priorizar su tratamiento.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

- **Documentación**: Matriz de Identificación y Valoración de Riesgos de Seguridad de la Información.

Paso 5: Tratamiento de Riesgos

Habiendo identificado los riesgos existentes que ha determinado la compañía, se identifican los controles para establecer el tratamiento de ello, posteriormente se realiza nuevamente una evaluación de la consecuencia y la probabilidad. Teniendo en cuenta la siguiente tabla**:**

ESCALA	DESCRIPCIÓN
10	No existen controles ni defensas
7	Los controles / defensas son limitados y no están documentados
5	Los controles / defensas son limitados y están documentados
3	Los controles / defensas son efectivos, pero no están documentados
1	Los controles / defensas son efectivos y están documentados

Tabla 8 criterios de evaluación de la consecuencia y la probabilidad

Dentro de este tratamiento se desarrolla un plan de acción para mitigar los riesgos y esto puede incluye controles como procedimientos, políticas, medidas tecnológicas y formación.

- **Documentación**: Plan de tratamiento de riesgos.

Paso 6: Seleccionar Controles de Seguridad

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Con base en la evaluación de riesgos, se continuará con la selección de los controles de seguridad adecuados en el Anexo A de la NTC ISO/IEC 27001:2022 (contiene 93 controles divididos en 4 controles). Estos controles pueden ser tecnológicos, organizacionales, físicos o de personas.

Y posteriormente determinar las acciones pertinentes las cuales deben ser proporcionales de acuerdo con el impacto en la conformidad de los productos y servicios.

Además de ello, se debe considerar aspectos importantes como lo son: Eliminar, Transferir, Tratar, Retener o compartir el riesgo, para su intervención**.**

Eliminar: Cuando se puedan implementar acciones que lleven a desaparecer el riesgo, se debe pensar en eliminar el riesgo.

Transferir: Si se puede mejorar cuando se transfiere el riesgo a un tercero que pueda responder.

Tratar: Si es viable y hay disponibilidad de recursos, tomar acciones para tratar el riesgo y mejorar.

Retener: Se toma este tratamiento cuando se puedan mejorar, pero es imprescindible mantener los controles existentes.

Compartir: Si las acciones para tratar el riego se deben involucrar terceros, para conjuntamente controlar y responder por el riesgo.

Una vez identificados los riesgos, cada proceso debe establecer los controles teniendo en cuenta: Controles preventivos, que disminuyen la probabilidad de ocurrencia o

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

materialización del riesgo; y Controles correctivos, que buscan combatir o eliminar las causas que lo generaron, en caso de materializarse.

- **Documentación**: Declaración de aplicabilidad, que documenta los controles seleccionados y justifica por qué se implementan o no.

Paso 7: Desarrollar del SGSI

Continuando con el proceso, se deberá desarrollar políticas y procedimientos de seguridad que soporten los controles seleccionados. Algunas políticas esenciales incluyen:

- Política de Control de Accesos.
- Política de Gestión de Incidentes de Seguridad.
- Política de Gestión de la Continuidad del Negocio.

- **Documentación**: Manual del SGSI, políticas y procedimientos relevantes.

Paso 8: Implementar Controles y Capacitar al Personal

Seguidamente se implementan los controles definidos, asegurando que las tecnologías y procesos se alineen con las políticas, se capacitara al personal para garantizar que comprenda sus roles y responsabilidades dentro del SGSI, así mismo todos los riesgos de seguridad de la información deben ser comunicados, aceptados por los líderes de proceso y como evidencia de esto debe quedar un acta de reunión.

- **Documentación**: Registro de formación y concienciación en seguridad de la información.

Paso 9: Monitorización y Medición del SGSI

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Luego de la implementación, se debe realizar seguimiento a la eficacia de las acciones propuestas para abordar los riesgos y oportunidades

Se realizará seguimiento y evaluación a:

- La efectividad de los controles existentes.
- La implementación de las acciones propuestas.
- La valoración del riesgo con base en la implementación de nuevos controles.
- La pertinencia y conveniencia de los riesgos identificados.
- Los responsables.
- **Documentación**: Informes de auditoría interna, registros de incidentes de seguridad.

Paso 10: Revisión por la Dirección

Para ir culminando, la alta dirección debe revisar el desempeño del SGSI regularmente para garantizar que sigue siendo eficaz y adecuado, y para identificar oportunidades de mejora.

- **Documentación**: Acta de revisión por la dirección.

Paso 11: Mejora Continua

Implementar un ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar – PHVA) para optimizar continuamente el SGSI. Esto incluye ajustar los controles y procesos en respuesta a nuevas amenazas, cambios organizativos o auditorías.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

- **Documentación**: Plan de mejoras, registro de acciones correctivas y preventivas.

Paso 12: Auditoría Externa y Certificación

Después de implementar el SGSI, la empresa puede someterse a una auditoría externa para verificar el cumplimiento de la NTC ISO/IEC 27001:2022. Si se aprueba, la empresa recibirá la certificación. Es de gran importancia realizar este proceso anual, o cada vez que se realice un programa de auditoría y cada vez que haya un cambio o materialización de riesgo de seguridad de la información.

Por última instancia, es importante definir el porcentaje que se tiene de cada uno de los numerales de la norma y las temáticas de los controles para ir identificando el porcentaje de avance de cumplimiento, para esta compañía sería de la siguiente manera:

ITEM	COMPONENTE	EVALUACIÓN (%)
4	Contexto de la organización	50%
5	Liderazgo	60%
6	Planificación	20%
7	Apoyo	35%
8	Operación	40%
9	Evaluación del desempeño	13%
10	Mejora	0%
A.5	CONTROLES ORGANIZACIONALES	8%
A.6	CONTROLES DE PERSONAS	8%
A.7	CONTROLES FISICOS	15%
A.8	CONTROLES TECNOLOGICOS	10%
	TOTAL	**24%**

Tabla 9: Porcentaje de cumplimiento de numerales y controles del grupo empresarial Asertempo – Polifuncionales.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

7. CONCLUSIONES

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la NTC ISO/IEC 27001:2022 podría permitirle a la organización establecer un marco robusto para la protección de sus activos de información, llegando a tener un resultado en una mejora significativa en la gestión de riesgos, asegurando la confidencialidad, integridad y disponibilidad de la información.

Además de ello, facultándose en el cumplimiento de las regulaciones y leyes aplicables en materia de seguridad de la información, lo cual no solamente reduce el riesgo de sanciones legales, sino que también puede llegar a ser una optimización en la reputación de la empresa frente a sus clientes y competencia.

Para ello también es gran importante fomentar una cultura de seguridad dentro de la organización para todo el personal, haciéndolos más conscientes de los riesgos y de la importancia de seguir las políticas y procedimientos establecidos, generar diferentes tipos de formación y concienciación continua, sería la clave para lograr este cambio cultural frente a la seguridad de la información.

Así mimo determinar la eficiencia operacional, a partir de la estandarización de procesos y la implementación de controles de seguridad y que se pueda gestionar dentro de la operación diaria de la organización, mejorando la respuesta ante incidentes de seguridad, minimizando riesgos y masificando la seguridad de la información.

