FACULTAD DE POSGRADOS

DISEÑO DE UN PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN PARA EL BRÓKER ABC.

Lic. Waldo Sami Salinas Bautista

2021

FACULTAD DE POSGRADOS

DISEÑO DE UN PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN PARA EL BRÓKER ABC.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magister en Gestión De La Seguridad De La Información

Lic. Waldo Sami Salinas Bautista

2021

AGRADECIMIENTOS

Agradezco a Dios que siempre me dio fortaleza para seguir adelante, a mi esposa y familia por todo el apoyo para la culminación del presente proyecto.

DEDICATORIA

El presente trabajo lo dedico a Dios, a mi esposa por ser un ejemplo de perseverancia, a mi madre por darme el coraje para seguir adelante cada día y a mi hermana por ser incondicional en cada paso de mi vida, a todos ellos este logro les pertenece.

RESUMEN

Dentro de las organizaciones los ciberataques afectan de manera directa a todos y cada uno de los departamentos de una empresa provocando el estancamiento parcial o total de las actividades, esto representa costos adicionales dentro de un presupuesto, ya que interfiere en la productividad del personal de la empresa.

Con gran frecuencia las víctimas de ataques informáticos son aquellas empresas que no cuentan con un CISO Chief Information Security Officer o con un SGSI Sistema de Gestión de Seguridad de la Información, debido a esto son vulnerables a ataques puesto que no cuentan con la capacidad necesaria para hacer frente a una intromisión no autorizada de seguridad informática.

Por lo tanto, el presente proyecto de titulación permitió definir e identificar aquellos procedimientos que permitan fortalecer la situación actual del Sistema de Gestión de Seguridad de la información a través de marcos de referencia que brindan las mejores prácticas para un adecuado sistema de seguridad informática.

Se utilizó la Norma Internacional ISO 27001 para el diagnóstico inicial de estado actual del SGSI.

Los resultados obtenidos demuestran que el Bróker ABC dentro del manejo de información personal está expuesto a ciber ataques internos y externos, en relación con sus competidores. Se identifico la ausencia de procedimientos, políticas y normas internas para el manejo de información producto del actual sistema de administración que posee la empresa. Eso conlleva a tomar medidas correctivas para prevenir este tipo de ataques puesto que es una realidad que afecta a las empresas del Ecuador y del mundo entero.

ABSTRACT

Within organizations, cyberattacks directly affect each and every one of the departments of a company causing the partial or total stagnation of activities, this represents additional costs within a budget, since it interferes in the productivity of the personnel of the company.

Very often the victims of computer attacks are those companies that do not have a CISO Chief Information Security Officer or an ISMS Information Security Management System, due to this they are vulnerable to attacks since they do not have the necessary capacity to deal with unauthorized computer security intrusion.

Therefore, this degree project made it possible to define and identify those procedures that make it possible to strengthen the current situation of the Information Security Management System through reference frameworks that provide the best practices for an adequate computer security system.

The International Standard ISO 27001 was used for the initial diagnosis of the current state of the ISMS.

The results obtained show that Broker ABC within the handling of personal information is exposed to internal and external cyber attacks, in relation to its competitors. The absence of procedures, policies, and internal norms for the handling of information product of the current administration system that the company has was identified. This leads to taking corrective measures to prevent this type of attack since it is a reality that affects companies in Ecuador and the entire world.

Contenido

1. Introducción.

1.1. Antecedentes

ABC es un bróker integral de seguros con más de 15 años de experiencia, trabajando con las mejores compañías a nivel nacional e internacional; las cuales certifican como una agencia reconocida y especializada en todas las ramas de los seguros. Cuentan con un equipo administrativo capacitado para atender a nuestros clientes de una manera eficaz, bajo los lineamientos de cada aseguradora, siempre buscando el beneficio para sus clientes.

1.2. Misión

Brindar soluciones integradas que se ajusten a las necesidades de los asegurados, personas físicas y jurídicas, para que los mismos puedan dedicarse a sus diferentes ocupaciones sabiendo que sus seres queridos, sus bienes, sus colaboradores y sus empresas se encuentra en manos de compañías de seguros de primera línea y con capacidad de respuesta.

1.3. Visión

Ser el bróker de seguros con mayor reconocimiento por su vocación de servicio, calidad, profesionalismo y resultados, enmarcado dentro de un alto sentido de responsabilidad y cumplimiento legal con principios éticos y de honestidad apoyando un equipo humano ético y comprometido.

1.4. El Problema

1.4.1. Análisis del Entorno

ABC no cuenta actualmente con un sistema de gestión de la seguridad de la información SGSI.

El manejo de la información de los clientes y potenciales clientes no es el adecuado de acuerdo con la Ley Orgánica de Protección de Datos personales.

No existe una conciencia de uso de la información, la actual administración no tiene presupuestado un fondo para un programa de seguridad de la información.

La información de los clientes se maneja únicamente en un archivo Excel.

Se ha perdido información debido a que no se cuenta con un sistema de back up, esto ocasionó que se pierda información de actuales clientes.

No se cuenta con antivirus, sistema de cifrado de información, control de contraseñas y los sistemas de seguridad cuentan con una configuración por defecto.

No se cuenta con manuales de procedimientos, políticas o controles documentados para el manejo de la información.

No se cuenta con personal de TI de planta o tercerizado para la administración de seguridad informática. Esto ha ocasionado un inadecuado manejo no solo de las redes sino también de las configuraciones de los equipos.

1.4.2. Problema en consideración

1.4.2.1. Análisis del problema

Manejo actual del proceso de administración de datos de clientes.

Sobreexposición de la información por falta de políticas de Seguridad de la información.

Identificación del problema: procesos ineficientes - inexistencia de tecnologías.

1.4.2.2. Razones por las cuales surgió el problema

Sobreexposición de información de clientes, esto generó la pérdida de potenciales clientes sobre la competencia de otros brókeres de seguros, no existe un control adecuado del manejo de información de los actuales asegurados por lo que la empresa asegura a personas mientras que ABC no cuenta con un seguro propio.

Cambios en la visión, estrategia u objetivos del negocio.

Tendencias comerciales u operativas que están impulsando cambios en el negocio (debido al aumento de ventas e incidencias de salud, requiere mejorar el aseguramiento de la información).

Procesos o sistemas que requieren mejoramiento o actualización.

1.4.2.3. Elementos que dieron origen al problema

Falta de procesos que controlen y aseguren a la información de los clientes y futuros clientes.

1.4.2.4. Impacto que tiene el problema en el negocio

Financiero: Pérdida de clientes, pérdida de ingresos.

Cultural = Problemas reputacionales ante un posible ataque.

Operacional = Interrupción de operaciones por pérdida de información.

1.4.2.5. Rango de tiempo que se tiene para resolver el problema

12 meses.

2. Desarrollo.

2.1. Objetivo.

2.1.1. Objetivo General.

Proponer la creación e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), donde identifique políticas, normas y procedimientos de seguridad de la información, que faciliten la implementación de mecanismos y controles utilizando el marco de referencia ISO/IEC 27001:2013.

2.1.2. Objetivos Específicos.

Realizar una evaluación del estado actual del SGSI.

Elaborar el informe del estado actual del SGSI.

Clasificar los tipos de información.

Identificar activos críticos.

Desarrollar políticas de Alto Nivel.

Definir un modelo de operaciones del SGSI.