Y finalmente poder lograr la certificación en la NTC ISO/IEC 27001:2022, lo que incrementaría la confianza de los clientes, proporcionado una ventaja competitiva en el mercado y permitiendo a la empresa diferenciarse ante sus competidores.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8. BIBLIOGRAFÍA

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems.

ACOSET. (2023). *Asociación Colombiana De Empresas De Servicios Temporales.* Retrieved from https://www.acoset.org/quienes-somos/

Asertempo Colombia S.A. (2023). *Asertempo Colombia*. Retrieved from https://www.asertempocolombia.com/es/

Chaudhary, S., Gkioulos, V. & Katsikas, S., (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. https://www.sciencedirect.com/science/article/pii/S157401372300059X

Congreso de Colombia. (2011). Ley 1273 de 2009: Un análisis crítico de la regulación de los delitos informáticos en Colombia.

Congreso de Colombia. (1990). El congreso de Colombia. *Ley 50, por la cual se introducen reformas al Código Sustantivo del Trabajo y se dictan otras disposiciones*. Retrieved from https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=281

Congreso de la República. (2008). Ley 1266 de 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*. Retrieved from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php

Congreso de la Republica. (2014). LEY 1712 DE 2014, *Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional*

y se dictan otras disposiciones. Retrieved from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Colombia. (1996). Presidente de la república. *Decreto 1530, por el cual se reglamentan parcialmente la Ley 100 de 1993 y el Decreto-ley 1295 de 1994*. Retrieved from https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=8804

Colombia. (2009). Congreso de Colombia. *Ley 1273, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"*. Retrieved from http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Colombia. (2012). Congreso de Colombia. *Ley 1581, por la cual se dictan disposiciones generales para la protección de datos personales*. Retrieved from https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

Deming, E. (1989). Calidad, productividad y competitividad. Ediciones Díaz Santos.

Figueras, S., & Gargallo, P. (2003). *Análisis Exploratorio de datos*. Retrieved from http://www.5campus.com/leccion/aed

García, A. (2015). La legislación colombiana frente al fraude electrónico: Un análisis de la Ley 1732 de 2014.

Guzmán, A. & Taborda, C. A. (2015). *Diseño de un sistema de gestión de la seguridad informática – SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C., a través de la auditoría*. [info:eu-repo/semantics/bachelorThesis, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional UNAD.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

https://repository.unad.edu.co/handle/10596/3448

Halfond, W. G. J., Viegas, J., & Orso, A. (2006). A Classification of SQL Injection Attacks and Countermeasures.

Henao, J & Lopera, J. (2007). Modelo De Madurez Para La Seguridad De La Información. Universidad Eafit. Departamento De Informática Y Sistemas.

International Organization for Standardization. (2022). *Information security, cybersecurity, and privacy protection.*

ISO/IEC JTC 1/SC 27 - Information security, cybersecurity, and privacy protection: About - ISO/IEC JTC 1/SC 27

ISO/IEC 27000 (2022). ISO/IEC 27000:202022 Tecnología de la Información – Técnicas de seguridad – Sistema de gestión de seguridad de la información.

ISO/IEC 27001:2022, *Information technology. Security techniques. Information security management systems. Requirements*.

ISO/IEC (2022). ISO 27002 Information security, cybersecurity and privacy protection, Information securityControls. Retrieved from https://www.iso.org/standard/27002

ISO/IEC (2022). ISO/IEC 27003:2022. Information Technology. Security techniques. Information Security Management Systems. Guidance

ISO/IEC 27005, *Information security, Cybersecurity and Privacy Protecton. Guidance on Managing Information Security Risks.*

ISO 31000:2018, *Risk management. Guidelines*

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Martinez, A. (2019). *Importancia de la implementación de un sistema de gestión de seguridad de la información (SGSI) en las empresas bajo la NTC- ISO/IEC 27001:2022.* Universidad militar nueva granada.

Matiz, J., & Rueda, M. (2020). Diseño de un modelo de seguridad y privacidad de la información para las empresas de empleo temporal basado en la NTC- ISO/IEC 27001:2022. Bogotá, Colombia. Retrieved from https://repository.ucatolica.edu.co/server/api/core/bitstreams/c8d5fde0-16cd-4e9f-aaab-36fcd566f7de/content

Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). (2022). Política de Gobierno Digital. *Gobierno digital.* Retrieved from https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

Moyano, L & Suarez, Y (2017). Plan de implementación del SGSI basado en la norma ISO 27001: 2013 para la empresa interfaces y soluciones. Bogotá, Colombia. Facultad tecnológica**.**

Presidente De La República De Colombia. (2015). Decreto 1078 De 2015. *Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*. Retrieved from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888

Restrepo, J. (2017). *Diagnóstico del estado actual de la seguridad de la información basado en la norma NTC- ISO/IEC 27001:2022:2013, de la institución información basado en la norma NTC- ISO/IEC 27001:2022:2013, de la institución educativa técnico industrial sede mercedes pardo de simmonds-.* Popayan- cauca : universidad abierta y a distancia (unad).

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

Rodríguez, L., Cruzado, C., Mejía, C., & Alarcón, M. (2020, Octubre 27). Aplicación de NTC- ISO/IEC 27001:2022 y su influencia en la seguridad de la información de una empresa privada. Perú. doi: http://dx.doi.org/10.20511/pyr2020.v8n3.786

Sampieri, R., Fernández, C., & Baptista, P. (2010). *Metodología de la Investigación.* México D.F: MacGraw-Hill.

Seger, A., (2012). The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web. https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf

UNAD. (2015). Repositorio Institucional UNAD: Diseño de un sistema de gestión de la seguridad informática – SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C., a través de la auditoría. Recuperado a partir de http://repository.unad.edu.co/handle/10596/3448

Velasco, A. (2008). El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. 333-366. Retrieved from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000100013&lng=en&tlng=es.

Zaque, O. (2018). Proyección Financiera y Tecnológica requerida para la Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), Bajo La Norma ISO/IEC 27001:2013 En La Empresa INDAIRE Ingeniería S.A.S. [En línea, [consultado el 2 de mayo de 2018. Disponible en Internet: http://repository.unad.edu.co/handle/10596/8595

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

ANEXO A

Análisis de situación actual de la organización, de acuerdo con los criterios establecidos:

Criterio	Calificación	Porcentaje
No Existe	0	0%
Muy Insuficiente	1	20%
Insuficiente	2	40%
Adecuado	3	60%
Bueno	4	80%
Excelente	5	100%

Numeral	Cláusula	Descripción	Criterio de Evaluación (1-5)	Calificación	Resultado
4	Contexto de la organización	Comprender la organización y su contexto. las necesidades y expectativas de las partes interesadas. y determinar el alcance del SGSI.			**50%**
4.1	Comprender la organización y su contexto	Identificar factores internos (cultura. estructura. capacidades) y externos (económicos. tecnológicos. legales. ambientales).	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	3	60%
4.2	Comprender las necesidades y expectativas de las partes interesadas	Identificar las partes interesadas relevantes y sus requisitos.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
4.3	Determinar el alcance del SGSI	Definir los límites y la aplicabilidad del SGSI considerando los factores internos y externos y los requisitos de las partes interesadas.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	3	60%

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

4.4	Sistema de gestión de seguridad de la información	La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
5	Liderazgo	Requisitos para la alta dirección. incluyendo el compromiso. la política de seguridad de la información. y roles y responsabilidades.			**60%**
5.1	Compromiso de la alta dirección	La alta dirección debe demostrar liderazgo y compromiso con el SGSI.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	4	80%
5.2	Política de seguridad de la información	Establecer una política adecuada y comunicarla dentro de la organización.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	3	60%
5.3	Roles. responsabilidades y autoridades	Definir y comunicar claramente los roles y responsabilidades relacionados con el SGSI.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
6	Planificación	Acciones para abordar riesgos y oportunidades. objetivos de seguridad de la información y planificación para lograrlos.			**20%**
6.1	Acciones para abordar riesgos y oportunidades	Identificar y planificar acciones para gestionar riesgos y oportunidades.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	0	0%

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

6.2	Objetivos de seguridad de la información	Establecer objetivos claros y medibles.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	1	20%
6.3	Planificación para lograr los objetivos	Definir cómo se alcanzarán los objetivos establecidos.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
7	Apoyo	Recursos necesarios. competencia. toma de conciencia. comunicación y control de la información documentada.			**35%**
7.1	Recursos	Asegurar que se disponen de los recursos necesarios para el SGSI.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
7.2	Competencia	Garantizar que el personal tiene la competencia necesaria.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	1	20%
7.3	Toma de conciencia	Asegurar que el personal es consciente de su papel en el SGSI.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	3	60%

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

7.4	Comunicación	Establecer procesos de comunicación efectivos.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	1	20%
7.5	Información documentada	Controlar la información documentada requerida por el SGSI.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
8	Operación	Planificación y control operacional. evaluación de riesgos de seguridad de la información. y tratamiento de riesgos.			**40%**
8.1	Planificación y control operacional	Implementar y controlar los procesos necesarios para cumplir con los requisitos del SGSI.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
8.2	Evaluación de riesgos de seguridad de la información	Identificar y evaluar los riesgos de seguridad de la información.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
8.3	Tratamiento de riesgos	Implementar controles para tratar los riesgos identificados.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
9	Evaluación del desempeño	Monitoreo. medición. análisis y evaluación. auditoría interna y revisión por la dirección.			**13%**

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

9.1	Seguimiento, medición análisis y evaluación	Realizar actividades de monitoreo y medición para evaluar el desempeño del SGSI.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	2	40%
9.2	Auditoría interna	Realizar auditorías internas periódicas.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	0	0%
9.3	Revisión por la dirección	La alta dirección debe revisar el SGSI a intervalos planificados.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	0	0%
10	Mejora	No conformidades y acciones correctivas. y mejora continua del SGSI.			**0%**
10.1	No conformidades y acciones correctivas	Identificar y corregir no conformidades.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	0	0%
10.2	Mejora continua	Mejorar continuamente la idoneidad. adecuación y eficacia del SGSI.	0: No existe 1: Muy Insuficiente 2: Insuficiente 3: Adecuado 4: Bueno 5: Excelente	0	0%

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

ANEXO B							
MATRIZ DE VALORACIÓN DE CONTROLES. ANEXO A - ISO/IEC 27001:2022							
ISO 27002:2022 ID Control	**Nombre del Control**	**Implementada (SI/NO)**	**Objetivo**	**Justificación**	**Cumplimiento**	**%**	**Control**
5.1	Políticas de seguridad de la información	Si	Asegurar la idoneidad, adecuación y eficacia continuas de la dirección y el apoyo a la seguridad de la información de acuerdo con los requisitos del negocio, legales, reglamentarios y contractuales.	Existen políticas de seguridad de la información sobre temas puntuales, donde se establen algunos controles y se encuentran en desarrollo de otros controles	**2**	**50%**	Documentar e implementar la política de seguridad de la información incluyendo todos los dominios de seguridad, un alcance definido y el compromiso de todo el personal de la organización
5.1	Revisión de las políticas de seguridad de la Información	No		No se evidencian actualizaciones de las Políticas desde el año 2023 que se realizó el primer intento para implementar la norma	**0**	**0%**	Al complementar el documento de política e implementar un SGSI, se deberá dejar explícita la tarea periódica de revisión y evaluación en unas fechas formales.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.10	Uso aceptable de los activos	Si	Asegurar que la información y otros activos asociados estén protegidos, utilizados y gestionados de forma adecuada	Se mantienen controles automatizados adecuados para el uso correcto de tecnologías informáticas, computadores y uso de correo electrónico y navegación en internet.	**3**	**90%**	Incluir el uso aceptable de los activos tecnológicos en el manual de funciones de los empleados y el SGSI
5.10	Manejo de activos	No		La Organización cumple satisfactoriamente con este control	**3**	**90%**	Este esquema debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles.
5.11	Devolución de activos	No	Proteger los activos de la organización como parte del proceso de cambio o terminación de empleo, contrato o acuerdo.	La Organización cumple satisfactoriamente con este control	**3**	**90%**	El personal y otras partes interesadas, según corresponda, deberían devolver todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.12	Clasificación de la información	No	Asegurar la identificación y comprensión de las necesidades de protección de la información de acuerdo con su importancia para la organización.	No se cumple con este requerimiento	**0**	**0%**	La información se debería clasificar según las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.
5.13	Etiquetado de la información	No	Facilitar la comunicación de la clasificación de la información y apoyar la automatización del procesamiento y la gestión de la información.	No se cumple con este requerimiento	**0**	**0%**	Debería elaborarse e implementarse un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el esquema de clasificación de la información adoptado por la organización
5.14	Políticas y procedimientos de transferencia de información	No	Mantener la seguridad de la información transferida dentro de una organización y con	No se cumple con este requerimiento	**0**	**0%**	Se debería establecer reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

			cualquier parte externa interesada.				facilidades de transferencia dentro de la organización y entre la organización y otras partes.
5.14	Mensajera electrónica	Si		El correo electrónico es el medio principal de comunicación de la organización. También se utiliza como repositorio de registros, actas, y otro tipo de constancias auditables. Además, se hacen Backup cada año laborado	**3**	**90%**	Se debe mantener el esquema de seguridad sobre el correo a nivel de contingencias, antivirus, antispam y revisar periódicamente la efectividad de todos los controles
5.15	Política de control de acceso	Si	Asegurar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.	No existe política formalmente definida y divulgada	**2**	**50%**	Diseñar e implementar una política de control de acceso de usuarios que incluya los procesos necesarios para autorización y control de acceso a los SGI

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.15	Acceso a redes y servicios de red	Si		Se cuenta con herramientas para la identificación de equipos en la red, pero no se mantienen controles sobre equipos de terceros	**2**	**50%**	Implementar un procedimiento de control de equipos conectados a la red, empleando herramientas tecnológicas o políticas de conexión e inventariado.
5.16	Registro y baja de usuarios	Si	Permitir la identificación única de individuos y sistemas que acceden a la información de la organización y otros activos asociados y permitir la asignación adecuada de derechos de acceso.	Se realiza un proceso de registro de usuarios para cada individuo con perfiles y permisos asignados según justifique el caso. No se realiza un seguimiento periódico y formal a los usuarios en desuso del sistema.	**3**	**90%**	Diseñar e implementar una política de control de acceso de usuarios que incluya los procesos necesarios para autorización y control de acceso e incluir en el proceso, la periodicidad y rigurosidad de la revisión de los usuarios creados.
5.17	Gestión de la información secreta de autentificación de los usuarios	Si	Para Asegurar la autenticación de entidades correcta y evitar errores en los procesos de autenticación	La Organización cumple satisfactoriamente con este control	**3**	**90%**	La asignación y gestión de la información de autenticación debería controlarse mediante un proceso de gestión