Elaborar métricas de los procesos.

Realizar una evaluación de riesgos de los activos críticos.

Elaborar de un Roadmap de planes de acción.

Elaborar informe final del programa.

2.1.3. Alcance

El alcance del diseño del Sistema de Gestión de Seguridad de la Información SGSI será para los procesos que gestionan la información digital de los clientes.

2.2 Proyecto

2.2.1. Fase 1 Diagnostico.

2.2.1.1. Metodología de evaluación del estado actual del SGSI

Para el desarrollo de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 del 2013 se ejecuta un análisis de la situación actual del Bróker ABC, el cual permite determinar las mejores alternativas a implementar para la creación del SGSI.

La encuesta realizada evalúa 14 Dominios de Seguridad dentro de la norma distribuidos en 114 controles que permiten evidenciar el nivel de cumplimiento de cada ítem, tabulando la información la siguiente calificación.

Tabla 1 Calificación de Controles

Calificación	Estado	Descripción
0	No Aplica	Control no aplica de acuerdo con el giro del negocio
1	Inexistente	No se ha implementado en la organización
50	Parcialmente implementado	Controles sin supervisión, políticas y procedimiento en borrador
100	Se cuenta con el control u objetivo	Implementado de acuerdo con las normas de seguridad

Una vez recolectada la información, analizada y tabulada se presentan los siguientes resultados a través de la calificación de los dominios.

Tabla 2 Calificación de evaluación

Eficacia	Significado	Detalle
0	Inexistente	No se cuenta con controles
1-20	Inicial	Existen salvaguardas, pero no se gestionan
21-40	Repetible	No se cuenta con un plan de incidentes
41-60	Efectivo	Despliegue y gestión de salvaguardas
61-80	Gestionado	Control eficaz y eficiente de salvaguardas
81-100	Optimizado	Procesos de mejora continua

Tabla 3 Calificación de Dominios

N	DOMINIO	CALIF. ACTUAL	OBJ.	CALIF. DE DOMINIO
1	Políticas de seguridad de la información	1,00	100,00	Inexistente
2	Organización de la seguridad de la información	16,76	100,00	Inicial
3	Seguridad relativa a los recursos humanos	13,25	100,00	Inicial
4	Gestión de activos	7,13	100,00	Inicial
5	Control de acceso	18,98	100,00	Inicial
6	Criptografía	15,14	100,00	Inicial
7	Seguridad física y del entorno	17,05	100,00	Inicial
8	Seguridad de las operaciones	7,16	100,00	Inicial
9	Seguridad de las comunicaciones	1,00	100,00	Inexistente
10	Adquisición, desarrollo y mantenimiento de los sistemas de información	1,78	100,00	Inicial
11	Relación con proveedores	1,00	100,00	Inexistente
12	Gestión de incidentes de seguridad de la información	1,00	100,00	Inexistente
13	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	9,17	100,00	Inicial
14	Cumplimiento	4,43	100,00	Inicial

Adaptado de ISO 27001 (Ministerio de Industria c. y., 2017)

La información presentada nos permite evidenciar que actualmente la gestión de seguridad de la información del Bróker ABC no se encuentra acorde a la norma ISO/IEC 27001 ubicando su calificación de Dominio como Inicial.

Utilizando el marco de referencia del Instituto Nacional de Normas y Tecnología (NIST) y tomando la misma calificación de dominios se tabuló la información de acuerdo con las 5 funciones de la norma Identificar, Proteger, Detectar, Responder y Recuperar tomando la calificación sobre 100 puntos.

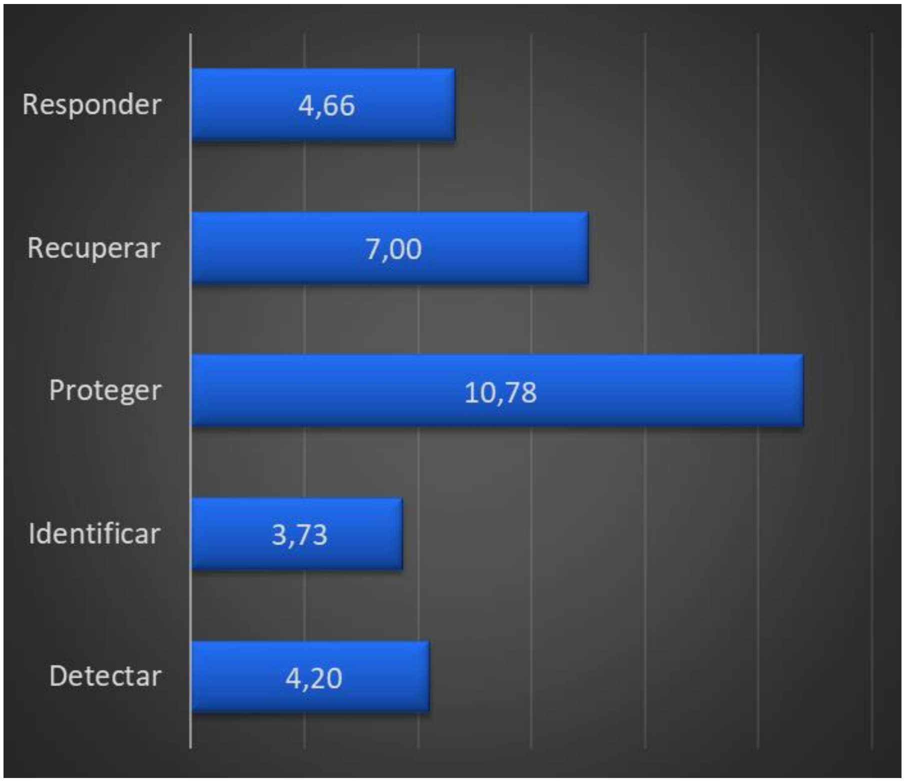


Figura 1 Calificación Evaluación cruce ISO/NIST

La información nos permite evidenciar que dentro de cada una de las funciones de NIST se encuentra en un proceso Inicial validando los resultados obtenidos en la evaluación con la norma ISO/IEC 27001.

2.2.2. Fase 2 Clasificación de la información.

La clasificación de la información busca asegurar que la información reciba un nivel adecuado de protección, de acuerdo con su importancia para la organización, de acuerdo con los niveles de importancia que permitan una adecuada manipulación de la información.

A través de Entidades o Sujetos de información se puede identificar aquellos que generan, almacenan y transmiten información para el Bróker ABC, según el giro del negocio se consideraron como entidades los Clientes, Prospectos, Empleados, Proveedores y la Organización.

Una vez definido los sujetos o entidades de información se proceden con la identificación del tipo de información que genera cada uno, a través de la siguiente tabla se presenta lo siguiente.

Tabla 4 Clasificación de la información

Sujetos de Información	Tipo de información	Definición
Clientes	Identificación	Información que permita identificar al cliente, información tomada de CI o pasaporte
	Ubicabilidad	Información que permita ubicar o contactar al cliente: dirección, teléfono, correo electrónico, redes sociales.
	Bancaria	Información que permita conocer su comportamiento dentro del sistema bancario
	Financiera	Información que permita conocer activos, pasivos, patrimonio, ingresos y gastos, nivel de endeudamiento
	Laboral	Información que permita conocer su actual situación laboral, así como su histórico
	TJ	Información que permita el débito de pagos por adquisición de productos
	Medica	Información que permita conocer el estado de salud del cliente
	Legal	Información que permita conocer la situación legal, juicios demandas personificación jurídica, tributos etc.
	Educación	Información que permita conocer el nivel educativo del cliente
	Hábitos y Hobbies	Información que permita conocer su el tratamiento de riesgo de acuerdo con el nivel de exposición de riesgo

Para realizar una evaluación de cada tipo de información se debe considerar los Principios de Seguridad de la información Privacidad Integridad Disponibilidad y Confidencialidad.