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.17	Uso de información secreta de autenticación	Si		La Organización cumple satisfactoriamente con este control	**3**	**90%**	Las contraseñas personales o los números de identificación personal (PIN) generados automáticamente durante los procesos de inscripción cómo información de autenticación secreta temporal no se puede adivinar y es única para cada persona y los usuarios deberían cambiarlos después del primer uso
5.17	Sistema de gestión de contraseñas	Si		La Organización cumple satisfactoriamente con este control.	**3**	**90%**	Mantener el esquema implementado de administración de contraseñas y extender el esquema a aplicaciones con las recomendaciones de buenas practicas

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.18	Aprovisionamiento del acceso de los usuarios	Si	Asegurar que el acceso a la información y otros activos asociados se define y autoriza de acuerdo con los requisitos de negocio	Se tienen directivas sobre el uso y administración de contraseñas, sin embargo, hace falta una formalidad en el procedimiento y auditorías al uso de las mismas.	**2**	**50%**	Los derechos de acceso a la información y a otros activos asociados se deberían aprovisionar, revisar, modificar y eliminar de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.
5.18	Revisión de los derechos de acceso del usuario	No		No se realiza la tarea periódicamente con el detalle requerido para identificar inconvenientes con los perfiles.	**0**	**0%**	Definir la periodicidad y detalle del procedimiento de los derechos de acceso de los usuarios después de cualquier cambio en la misma organización
5.18	Eliminación o ajuste de los derechos de acceso	No		La Organización no cumple con este control	**0**	**0%**	Se deben establecer actividades de control sobre los privilegios ya no necesarios y se debe establecerse un procedimiento formal y consistente dentro del SGSI

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.19	Política de seguridad de la información para las relaciones con los proveedores	No	Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores.	No cumple con el criterio	**0**	**0%**	identificar y documentar los tipos de proveedores (por ejemplo, Servicios de TIC, logística, servicios públicos, servicios financieros, componentes de infraestructura de TIC) que pueden afectar a la confidencialidad, integridad y disponibilidad de la información de la organización
5.2	Funciones y responsabilidades en materia de seguridad de la información	Si	Establecer una estructura definida, aprobada y entendida para la implementación operación y gestión de la seguridad de la información dentro de la organización.	Existen funciones definidas con respecto a las responsabilidades sobre la información manejada y los activos que la soportan. El área de seguridad de la información tiene claras sus responsabilidades	**3**	**90%**	Establecer las responsabilidades y responsables definidos, incluyéndolas en los manuales de funciones con algunas actividades específicas de clasificación de la información y administración de activos de información.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.22	Seguimiento y revisión de los servicios de los proveedores	No	Mantener un nivel acordado de seguridad de la información y prestación de servicios de acuerdo con los acuerdos con los proveedores	No cumple con el criterio	**0**	**0%**	La organización debería monitorear, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información del proveedor y en la prestación de servicios.
5.22	Gestión de los cambios en los servicios de los proveedores	No		No cumple con el criterio	**0**	**0%**	Se debe monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos y monitorear los cambios realizados por los proveedores
5.20	Abordar la seguridad en los acuerdos con los proveedores	No	Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores	No cumple con el criterio	**0**	**0%**	Establecer requisitos de la seguridad de la información para cada proveedor en función del tipo de relación con el proveedor

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.21	Cadena de suministro de tecnologías de la información y la comunicación	No	Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores	No cumple con el criterio	**0**	**0%**	Debería definirse y aplicarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC
5.24	Responsabilidades y procedimientos	Si	Asegurar una respuesta rápida, eficaz, coherente y ordenada a los incidentes de seguridad de la información, incluida la comunicación sobre los eventos de seguridad de la información.	Existen funciones definidas con respecto a las responsabilidades sobre la información manejada y los activos que la soportan. El área de seguridad de la información tiene claras sus responsabilidades	**3**	**90%**	La organización debería planificar y prepararse para gestionar los incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información
5.25	Evaluación y decisión sobre eventos de seguridad de la información	No	Asegurar la categorización y priorización efectivas de los eventos de seguridad de la información	No cumple con este control	**0**	**0%**	La organización debería evaluar los eventos de seguridad de la información y decidir si se debiesen clasificar como

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

							incidentes de seguridad de la información.
5.26	Respuesta a los incidentes de seguridad de la información	No	Asegurar una respuesta eficaz a los incidentes de seguridad de la información	No se tiene la conciencia de la gravedad de un incidente de seguridad (a nivel de usuarios finales) lo que hace lento el proceso de recolección de evidencia.	**0**	**0%**	Diseñar e implementar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria.
5.27	Aprendizaje de los incidentes de seguridad de la información	Si	Reducir la probabilidad o las consecuencias de futuros incidentes.	Se realizan estudios de algunos incidentes de seguridad, pero no se tiene un registro formal o seguimiento de los incidentes	**1**	**10%**	Además de tipificar esta labor como parte de las actividades del oficial de seguridad, definir el procedimiento adecuado en el SGSI y realizar la revisión a todos los reportes de incidentes e incluirlo en el plan de mejoramiento

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.28	Recopilación de pruebas	No	Asegurar una gestión coherente y eficaz de las pruebas relacionadas con los incidentes de seguridad de la información para los fines de las acciones disciplinarias y legales	La Organización no realiza pruebas de vulnerabilidad a sus sistemas críticos bajo requerimiento.	**0**	**0%**	Dada la criticidad de la información, debería implementarse un esquema de pruebas internas (ya sea por capacitación de un funcionario o por un sistema) que permita una revisión periódica interna al respecto, además de ello procedimientos para la recolección, adquisición y preservación de pruebas relacionadas con eventos de seguridad de la información
5.29	Planificación de la continuidad de la seguridad de la información	No	Proteger la información y otros activos asociados durante la interrupción	No se han implementado los planes de continuidad del negocio en todos los procesos críticos	**0**	**0%**	Se debe realiza y probar los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.29	Implementación de la continuidad de la seguridad de la información	No		No cumple con este control	**0**	**0%**	Se debería mantener un esquema único de planes de continuidad del negocio para garantizar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento. Unificar los términos de análisis para el impacto y los riesgos evaluados en los planes de continuidad del negocio.
5.29	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No		No cumple con este control	**0**	**0%**	Se deberían considerar y priorizar las consecuencias de la pérdida de confidencialidad e integridad de la información, además de la necesidad de mantener la disponibilidad.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.3	Segregación de funciones	No	Reducir el riesgo de fraude, error y omisión de los controles de seguridad de la información	La Organización no cumple con este control	**0**	**0%**	La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un profesional dedicado a estas funciones con el fin de incluir los controles mínimos de seguridad sobre los datos y mantener la segregación de funciones.
5.31	Identificación de la legislación aplicable y de los requisitos contractuales	No	Asegurar el cumplimiento de los requisitos estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información.	La Organización no cumple con este control	**0**	**0%**	Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deberían ser identificados, documentados y actualizados.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.31	Regulación de los controles cifrados	Si		Se tienen identificados y aplicados los lineamientos específicos sobre uso de controles criptográficos a la información	**3**	**90%**	Se recomienda buscar asesoramiento jurídico para Asegurar el cumplimiento de la legislación y las normativas pertinentes, especialmente cuando la información cifrada o las herramientas de cifrado se desplazan a través de las fronteras jurisdiccionales
5.32	Derechos de propiedad intelectual	No	Asegurar el cumplimiento de los requisitos legales, legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos propietarios.	La Organización cumple satisfactoriamente con este control	**0**	**0%**	La organización debería aplicar los procedimientos apropiados para proteger los derechos de propiedad intelectual.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.33	Protección de los registros	Si	Asegurar el cumplimiento de los requisitos legales, legales, reglamentarios y contractuales, así como de las expectativas comunitarias o sociales relacionadas con la protección y disponibilidad de los registros.	Los registros organizacionales son administrados de la misma forma que el resto de la información operacional de la organización	**2**	**50%**	Establecer procedimientos especiales de seguridad para los registros organizacionales. Los registros deberían estar protegidos de pérdidas, destrucción, falsificación, acceso no autorizado y liberación no autorizada
5.34	Privacidad y protección de la información personal identificable	Si	Asegurar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los aspectos de seguridad de la información de la protección de la IIP.	La Organización cumple satisfactoriamente con este control	**3**	**90%**	La organización debería identificar y cumplir con los requisitos relativos a la preservación de la privacidad y la protección de la IIP de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.35	Revisión independiente de la seguridad de la información	No	Asegurar la idoneidad, adecuación y eficacia continuas del enfoque de la organización para gestionar la seguridad de la información.	No cumple con este control	**0**	**0%**	La dirección debería planificar e iniciar revisiones independientes periódicas. Las revisiones deberían incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad de la información, lo que incluye la política de seguridad de la información, las políticas de temas específicos y otros controles.
5.36	Cumplimiento de las políticas y normas de seguridad	No	Asegurar que la seguridad de la información se implementa y opera de acuerdo con la política de seguridad de la información de la organización, las políticas, reglas y	No cumple con este control	**0**	**0%**	Se deberían registrar los resultados de las revisiones y acciones correctivas llevadas a cabo por los gerentes, los propietarios de servicios, productos o información y se deberían conservar estos documentos

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.36	Revisión del cumplimiento técnico	Si	normas específicas por tema.	Si existe política de seguridad formalmente establecida dentro del marco de un SGSI, pero no se le hace un seguimiento	**3**	**90%**	Se debe realizar los controles al cumplimiento de esta
5.37	Procedimientos operativos documentados	No	Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.	No se tienen manuales operativos sobre los procesos fundamentales del área.	**0**	**0%**	Los manuales deben incluir procedimientos contingentes del área, así como las actividades en casos de emergencia. Todo debe estar alineado o incluido en el SGSI
5.4	Responsabilidades de gestión	Si	Asegurar que la dirección comprenda su papel en la seguridad de la información y emprender acciones encaminadas a asegurar que todo el personal sea consciente y cumpla con sus responsabilidades en materia de	Existe una definición de responsabilidades para cada rol dentro de la organización, pero aún no se ha incluido el detalle del tema de seguridad de la información y solamente se tienen roles para las jefaturas y cargos superiores.	**2**	**50%**	Contar con los perfiles mínimos para cumplir los roles faltantes necesarios e incluir las responsabilidades de seguridad en el SGSI

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

			seguridad de la información				
5.5	Contacto con las autoridades	No	Asegurar un flujo de información adecuado con respecto a la seguridad de la información entre la organización y las autoridades legales, reglamentarias y de supervisión pertinentes.	No se tiene contacto con autoridades, de acuerdo con la criticidad de la información manejada.	**0**	**0%**	Es de gran importancia contar con contactos directos con autoridades competentes y expertas en diversas disciplinas concernientes a la seguridad.
5.6	Contacto con grupos de interés especiales	Si	Asegurar que se produce un flujo adecuado de información con respecto a la seguridad de la información	El área de seguridad se mantiene en constante contacto con grupos de interés en seguridad tanto por sus capacitaciones internas como por su interacción con proveedores	**3**	**90%**	Inscribir a los miembros del grupo de seguridad de la información en listas de correo especializadas e incrementar el contacto con los grupos de interés u otros foros de seguridad especializados y

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

				especializados en los temas.			asociaciones profesionales.
5.8	Seguridad de la información en la gestión de proyectos	No	Asegurar que los riesgos de seguridad de la información relacionados con los proyectos y los entregables se aborden de forma eficaz en la gestión de proyectos durante todo el ciclo de vida del proyecto.	La Organización no cumple con este control	**0**	**0%**	La seguridad de la información se debería integrar en la gestión de proyectos para asegurar que los riesgos de seguridad de la información se aborden como parte de la gestión del proyecto. Esto se puede aplicar a cualquier tipo de proyecto independientemente de su complejidad, tamaño, duración, disciplina o área de aplicación

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.8	Análisis y especificación de los requisitos de seguridad de información	No		La Organización no cumple con este control	**0**	**0%**	Hace falta la identificación de los incidentes concernientes a la seguridad de la información, lo cual se puede realizar durante la campaña de concientización y entrenamiento, identificar claramente los incidentes relacionados con la seguridad de la información y su reporte. La caracterización debe traducirse en la forma como se hace seguimiento en la mesa de ayuda y dentro del grupo de seguridad
5.9	Inventario de activos	Si	Identificar la información de la organización y otros activos asociados para preservar su seguridad de la información y asignar la	La Organización lleva un listado de algunos activos y cuanta con algunos controles	**2**	**50%**	Centralizar el inventario de todos los activos en un listado maestro, enmarcado en un procedimiento y asignado y designar al responsable por su mantenimiento.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

5.9	Propiedad de los activos	No	propiedad apropiada.	La Organización no cumple con este control	**0**	**0%**	Se debe realizar revisiones periódicas de la información identificada y otros activos asociados con respecto al inventario de activos y aplicar automáticamente una actualización de inventario en el proceso de instalación, cambio o eliminación de un activo.
6.1	Selección	Si	Asegurar que todo el personal es elegible y adecuado para las funciones para las que se considera y que sigue siendo elegible y adecuado durante su empleo	Se tiene implementado estudios de seguridad de todo el personal que podría ingresar a la compañía	3	50%	Las verificaciones de los antecedentes de todos los candidatos a convertirse en personal deberían llevarse a cabo antes de incorporarse a la organización y de forma continuada, tomando en consideración las leyes, los reglamentos y la ética aplicables y ser proporcionales a los requisitos de la empresa, la

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

							clasificación de la información a la que se va a acceder y los riesgos percibidos.
6.2	Condiciones del empleo	Si	Asegurar que el personal comprenda sus responsabilidades de seguridad de la información para las funciones para las que se consideran.	Se cumple con el control y las descripciones de responsabilidades de seguridad dentro de los contratos y acuerdos para cargos de jefaturas y superiores	**3**	**90%**	Mantener el control implementado y describir los acuerdos contractuales de empleo deberían indicar las responsabilidades del personal y de la organización en materia de seguridad de la información para todos los niveles de la organización