La confidencialidad significa preservar las restricciones autorizadas sobre el acceso o divulgación, incluyendo los medios para proteger la privacidad y la información propietaria.

La Integridad significa proteger contra la destrucción o modificación inadecuada de la información e incluye asegurar el no repudio y autenticidad de la información.

La disponibilidad significa asegurar que se puede acceder y usar la información de manera confiable y en el momento adecuado.

La Privacidad es compone el ámbito personal de un individuo y que debe mantenerse de forma reservada y secreta.

A partir de ellos se define el impacto que puede llegar a alcanzar la pérdida de cada uno de los principios definidos de la siguiente manera:

Pérdidas Financieras.

Interrupción de las operaciones.

Degradación de la imagen institucional.

Perdida o destrucción de Activos.

La tabulación de cada uno de los impactos que se puedan generar da como resultado la criticidad de la información clasificada de acuerdo con un modulador de riesgo.

Tabla 5 Modulador de Riesgo

	Niveles de impacto				
Descripción del Impacto	**INSIGNIFICANTE**	**MENOR**	**MODERADO**	**MAYOR**	**CATASTRÓFICO**
1. Pérdidas financieras			< 3% Patrimonio	Entre 4%-19% Patrimonio	>20% Patrimonio
3. Interrupción de operaciones parciales y/o totales		< 2días	2-5 días	>5 día y <10 días	>10 días
4. Pérdida / Degradación de la Imagen institucional				Fuga Hasta 50% Clientes	Fuga >50% Clientes
6. Pérdidas / Destrucción / afectación de bienes materiales	Sin pérdida de activos	Depreciación de activos	Deterioro de activos hasta 10% mayor al promedio	Deterioro de activos hasta 50% al promedio	Deterioro o Perdida total del Activo

2.2.3. Fase 3 Inventarios de activos de información.

La identificación de la información se lo realiza a través de un inventario de activos de información el cual debe contener un propietario de la información que será el responsable de la administración del activo.

De acuerdo con la norma ISO 27001 literal A.8 Gestión de Activos dentro de su ámbito de control señala lo siguiente: La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.

2.2.3.1. Identificación de activos críticos

Una vez definido la sección 2.3.2. Clasificación de la información. Se procede a realizar el inventario de activos que posee actualmente el Bróker ABC que permite reflejar lo siguiente:

Identificador: Código alfanumérico que permite identificar al activo.

Nombre del Activo: Nombre asignado al activo.

Características del Activo: Permite identificar si el activo genera, crea, transmite, comparte y almacena información.

Identificación del Activo de Información: Permite identificar el activo contenedor de información crítica según lo establecido en la sección 2.3.2. Clasificación de la información.

Formato: Permite identificar el formato del tipo de información crítica ubicada en el activo de información.

Procesos: Permite identificar todos y cada uno de los procesos en los que el activo de información genera, crea, transmite, comparte y almacena información crítica del activo.

Responsable: Personal de Bróker ABC responsable del tratamiento de la información del activo crítico.

Tipo de Información: Detalle de la información crítica almacenada en el activo de información según lo establecido en la sección 2.3.2. Clasificación de la información.

Criterio: Calificación del tipo de información según lo establecido en la sección 2.3.2. Clasificación de la información según los principios de Seguridad de la información.

Criticidad: Promedio resultante de la calificación de cada uno de los principios de Seguridad de la información.

Ubicación del Activo: Ubicación Física del activo de información.

Tabla 6 Identificación de activos críticos

Identificador	Nombre del Activo	Caracteristicas del Activo					Identificación del Activo de Informacion	Formato	Procesos	Responsable	Tipo de Informacion	Criterio				Criticidad	Ubicación del Activo
		Genera	Crea	Transmite	Comparte	Almacena						P	I	D	C		
ACIF_0001	Computador Portatil Gerente Comercial	X	X	X	X	X	Carpeta Clientes Actuales	Archivos de Imagen - Archivo de Excel	Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Identificación de Clientes						Oficina Gerente Comercial
									Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Ubicabilidad de Clientes						
									Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Bancaria de Clientes						
									Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Financiera de Clientes						
									Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Laboral de Clientes						
									Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información TJ de Clientes						
									Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Medica de Clientes						
									Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Legal de Clientes						
									Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Educación de Clientes						
									Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Habitos y Hobies de Clientes						
							Carpeta Seguros Actual	Medio electronico	Colocacion de nuevos productos	Gerente Comercial	Información Catálogo Productos & Precios de Organización						
							Carpeta Seguros Actual	Medio electronico	Colocacion de nuevos productos / Afiliacion Inicial / Renovacion / Siniestros	Gerente Comercial	Información Catálogo Productos & Precios de Proveedores						

2.2.3.2. Definición del modelo operacional del SGSI

Para la definición del Modelo operacional el Sistema de Gestión de Seguridad de la información se tomaron en cuenta los siguientes aspectos:

1. Enfoque de Negocios.
2. Clasificación de Dominios.
3. Modelo Canvas.

Un SGSI definido por la norma ISO 27001 no sólo debe considerar el contexto tecnológico, las necesidades de la organización deben ser sostenibles a lo largo del tiempo.

Una metodología que tome en cuenta estos aspectos permitirá tener un mejor contexto del SGSI con relación a los objetivos Estratégicos, tácticos y operativos de la organización.

Figura 2 Enfoque de Negocios Tomado de (INCIBE, 2016)

Figura 3 Enfoque de Estrategias Tomado de (INCIBE, 2016)

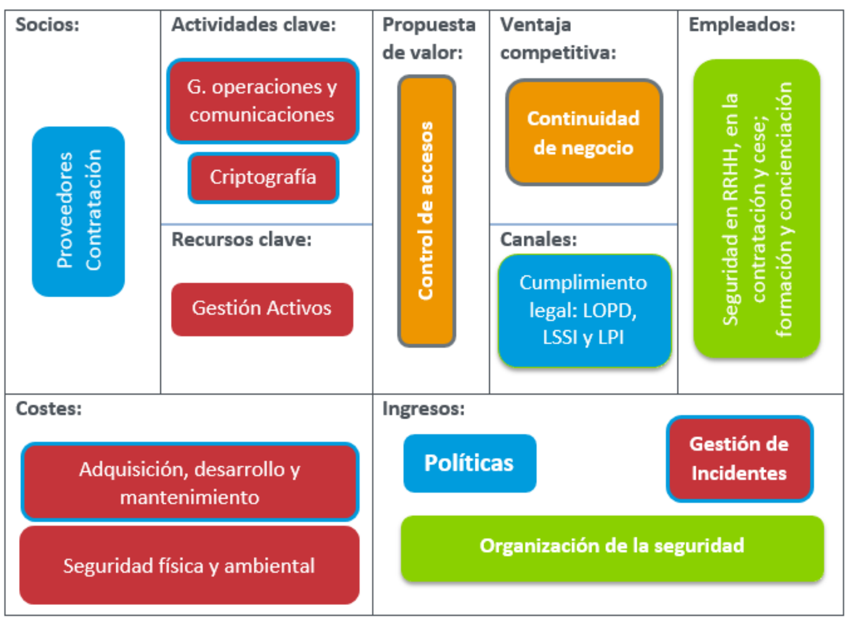


Figura 4Enfoque Canvas Tomado de (INCIBE, 2016)

Al tener una visión global de la norma con enfoque de negocio, la seguridad y aspectos clave del bróker se procedió con el diseño del modelo operacional tomando como base la norma ISO 27001 y el marco de referencia NIST.