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

6.3	Sensibilización, educación y formación en materia de seguridad de la información	Si	Asegurar que el personal y las partes interesadas pertinentes conozcan y cumplan con sus responsabilidades en materia de seguridad de la información.	Se realizan constantes recordatorios sobre esquemas y controles de seguridad a través de medios tecnológicos, pero no existe un plan formal de entrenamiento o conciencia en seguridad.	**2**	**50%**	El personal de la organización y las partes interesadas pertinentes deberían recibir una sensibilización, educación y formación adecuadas en materia de seguridad de la información, así como actualizaciones periódicas de la política de seguridad de la información de la organización y de las políticas y procedimientos específicos, según sea pertinente para su función laboral
6.4	Proceso disciplinario	Si	Asegurar que el personal y otras partes interesadas comprendan las consecuencias de la violación de la política de seguridad de la información, para disuadir y tratar adecuadamente al	Se tienen algunos procesos establecidos, pero no son claros los procesos disciplinarios que se producen por temas de seguridad	**2**	**50%**	Se debería formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

			personal y otras partes interesadas pertinentes que hayan cometido la violación.				política de seguridad de la información
6.5	Terminación o cambio de responsabilidades laborales	No	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo o contratos.	La Organización no cumple con este control	**0**	**0%**	Definir el proceso para administrar la terminación o el cambio de empleo, el cual defina qué responsabilidades y deberes de seguridad de la información deberían seguir siendo válidos después de la terminación o el cambio.
6.6	Acuerdos de confidencialidad o no divulgación	Si	Mantener la confidencialidad de la información accesible por el personal o terceros.	Además de los acuerdos de confidencialidad, no se hacen controles adicionales sobre el intercambio de información.	**2**	**50%**	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deberían ser identificados, documentados, revisados y firmados

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

							regularmente por el personal y otras partes interesadas pertinentes.
6.7	Teletrabajo	No	Asegurar la seguridad de la información cuando el personal trabaja de forma remota.	No existe dentro de la compañía	**0**	**0%**	
6.8	Notificación de sucesos relacionados con la seguridad de la información	No	Apoyar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que pueden ser identificados por el personal	No se cumple con este requerimiento	**0**	**0%**	La organización debería proporcionar un mecanismo para que el personal informe sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados de manera oportuna

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

6.8	Notificación de deficiencias en la seguridad de la información	No		No se cumple con este requerimiento	**0**	**0%**	Debería tenerse en cuenta el procedimiento para informar sobre los eventos de seguridad de la información y el punto de contacto al que deberían notificarse los eventos. El mecanismo de presentación de informes debería ser lo más fácil, accesible y disponible posible. Los eventos de seguridad de la información incluyen incidentes, infracciones y vulnerabilidades.
						32%	
7.1	Perímetros de seguridad física	Si	Evitar el acceso físico no autorizado, los daños y las interferencias en la información de la organización y otros activos asociados.	La Organización cumple satisfactoriamente con este control	**4**	**95%**	Los perímetros de seguridad deberían definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

7.10	Gestión de medios extraíbles	No	Asegurar únicamente la divulgación, modificación, eliminación o destrucción autorizada de la información en los medios de almacenamiento.	No existe una política estricta sobre el uso de medios removibles dentro de la organización	**0**	**0%**	Los medios de almacenamiento deberían gestionarse a través de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización
7.10	Eliminación de medios de almacenamiento	No		La Organización no cumple con este control	**0**	**0%**	Es necesario establecer una política rigurosa en el SGSI acompañada de un procedimiento para la destrucción de medios específicamente identificados.
7.10	Retirada de activos	Si		El proveedor de equipo tecnológicos se encarga del manejo adecuado de los medios fijos o removibles de almacenamiento	**3**	**90%**	Se debe reforzar la práctica de disposición de medios de almacenamiento y reutilización de equipos mediante una política fuerte dentro del SGSI que

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

							no discrimine ningún caso y solicitar las certificaciones de disposición.
7.11	Servicios públicos de respaldo	No	Evitar la pérdida, daño o compromiso de información y otros activos asociados o la interrupción de las operaciones de la organización debido al fracaso y la interrupción de los servicios públicos de respaldo.	Se cuenta con planta eléctrica	**4**	**90%**	Las instalaciones de procesamiento de la información deberían estar protegidas contra los cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de respaldo
7.12	Seguridad del cableado	Si	Evitar la pérdida, daño o compromiso de información y otros activos asociados o la interrupción de las operaciones de la organización debido al cableado de alimentación y comunicaciones	La Organización cumple satisfactoriamente con este control	**3**	**90%**	Los cables que transportan energía, datos o servicios de información de respaldo deberían estar protegidos contra la interceptación, las interferencias o los daños

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

7.13	Mantenimiento del equipo	Si	Evitar la pérdida, daño o compromiso de información y otros activos asociados o la interrupción de las operaciones de la organización debido al cableado de alimentación y comunicaciones	La Organización cuenta con cronograma de mantenimiento, tomando en consideración si este mantenimiento lo realiza el personal del emplazamiento o externo a la organización	**4**	**95%**	Se debe mantener el esquema de contratos de mantenimiento constantes sobre los equipos tecnológicos o solicitarle los mantenimientos a el proveedor.
7.14	Eliminación segura o reutilización de los equipos	No	Evitar fugas de información del equipo que se va a desechar o reutilizar	La Organización no cumple con este control	**0**	**0%**	Los elementos del equipo que contienen medios de almacenamiento deberían verificarse para Asegurar que los datos confidenciales y el software con licencia se han eliminado o sobrescrito de forma segura antes de desecharlos o volver a utilizarlos
7.2	Controles físicos de entrada	Si	Asegurar que solo se produce el acceso físico autorizado a la información de la organización y a	La Organización cumple satisfactoriamente con este control	**4**	**95%**	Las áreas seguras deberían protegerse mediante controles de entrada y puntos de acceso adecuados

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

7.2	Zonas de entrega y carga	No Aplica	otros activos asociados.	La Organización no cumple con este control	**0**	**0%**	NO APLICA
7.3	Protección de oficinas, salas e instalaciones	Si	Impedir el acceso físico no autorizado, los daños y las interferencias en la información de la organización y otros activos asociados en oficinas, salas e instalaciones.	Todas las áreas dentro de las instalaciones se encuentran controladas y monitoreadas. Se mantienen cerradas las puertas de las oficinas y se ingresa por medio de huella	**3**	**90%**	Se debería diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.
7.4	Monitoreo de la seguridad física	Si	Detectar y disuadir el acceso físico no autorizado	Se cuenta con empresa de seguridad física independiente a la organización	**3**	**50%**	Las instalaciones deberían ser vigiladas continuamente para el acceso físico no autorizado
7.5	Protección contra las amenazas externas y medioambientales	Si	Prevenir o reducir las consecuencias de los eventos originados por amenazas físicas y ambientales.	Actualmente no hay unos esquemas definidos en el área de TI para garantizar que se generen afectaciones por parte de amenazas externas o ambientales.	**1**	**10%**	Se debería diseñar y aplicar la protección contra las amenazas físicas y ambientales, como los desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

7.6	Trabajo en zonas seguras	Si	Proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas	La Organización cumple satisfactoriamente con este control	**3**	**90%**	Deberían diseñarse y aplicarse medidas de seguridad para trabajar en zonas seguras.
7.7	Política de escritorio y pantallas limpios	Si	Reducir los riesgos de acceso no autorizado, pérdida y daños a la información en escritorios, pantallas y otros lugares accesibles durante y fuera del horario de trabajo normal	Se tiene un política de escritorio limpio y la información en la nube o servidor, pero no se lleva un control de este.	**2**	**50%**	Se deberían definir y aplicar de forma adecuada reglas de escritorio claras para papeles y medios de almacenamiento extraíbles, así como reglas de pantalla clara para las instalaciones de procesamiento de información
7.8	Ubicación y protección de los equipos	Si	Reducir los riesgos derivados de amenazas físicas y ambientales, así como del acceso y los daños no autorizados	Se ubican los equipos tecnológicos buscando mantener el menor nivel de exposición a terceros o visitantes	**3**	**90%**	Debe reforzarse el esquema estableciendo una directiva explicita o una política dentro del SGSI que requiera la protección y ubicación de los equipos tecnológicos

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

							en áreas protegidas a la vista.
7.9	Seguridad de equipos y activos fuera de las Instalaciones	Si	Para evitar pérdidas, daños, robos o riesgos de dispositivos externos e interrupciones en las operaciones de la empresa	Se mantienen controles estrictos sobre la salida de equipos e información.	**3**	**90%**	El SGSI debe dictaminar las políticas de uso de equipos de cómputo fuera de las instalaciones de la organización que permitan a directivos y altos rangos, conocer los requerimientos de seguridad para el uso de estos elementos y tener los activos asegurados
						60%	
8.1	Política de dispositivos móviles	No Aplica	Proteger la información contra los riesgos introducidos mediante el uso de dispositivos finales de usuario.	No existe una política formal sobre el uso de móvil y las líneas que se manejan son personales	**0**	**0%**	NO APLICA
8.1	Equipo de usuario desatendido	Si		La Organización cuenta con un política, que indica que cada	**3**	**90%**	La asignación y el uso de los derechos de acceso privilegiado deberían

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

				vez que se deje el equipo de computo debe quedar bloqueado o suspendido			ser restringidos y gestionados
8.14	Disponibilidad de instalaciones para el tratamiento de la información	No	Asegurar el funcionamiento continuo de las instalaciones de procesamiento de información	No cumple con este control	**0**	**0%**	Las instalaciones de procesamiento de información deberían implementarse con redundancia suficiente para satisfacer los requisitos de disponibilidad.
8.13	Copia de seguridad de la información	Si	Permitir la recuperación de la pérdida de datos o sistemas.	La Organización cumple satisfactoriamente con este control	**4**	**95%**	Mantener el esquema de backups y extenderlo a sistemas de información alternativos como son los usuarios finales.
8.15	Registro de evento	No	Para registrar eventos, generar pruebas, Asegurar la integridad de la información de registro, evitar el acceso no autorizado, identificar eventos de seguridad de la	La Organización no cumple con este control	**0**	**0%**	Debería producirse, almacenarse, protegerse y analizarse los registros que recogen las actividades, las excepciones, los fallas y otros eventos relevantes.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.15	Protección de la información de registro	Si	información que pueden dar lugar a un incidente de seguridad de la información y respaldar las investigaciones.	Se cuenta con un bloqueo para usuario que no sean del área de TI	**2**	**0%**	Los usuarios, incluidos aquellos con derechos de acceso con privilegios, no deberían tener permiso para eliminar o desactivar registros de sus propias actividades
8.15	Registros del administrador y del operador	No		La Organización no cumple con este control	**0**	**0%**	Realizar las revisiones periódicas, definir el procedimiento de monitoreo y su relación con el de reacción a incidentes.
8.17	Sincronización del reloj	Si	Permitir la correlación y el análisis de los eventos relacionados con la seguridad y otros datos registrados y apoyar las investigaciones sobre incidentes de seguridad de la información	La Organización cumple con este control	**4**	**95%**	Los relojes de los sistemas de procesamiento de información utilizados por la organización deberían sincronizarse con las fuentes de tiempo aprobadas

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.18	Uso de programas de utilidad privilegiados	Si	Asegurar que el uso de programas de utilidad no perjudique los controles del sistema y de las aplicaciones para la seguridad de la información	La Organización cumple satisfactoriamente con este control	**2**	**50%**	Mantener el esquema implementado. Extender las restricciones en el dominio para todos los usuarios finales.
8.19	Instalación de software en sistemas operativos	Si	Asegurar la integridad de los sistemas operativos y evitar la explotación de las vulnerabilidades técnicas	Se realiza el control por medio de un software para identificar os tiempo perdidos y las conexiones.	**3**	**90%**	Todos los servicios de administración, especialmente los remotos, deben incluir una limitante en los tiempos y horario de acceso. Para los servicios de Carga y Recolección de datos debería regularse el horario de conexiones.
8.19	Restricciones a la instalación de software	No		No se cumple con este requerimiento	**0**	**0%**	Deberían implementarse procedimientos y medidas para administrar de forma segura la instalación de software en sistemas operativo

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.2	Gestión de los derechos de acceso privilegiados	No	Asegurar que solo los usuarios autorizados, los componentes de software y los servicios se proporcionan con derechos de acceso con privilegios	La Organización no cumple con este control	**0**	**0%**	Se debería controlar mediante un proceso de autorización de acuerdo con la política de control de acceso específica para cada tema
8.24	Política de uso de controles cifrados	Si	Asegurar el uso adecuado y efectivo del cifrado para proteger la confidencialidad, autenticidad o integridad de la información de acuerdo con los requisitos de seguridad de la empresa y la información y tomando en consideración los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con el cifrado	La organización cuenta con accesos restringidos a paginas no fiables, redes sociales, entre otras.	2	**50%**	La organización debería reducir los riesgos de que su personal acceda a sitios web que contienen información ilegal o que se sabe que contienen virus o material de phishing
8.24	Gestión de claves	Si		Se tienen directivas sobre el uso y administración de claves, sin embargo, hace falta una formalidad en el procedimiento y auditorías al uso de estas.	**2**	**50%**	Documentar dentro del SGSI una política de administración de gestión de claves formal que incluya manejo, almacenamiento, cambio y construcción de claves.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.20	Controles de red	Si	Proteger la información de las redes y sus instalaciones de procesamiento de información de apoyo frente a riesgos a través de la red.	A pesar de contar con los elementos necesarios para el monitoreo de la red, no se realizan controles adecuados sobre tráfico, conexiones o revisión de anomalías.	**2**	**50%**	Las redes y los dispositivos de red deberían estar protegidos, gestionados y controlados para proteger la información de los sistemas y las aplicaciones
8.21	Seguridad de los servicios de red	Si	Asegurar la seguridad en el uso de los servicios de red.	La red interna cuenta con controles pertinentes para no poder tener acceso de terceros en la red.	**3**	**90%**	Deberían identificarse, implementarse y supervisarse los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.
8.22	Separación en las redes	No	Dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades de la empresa	No se cumple con este control	**0**	**0%**	La organización debería considerar la gestión de la seguridad de las grandes redes dividiéndolas en dominios de red separados y separándolas de la red pública (es decir, Internet). Los dominios se pueden