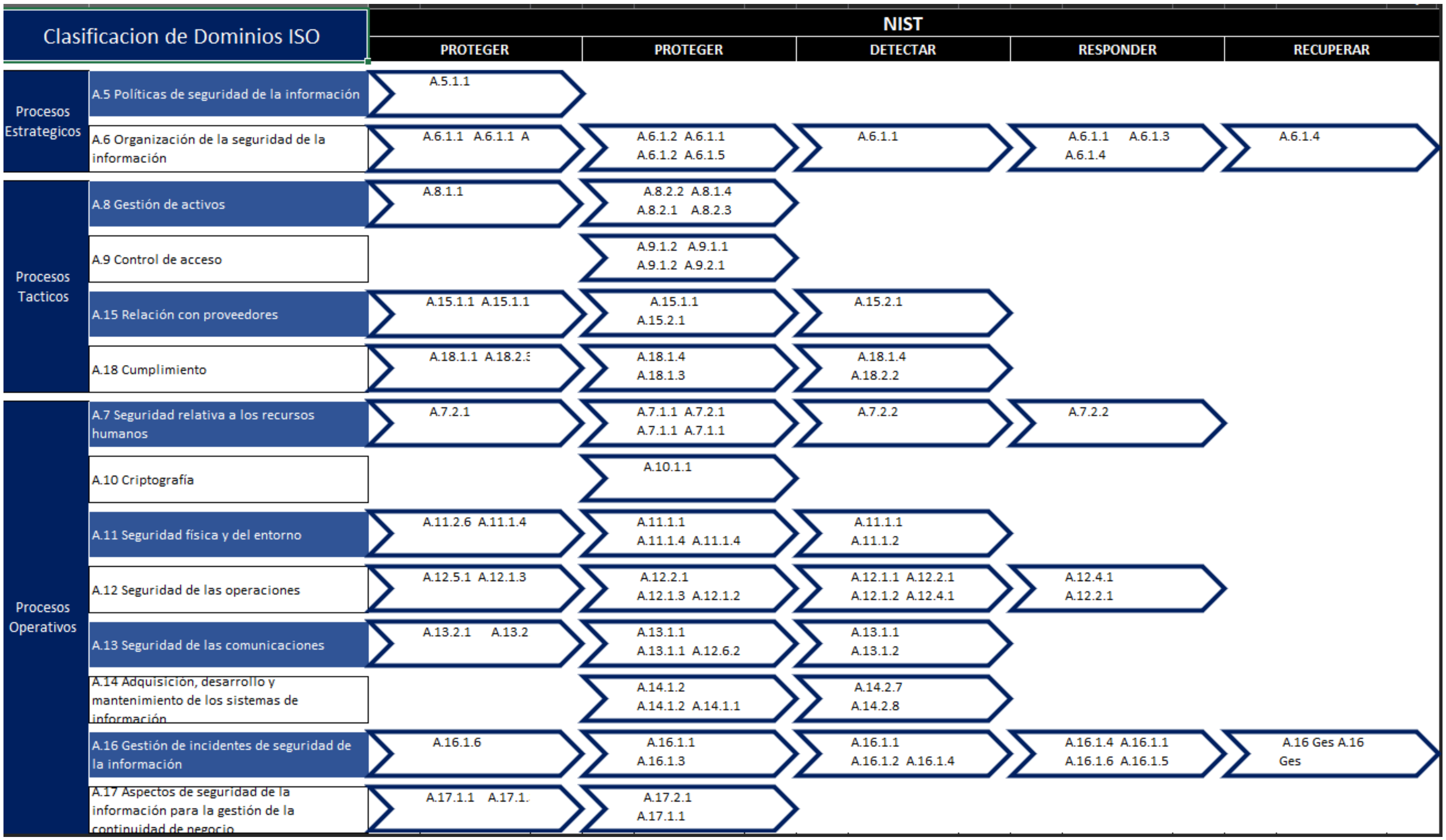


Figura 5 Metodología de Evaluación SGSI adaptado de ISO (Ministerio de Industria c. y., 2017) NIST (Technology, 2018)

2.2.3.3. Métricas de los procesos

Para Identifica las métricas que se van a utilizar se tomara el marco de Referencia NIST de acuerdo con las funciones Identificar, Proteger, Detectar, Responder, Recuperar tomando en cuenta el activo de información definido.

Las métricas serán definidas por el marco de referencia COBIT, a continuación, se presenta la relación ISO NIST COBIT.

Cod	Nombre Norma ISO 27001
A.5	Políticas de seguridad de la información
A.6	Organización de la seguridad de la información
A.7	Seguridad relativa a los recursos humanos
A.8	Gestión de activos
A.9	Control de acceso
A.10	Criptografía
A.11	Seguridad física y del entorno
A.12	Seguridad de las operaciones
A.13	Seguridad de las comunicaciones
A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información
A.15	Relación con proveedores
A.16	Gestión de incidentes de seguridad de la información
A.17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio
A.18	Cumplimiento

		NIST / ISO
Identificar	Gestión de activos	A.8.1.1 Inventario de activos
Proteger	Seguridad de datos	A.8.2.2 Etiquetado de la información
		A.8.2.3 Manipulado de la información
		A.8.3.1 Gestión de soportes extraíbles
		A.8.3.2 Eliminación de soportes
		A.8.3.3 Soportes físicos en tránsito
	Procesos y procedimientos de protección de la información	A.8.1.4 Devolución de activos
		A.8.2.3 Manipulado de la información
		A.8.3.1 Gestión de soportes extraíbles
		A.8.3.2 Eliminación de soportes

Figura 6 Cruce Norma ISO / NIST adaptado de (Technology, 2018)

RELACION NIST / COBIT

NIST / ISO			COBIT 5															
			APO					BAI			DSS							
Identificar	Gestión de activos	A.8.1.1 Inventario de activos						BAI09.01	BAI09.02									
Proteger	Seguridad de datos	A.8.2.2 Etiquetado	APO01.06	APO13.01								DSS05.02		DSS05.04	DSS05.06	DSS05.07	DSS06.02	
		A.8.2.3 Manipulado de la información	APO01.06	APO13.01				BAI02.01	BAI06.01	BAI09.03	DSS04.07	DSS05.02	DSS05.03	DSS05.04	DSS05.06	DSS05.07	DSS06.02	DSS06.06
		A.8.3.1 Gestión de soportes extraíbles		APO13.01						BAI09.03		DSS05.02			DSS05.06			
		A.8.3.2 Eliminación de soportes								BAI09.03					DSS05.06			
		A.8.3.3 Soportes físicos en tránsito		APO13.01						BAI09.03		DSS05.02			DSS05.06			
	Procesos y procedimientos de protección de la	A.8.1.4 Devolución	APO07.01	APO07.02	APO07.03	APO07.04	APO07.05											
		A.8.2.3 Manipulado de la información	APO01.06	APO13.01				BAI02.01	BAI06.01	BAI09.03	DSS04.07	DSS05.02	DSS05.03	DSS05.04	DSS05.06	DSS05.07	DSS06.02	DSS06.06
		A.8.3.1 Gestión de soportes extraíbles		APO13.01						BAI09.03		DSS05.02			DSS05.06			
		A.8.3.2 Eliminación de soportes								BAI09.03					DSS05.06			

Figura 7 Cruce NIST/ISO VS COBIT5 adaptado de ISO (Ministerio de Industria c. y., 2017) NIST (Technology, 2018)

Como se puede revisar los procesos que tienes mayor énfasis dentro de la norma ISO 27001 A.8 gestión de Activos con relación al marco de referencia COBIT 5 son los siguientes procesos.