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

							elegir en función de los niveles de confianza, criticidad y sensibilidad
8.25	Política de desarrollo segura	No	Asegurar que la seguridad de la información se diseña e implementa dentro del ciclo de vida de desarrollo seguro del software y los sistemas.	No se cumple con este control	**0**	**0%**	Debería establecerse y aplicarse normas para el desarrollo seguro de software y sistemas.
8.26	Seguridad de los servicios de aplicaciones en las redes publicas	No	Asegurar que todos los requisitos de seguridad de la información se identifican y se abordan al desarrollar o adquirir aplicaciones.	No se cumple con este control	**0**	**0%**	Se debería identificar y especificar los requisitos de seguridad de las aplicaciones. Estos requisitos se determinan generalmente a través de una evaluación de riesgos

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.26	Protección de las transacciones de los servicios de aplicación	No		No se cumple con este control	**0**	**0%**	El nivel de confianza requerido en la integridad de la información intercambiada o procesada y los mecanismos para identificar la falta de integridad (por ejemplo, comprobación de redundancia cíclica, phishing, firmas digitales)
8.27	Principios de ingeniería de sistemas seguros	No	Asegurar que los sistemas de información se diseñan, implementan y operan de forma segura dentro del ciclo de vida del desarrollo	No se cumple con este control	**0**	**0%**	Los principios para la ingeniería de sistemas seguros deberían establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.
8.29	Pruebas de seguridad del sistema	Si	Validar si se cumplen los requisitos de seguridad de la información cuando las aplicaciones o el código se	La Organización realiza pruebas de vulnerabilidad a sus sistemas críticos bajo requerimiento.	**2**	**50%**	Dada la criticidad de la información, debería implementarse un esquema de pruebas internas (ya sea por capacitación de un

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

			despliegan en el entorno de producción.				funcionario o por un sistema) que permita una revisión periódica interna al respecto
8.29	Pruebas de aceptación del sistema	Si		Se mantienen controles automatizados adecuados para el uso correcto de tecnologías informáticas, computadores y uso de correo electrónico y navegación en internet.	**3**	**90%**	Incluir el uso aceptable de los activos tecnológicos en el manual de funciones de los empleados y el SGSI
8.3	Restricción del acceso a la información	Si	Asegurar únicamente el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados	La Organización cumple satisfactoriamente con este control	**3**	**90%**	El acceso a la información y a otros activos asociados deberían restringirse de conformidad con la política establecida sobre el control del acceso relativa a temas específicos.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.30	Desarrollo tercerizado	Si	Asegurar la aplicación de las medidas de seguridad de la información requeridas por la organización en el desarrollo de sistemas tercerizados	El acceso físico y lógico a terceros es regulado de forma contractual y de políticas de seguridad a nivel general.	**2**	**50%**	La organización debería dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas tercerizados
8.31	Separación de los entornos de desarrollo, prueba y operación	No	Proteger el entorno de producción y los datos del peligro que suponen las actividades de desarrollo y prueba.	No se cuenta con ambientes de Producción y Desarrollo separados.	**0**	**0%**	Los controles y protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos. El SGSI debería incluir lineamientos de manejo de los datos en Desarrollo y Pruebas.
8.31	Entorno de desarrollo seguro	No		No se cuenta con un estándar para el desarrollo seguro de aplicaciones	**0**	**0%**	Diseñar e implementar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.32	Gestión del cambio	Si	Para preservar la seguridad de la información al ejecutar los cambios	Se encuentran formatos y registros de gestión de cambios, pero desde el área de SST, que se utilizando en el sistema.	**2**	**50%**	Se debe implementar procedimientos de control de cambios deberían documentarse y aplicarse para Asegurar la confidencialidad, la integridad y la disponibilidad de la información en las instalaciones de procesamiento de la información y en los sistemas de información, para todo el ciclo de vida de desarrollo del sistema, desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores
8.32	Procedimientos de control de cambios del sistema	Si		La Organización cumple satisfactoriamente con este control	**3**	**90%**	Mantener el esquema implementado.
8.32	Revisión técnica de las aplicaciones tras los cambios de plataforma operativa	Si		La Organización cumple satisfactoriamente con este control	**3**	**90%**	Mantener el esquema implementado.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.32	Restricciones a los cambios en los paquetes de software	Si		La Organización cumple satisfactoriamente con este control	**3**	**90%**	Mantener el esquema implementado.
8.33	Protección de los datos de prueba	No	Asegurar la pertinencia de las pruebas y la protección de la información operativa utilizada para las mismas.	No se cuenta con proceso de protección de los datos de prueba	**0**	**0%**	Los controles de protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos.
8.34	Controles de auditoría de los sistemas de información	No	Minimizar el impacto de las auditorías y otras actividades de garantía en los sistemas operativos y los procesos del negocio.	No se ha realizado la primera auditoria	**0**	**0%**	Documentar e implementar dentro del SGSI, los casos y controles para tener en cuenta para las actividades de auditoría sobre sistemas en producción.
8.4	Control de acceso al código fuente del programa	Si	Para evitar la introducción de funciones no autorizadas, evite cambios no intencionados o malintencionados y mantenga la confidencialidad de la propiedad intelectual valiosa	La Organización cumple satisfactoriamente con este control	**3**	**90%**	Se debe generar un acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se deberían administrar adecuadamente

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.5	Procedimientos seguros de inicio de sesión	No	Asegurar que un usuario o una entidad se autentique de forma segura cuando se conceda acceso a sistemas, aplicaciones y servicios.	La Organización no cumple con este control	**0**	**0%**	Debería elegirse una técnica de autenticación adecuada para fundamentar la identidad reclamada de un usuario, software, mensajes y otras entidades.
8.6	Gestión de capacidad	No	Asegurar la capacidad necesaria de los servicios de procesamiento de información, los recursos humanos, las oficinas y otros servicios	La Organización no cumple con este control	**0**	**0%**	La utilización de los recursos debería supervisarse y ajustarse de conformidad con las necesidades de capacidad actuales y previstas
8.7	Controles contra malware	Si	Asegurar que la información y otros activos asociados estén protegidos contra malware.	La Organización cumple satisfactoriamente con este control	**3**	**90%**	Mantener el esquema de revisión a toda la red, incrementar los controles manualmente a equipos detectados con infección. Realizar una revisión completa cada cierto periodo de tiempo, se recomienda cada mes para activos críticos, cada 3 meses para el resto.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32

8.8	Gestión de las vulnerabilidades técnicas	Si	Evitar la explotación de vulnerabilidades técnicas.	La Organización realiza pruebas de vulnerabilidad a sus sistemas críticos bajo requerimiento.	**2**	**50%**	Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debería evaluar la exposición de la organización a esas vulnerabilidades y se deberían adoptar las medidas apropiadas.

www.uniagraria.edu.co | NIT N° 860.531.081-5 | CL. 170 No. 54 A -10 Bogotá D.C - Colombia PBX: 667 1515 | Cr. 2 No. 4 - 21 Facatativá Tel. 890 07 37 - 890 07 32