APO13.01 Establecer y mantener un SGSI.

BAI09.03 Gestionar el ciclo de vida de los activos.

DSS05.02 Gestionar la seguridad de la red y las conexiones.

DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

Métricas modelo	
APO13.01 Establecer y mantener un SGSI.	DSS05.02 Gestionar la seguridad de la red y las conexiones.
a. Nivel de satisfacción de las partes interesadas con el plan de seguridad en toda la empresa	a. Número de brechas del firewall b. Número de vulnerabilidades descubiertas c. Porcentaje de tiempo que la red y los sistemas no están disponibles debido a incidentes de seguridad
BAI09.03 Gestionar el ciclo de vida de los activos.	DSS05.06 Gestionar documentos sensibles y dispositivos de salida.
a. Porcentaje de activos gestionados desde la adquisición hasta su disposición b. Porcentaje de uso por activo c. Porcentaje de activos desplegados que siguen el ciclo de vida de implementación estándar	a. Número de dispositivos de salida robados. b. Porcentaje de documentos sensibles y dispositivos de salida identificados en el inventario

Figura 8 Métricas Modelo de Evaluación de SGSI adaptado de (ISACA, 2012)

2.2.4. Fase 4 Análisis de amenazas y vulnerabilidades de activos de información críticos.

2.2.4.1. Evaluación de Riesgos de Activos Críticos

2.2.4.1.1. Identificación de Amenazas y Vulnerabilidades

2.2.4.1.1.1. Amenaza

Evento que puede desencadenar en un incidente de seguridad.

Para la presente evaluación de amenazas se procede a utilizar los marcos de referencia MargerIt y el Anexo C de la norma ISO 27005.

Para el uso de la herramienta MargerIt se procedió con la elaboración de una matriz que permita identificar la amenaza según el tipo de Activo, así según lo definido en la sección 2.3.3.1. Identificación de activos críticos, se definió como uno de sus activos críticos el equipo Laptop del Gerente Comercial, este al ser catalogado según el marco de referencia MargeriT como Tipo de activo [HW] Equipamiento informático (hardware) presentan las siguientes amenazas.

Tabla 7 Anexo C ISO 27005

Amenaza		Tipo de Activo [HW] Equipamiento informático (hardware)
[N] Desastres naturales	[N.1] Fuego	D
	[N.2] Daños por agua	D
	[N.*] Desastres naturales	D
[I] De origen industrial	[I.1] Fuego	D
	[I.2] Daños por agua	D
	[I.*] Desastres industriales	D
	[I.3] Contaminación mecánica	D
	[I.4] Contaminación electromagnética	D
	[I.5] Avería de origen físico o lógico	D
	[I.6] Corte del suministro eléctrico	D
	[I.7] Condiciones inadecuadas de temperatura o humedad	D
	[I.11] Emanaciones electromagnéticas	C
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	C
	[E.2] Errores del administrador	D I C
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D
	[E.24] Caída del sistema por agotamiento de recursos	D
	[E.25] Pérdida de equipos	D C
[A] Ataques intencionados	[A.6] Abuso de privilegios de acceso	C I D
	[A.7] Uso no previsto	D C I
	[A.11] Acceso no autorizado	C I
	[A.23] Manipulación de los equipos	C D
	[A.24] Denegación de servicio	D
	[A.25] Robo	D C
	[A.26] Ataque destructivo	D

Para el uso del Anexo C de la norma ISO 27005 se procedió con la toma total de las amenazas para evaluación del activo las cuales serán definidas a partir del análisis de vulnerabilidades.

Tabla 8 Identificación de amenazas según su origen

Tipo	Amenazas	Origen		
		D (deliberadas)	A (accidentales)	E (ambientales)
Daño físico	Fuego	D	A	E
	Daño por agua	D	A	E
	Contaminación	D	A	E
	Accidente importante	D	A	E
	Destrucción del equipo o los medios	D	A	E
	Polvo, corrosión, congelamiento	D	A	E
Eventos naturales	Fenómenos climáticos			E
	Fenómenos sísmicos			E
	Fenómenos volcánicos			E
	Fenómenos meteorológicos			E
	Inundación			E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	D	A	
	Pérdida de suministro de energía	D	A	E
	Falla en el equipo de telecomunicaciones	D	A	
Perturbación debida a la radiación	Radiación electromagnética	D	A	E
	Radiación térmica	D	A	E
	Impulsos electromagnéticos	D	A	E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D		
	Espionaje remoto	D		
	Escucha encubierta	D		
	Hurto de medios o documentos	D		
	Hurto de equipo	D		
	Recuperación de medios reciclados o desechados	D		
	Divulgación	D	A	
	Datos provenientes de fuentes no confiables	D	A	
	Manipulación con hardware	D		
	Manipulación con software	D	A	
	Detección de la posición	D		
Fallas técnicas	Falla del equipo		A	
	Mal funcionamiento del equipo		A	
	Saturación del sistema de información	D	A	
	Mal funcionamiento del software		A	
	Incumplimiento en el mantenimiento del sistema de información	D	A	
Acciones no autorizadas	Uso no autorizado del equipo	D		
	Copia fraudulenta del software	D		
	Uso de software falso o copiado	D	A	
	Corrupción de los datos	D		
	Procesamiento ilegal de los datos	D		
Compromiso de las funciones	Error en el uso		A	
	Abuso de derechos	D	A	
	Falsificación de derechos	D		
	Negación de acciones	D		
	Incumplimiento en la disponibilidad del personal	D	A	E

2.2.4.1.1.2. Vulnerabilidad

Posibilidad de materialización de una amenaza.

Para el análisis de vulnerabilidades de los activos de información se utilizó el Anexo D de la norma ISO 27005 en el cual se presenta una conexión directa entre amenazas y vulnerabilidades según su categoría.

Tabla 9 Anexo D ISO 27005

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
Hardware	Sensibilidad a la radiación electromagnética	Radiación electromagnética
Hardware	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
Hardware	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
Hardware	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
Hardware	Almacenamiento sin protección	Hurto de medios o documentos
Hardware	Falta de cuidado en la disposición final	Hurto de medios o documentos
Hardware	Copia no controlada	Hurto de medios o documentos

Con el Anexo presentado se procedió a realizar la vinculación de todas amenazas presentadas con las posibles vulnerabilidades según los marcos de referencia.

Los marcos de referencia seleccionados al contener un modelo de estándar de las posibles amenazas y vulnerabilidades que se puede encontrar en una organización no permiten tener una visión especifica a las necesidades del Bróker ABC, por lo que se procede a identificar aquellas vulnerabilidades reales de acuerdo con el entorno organizacional.

2.2.4.1.1.3. Riesgo Inherente

El riesgo inherente es aquel que puede existir de manera intrínseca en toda actividad.

Para la calificación del riesgo inherente se debe tomar en cuenta que es el resultado de la probabilidad por el impacto.

Probabilidad: Cálculo matemático de las posibilidades que existen de que un evento se cumpla o suceda al azar calificándolo de la siguiente manera.

Tabla 10 Identificación de Riesgo

RARO	Sería especialmente raro que ocurriera
POCO PROBABLE	Probabilidad baja
POSIBLE	Probabilidad media
PROBABLE	Probabilidad alta
CERTEZA	Probabilidad muy alta

Impacto: Es la diferencia entre las estimaciones del estado de seguridad del activo antes y después de materializar las amenazas.

Tabla 11 Descripción del Impacto

	Niveles de impacto				
Descripción del Impacto	INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
1. Pérdidas financieras			< 3% Patrimonio	Entre 4%-19% Patrimonio	>20% Patrimonio
3. Interrupción de operaciones parciales y/o totales		< 2días	2-5 días	>5 día y <10 días	>10 días
4. Pérdida / Degradación de la Imagen institucional				Fuga Hasta 50% Clientes	Fuga >50% Clientes
6. Pérdidas / Destrucción / afectación de bienes materiales	Sin perdida de activos	Depreciación de activos	Deterioro de activos hasta 10% mayor al promedio	Deterioro de activos hasta 50% al promedio	Deterioro o Perdida total del Activo

Calificación de severidad del riesgo.

A partir de la evaluación de Probabilidad x Impacto se procede a definir el riesgo que posee el activo de información crítico seleccionado, según lo establecido en la sección 2.3.2. Clasificación de la información, y la sección 2.3.3.1. Identificación de activos críticos.

Tabla 12 Mapa de Calificación de severidad de riesgo

MAPA DE CALIFICACIÓN SEVERIDAD DE RIESGO						
		IMPACTO				
		INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
Probabilidad	RARO	BAJO	BAJO	MODERADO	MODERADO	ALTO
	POCO PROBABLE	BAJO	BAJO	MODERADO	ALTO	ALTO
	POSIBLE	BAJO	MODERADO	MODERADO	ALTO	CRÍTICO
	PROBABLE	BAJO	MODERADO	ALTO	CRÍTICO	CRÍTICO
	CERTEZA	MODERADO	MODERADO	ALTO	CRÍTICO	CRÍTICO

2.2.4.1.2. Análisis de Riesgo y Planes de Acción

2.2.4.1.2.1. Riesgo Residual

Los peligros que persisten después de haber implementado todos los controles y medidas de prevención respecto del riesgo inherente se denomina riesgo residual.

Para realizar el análisis de riesgo se deben inventariar todos los controles existentes de acuerdo con las vulnerabilidades aplicadas al Bróker.

Se analizó cada uno de los controles encontrados, lo que permitió definir el riesgo Residual y a partir de este se generan planes de acción que serán el cuerpo de nuestro programa de SGSI.

2.3. Resultados y Entregables

2.3.1. Fase 1 Diagnóstico

2.4.1.1. Informe de Evaluación del estado actual de la Gestión del SGSI

Una vez realizada la evaluación del estado actual de Sistema de Gestión de Seguridad de la Información se definieron las siguientes acciones de mejora tomando dentro de cada Control establecido en la norma ISO 27001, únicamente se mostrar la principal acción de mejora, el documento completo se lo podrá revisar en la sección de Anexos.

ACCIONES DE MEJORA		
Controles & Objetivos	**Acciones**	
Políticas de seguridad de la información	Proporcionar orientación y apoyo al programa de SGSI a través de	
	1	Elaboración de Política se SGSI que evidencia una estructura y jerarquía de administración de los activos de información críticos cubriendo riesgos y controles relevantes según la norma ISO
Organización de la seguridad de la información	Establecer un marco de gestión que permita administrar el programa de SGSI mediante	
	1	Elaboración de una política que permita definir roles y responsabilidades asignados de acuerdo con las capacidades y competencia del personal a través de una matriz RACI
Seguridad relativa a los recursos humanos	Asegurarse que los empleados entiendan sus obligaciones y responsabilidades según:	
	1	Evaluaciones que permitan identificar el entendimiento de las normas y políticas internas con realización al programa de SGSI
Gestión de activos	Identificar los activos de la organización tomando en cuenta lo siguiente	
	1	Elaboración de un esquema estructurado para la identificación y clasificación de activos de información que no solo contenga la información de clientes sino un propietario del manejo de la información basado en la confidencialidad, integridad y disponibilidad
Control de acceso	Limitar el acceso a los recursos de tratamiento de la información y a la información a través de:	
	1	Elaboración de política de control de acceso el cual deberá contener Segregación de documentación de aprobación de acceso, control y supervisión, sistemas de autenticación y evaluación del sistema de control de acceso
Criptografía	Definir un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y /o integridad de la información mediante:	
	1	Elaboración de política de controles criptográficos

Figura 9 Acciones de Mejora

ACCIONES DE MEJORA		
Controles & Objetivos	**Acciones**	
Seguridad física y del entorno	Prevenir el acceso físico no autorizado y mantenimiento de instalaciones utilizando	
	1	Uso de sistemas biométricos o tarjetas de proximidad
Seguridad de las operaciones	Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información. Mediante:	
	1	Procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.
Seguridad de las comunicaciones	Asegurar la protección de la transmisión de la información a través de	
	1	Elaboración de procedimientos de transmisión segura de información manteniendo el principio de confidencialidad y privacidad
Adquisición, desarrollo y mantenimiento de los sistemas de información	Garantizar que la seguridad de la información sea parte integral de los sistemas de información utilizando:	
	1	Procedimientos para analizar riesgos y requisitos funcionales y técnicos en la adquisición de sistemas y software
Relación con proveedores	Asegurar la protección de los activos de la organización mediante	
	1	Elaboración de políticas relacionados con la gestión de proveedores que involucran servicios de TI
Gestión de incidentes de seguridad de la información	Asegurar un enfoque eficaz para la gestión de incidentes de seguridad de la información que incluya	
	1	Políticas y procedimientos para la gestión de incidentes
Aspectos de seguridad de la información para la gestión de la continuidad de negocio	Integrar la seguridad de la información a los sistemas de gestión de la continuidad de negocio de la organización mediante	
	1	Elaboración de un plan de continuidad de negocio que identifique impacto, plazos de restauración del servicio, acuerdos de responsabilidad y procedimientos de recuperación
Cumplimiento	Evitar incumplimientos de las obligaciones legales relativas a la seguridad de la información tomando en cuenta	
	1	Ley Orgánica de Tratamiento de Datos Personales

2.3.2. Fase 2 Clasificación de la Información

2.3.2.1. Clasificación de los tipos de Información

La Clasificación de la información del Bróker ABC de acuerdo con las entrevistas realizadas se pudo definir lo siguiente únicamente tomando la entidad Clientes.

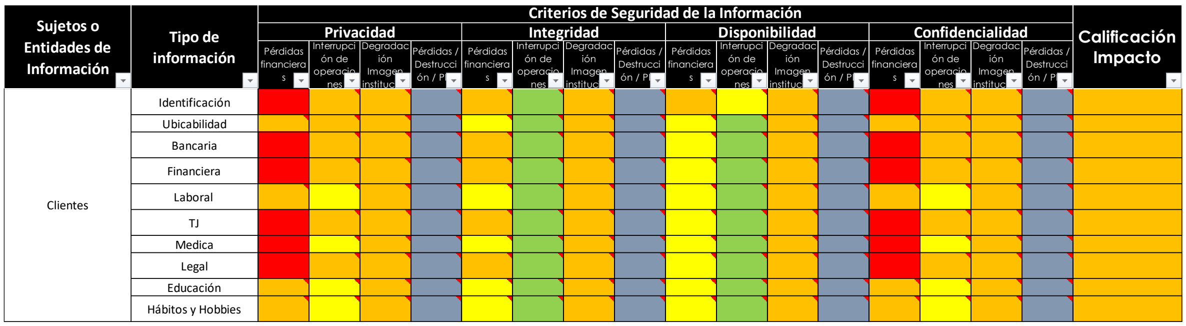


Figura 10 Criterios de Seguridad de la información

2.3.3. Fase 3 Inventario de Activos de Información

2.3.3.1. Activos de Información críticos identificados y clasificados

Una vez realizado el inventario de activos de información a continuación se presenta el resultado resumen del inventario de los activos de información, dentro de la sección de Anexos se podrá visualizar el documento completo.

Identificador	Nombre del Activo	Identificación del Activo de Información	Formato	Procesos	Responsable	Tipo de Información	Criterio				Criticidad	Ubicación del Activo
							P	I	D	C		
ACIF_0001	Computador Portátil Gerente Comercial	Carpeta Clientes Actuales	Archivos de Imagen - Archivo de Excel	Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Identificación de Clientes						Oficina Gerente Comercial
				Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Ubicabilidad de Clientes						
				Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Bancaria de Clientes						
				Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Financiera de Clientes						
				Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Laboral de Clientes						
				Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información TJ de Clientes						
				Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Medica de Clientes						
				Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Legal de Clientes						
				Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Educación de Clientes						
				Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Hábitos y Hobbies de Clientes						
		Carpeta Seguros Actual	Medio electrónico	Colocación de nuevos productos	Gerente Comercial	Información Catálogo Productos & Precios de Organización						
		Carpeta Seguros Actual	Medio electrónico	Colocación de nuevos productos / Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Catálogo Productos & Precios de Proveedores						

Figura 11 Inventario de Activos de información

2.3.4. Fase 4 Análisis de amenazas y vulnerabilidades de activos de información críticos

2.3.4.1. Amenazas Identificadas

Entidad	Nombre Activo	Tipo de Información	Identificar posibles amenazas		
			Fuente	Descripción	Subtipo de Amenaza
Clientes	Computador Portátil Gerente Comercial	Identificación Ubicabilidad Bancaria Financiera Laboral TJ Medica Legal Educación Hábitos y hobbies	Margerit	[N] Desastres naturales	[N.*] Desastres naturales
				[I] De origen industrial	[I.1] Fuego
					[I.2] Daños por agua
					[I.*] Desastres industriales
					[I.4] Contaminación electromagnética
					[I.5] Avería de origen físico o lógico
					[I.6] Corte del suministro eléctrico
					[I.7] Condiciones inadecuadas de temperatura o humedad
					[I.11] Emanaciones electromagnéticas
				[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios
					[E.2] Errores del administrador
					[E.23] Errores de mantenimiento / actualización de equipos (hardware)
					[E.24] Caída del sistema por agotamiento de recursos
					[E.25] Pérdida de equipos
				[A] Ataques intencionados	[A.6] Abuso de privilegios de acceso
					[A.7] Uso no previsto
					[A.11] Acceso no autorizado
					[A.23] Manipulación de los equipos
					[A.24] Denegación de servicio
					[A.25] Robo
					[A.26] Ataque destructivo

Figura 12 Identificación de Amenazas

2.3.4.1. Principales Vulnerabilidades Reales Identificadas

Entidad	Nombre Activo Información	Tipo de Información	Vulnerabilidades reales	
			Tipo	Ejemplo
Clientes	Computador Portátil Gerente Comercial	Identificación Ubicabilidad Bancaria Financiera Laboral TJ Medica Legal Educación Hábitos y hobbies	Hardware	Ausencia de esquemas de reemplazo periódico.
			Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.
			Hardware	Ausencia de un eficiente control de cambios en la configuración
			Organización	Ausencia de procedimientos para la introducción del software en los sistemas operativos
			Organización	Ausencia de procedimientos para el manejo de información clasificada
			Personal	Entrenamiento insuficiente en seguridad
			Personal	Uso incorrecto de software y hardware
			Red	Líneas de comunicación sin protección
			Red	Conexiones de red pública sin protección
			Software	Configuración incorrecta de parámetros
			Software	Asignación errada de los derechos de acceso
			Software	Descarga y usos no controlados de software

Figura 13 Identificación de Vulnerabilidades

2.3.5. Fase 5 Documentos clave del SGSI

2.3.5.1. Políticas de alto nivel

Para el cumplimiento de la presente política es necesario que todo el personal conozca los principios y guías en aspectos específicos de la seguridad de la información para su adecuada implementación.

Las políticas deberán contar con la aprobación del directorio y deberán ser comunicadas a todo el personal para su implementación, uso y adecuado tratamiento según lo requiera cada puesto de trabajo, a continuación, se presentan las siguientes políticas que deberán elaborarse de acuerdo con el alcance establecido en el presente documento:

- Política del Sistema de Gestión de Seguridad de la Información (SGSI).
- Política de software no autorizado.
- Política de descarga de ficheros (red externa/interna).
- Política de copias de seguridad.
- Política de uso de los servicios de mensajería.
- Política de retención de registros.
- Política sobre el uso de los servicios de red.
- Política de teletrabajo.
- Política sobre el uso de controles criptográficos.
- Política de uso de licencias de software.
- Política de protección de datos y privacidad.
- Política de definición de roles y responsabilidades organizacionales.
- Política para la gestión de incidentes.
- Política o plan de continuidad del negocio.

2.3.5.2 Planes de Acción y Roadmap

.

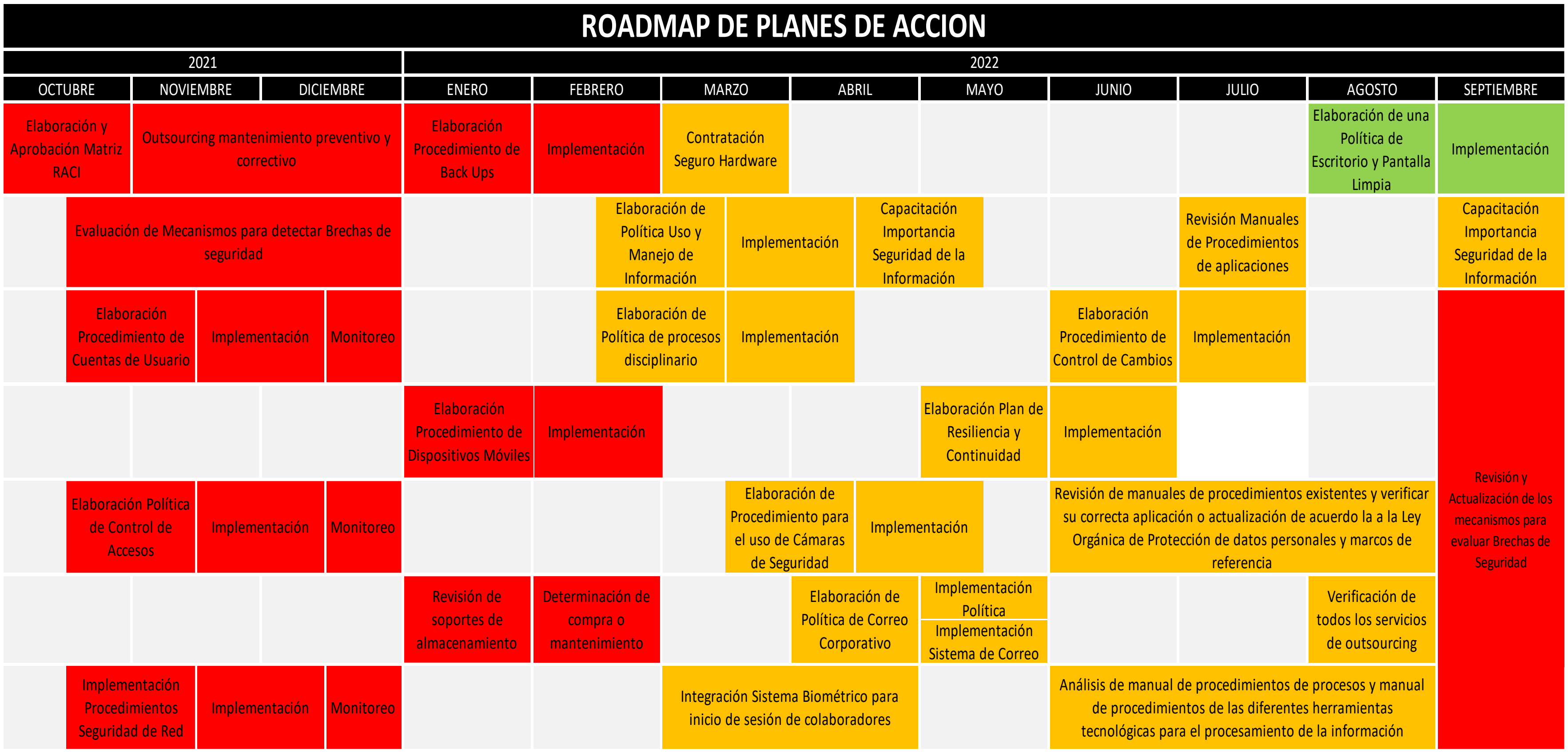


Figura 14Roadmap de Planes de Acción

3. Conclusiones

El presente trabajo permite diagnosticar, analizar y proponer los fundamentos básicos para la implementación de un Sistema de Gestión de Seguridad de la Información tomando como referencia la norma ISO 27001 relacionado con las actividades del Bróker ABC.

El diagnóstico inicial del actual sistema de gestión de seguridad de la información sobre el caso de estudio es primordial, no solo para reconocer la situación actual sino también para evaluar su funcionamiento estructural, además permite la identificación de procesos y políticas que se desarrollan dentro de las actividades del bróker.

La clasificación y la identificación de activos críticos es fundamental para el desarrollo de políticas de alto nivel, una evaluación clara no solo permitirá identificar las entidades, sino también permitirá identificar propietarios de los activos y responsables dentro de los procesos de tratamiento de la información.

Una adecuada definición de políticas del programa de SGSI evitará que se materialicen posibles riesgos minimizando su impacto para la organización, evitando la afectación del adecuado funcionamiento de la organización.

Un Sistema de Gestión de Seguridad de la Información es tan importante como los procesos Core de negocio, al estar en contacto transversal con toda la organización permite desarrollar buenas prácticas en base al riesgo de cada uno de sus activos.

La implementación de un SGSI por parte del Bróker ABC certifica que el manejo, control y administración de la información personal de los clientes sea privada, garantizando la integridad, disponibilidad y confidencialidad.

Para que el programa cumpla con su propósito y objetivos, todos los colaboradores de la empresa deben conocer, cumplir y aplicar la normativa, procedimientos, políticas y controles definidos en el presente documento de seguridad de la información.

4. Referencias

(ICONTEC), I. C. (01 de 09 de 2009). NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27005 . *TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN*. (I. C. (ICONTEC), Ed.) BOGOTA, COLOMBIA. Obtenido de NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27005 TECNOLOGÍA DE LA INFORMACIÓN.

Colombia, F. P. (21 de 12 de 2017). *funcionpublica.gov.co*. (P. Ambrosio, Editor) Recuperado el 05 de 05 de 2021, de Documento Técnico -INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD: https://www.funcionpublica.gov.co/eva/red/publicaciones/documento-t%C3%A9cnico---instrumento-de-evaluaci%C3%B3n-mspi

INCIBE. (18 de 07 de 2016). *INCIBE.* Recuperado el 15 de 08 de 2021, de INCIBE: https://www.incibe.es/en/node/4846

ISACA. (2012). *COBIT ® 5 para Seguridad de la Información.* Estados Unidos. Obtenido de COBIT ® 5 para Seguridad de la Información.

Ministerio de Industria, c. y. (05 de 2014). *MINCOTUR*. Recuperado el 05 de 05 de 2021, de UNE-EN ISO/IEC 27002 Tecnología de la información: https://www.eoi.es/es/file/164952/download?token=eQUyOf6C

Ministerio de Industria, c. y. (05 de 2017). *MINCOTUR*. Recuperado el 06 de 05 de 2021, de Norma Española UNE-EN ISO/IEC 27001: https://www.eoi.es/es/file/166057/download?token=k6tPtilN

Públicas, M. d. (10 de 2012). *ADMINISTRACION ELECTRONICA.GOB.ES.* (M. d. Públicas, Ed.) Recuperado el 09 de 08 de 2021, de MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. : https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

Technology, N. I. (16 de 04 de 2018). *NIST*. Recuperado el 08 de 07 de 2021, de Marco para la mejora de la seguridad cibernética en infraestructuras críticas: https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

ANEXOS

5. Anexos

ANEXO 1 Metodología del estado actual del SGSI

EVALUACION DIAGNOSTICO								
NIVEL	ISO 27001	Nombre Norma	Controles & Objetivos	Preguntas	Calif Preguntas	Ponderación Actual	Objetivo	Calificación de Dominio
NIVEL 1	A.5	Políticas de seguridad de la información				1	100	INEXISTENTE
NIVEL 2	A.5.1	Directrices de gestión de la seguridad de la información	Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.			1	100	INEXISTENTE
NIVEL 3	A.5.1.1	Políticas para la seguridad de la información	Control: Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada?	1	1	100	INEXISTENTE
				¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes?	1			
				¿Hay acuerdos adecuados de cumplimiento y refuerzo?	1			
				¿Están las políticas bien escritas, legibles, razonables y son viables?	1			
				¿Incorporan controles adecuados y suficientes?	1			
				¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.?	1			
NIVEL 3	A.5.1.2	Revisión de las políticas para la seguridad de la información	Control: Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	¿Todas las políticas tienen un formato y estilo consistentes?	1	1	100	INEXISTENTE
				¿Están todos al día, habiendo completado todas las revisiones debidas?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 1	A.6	Organización de la seguridad de la información				16,75833333	100	INICIAL
NIVEL 2	A.6.1	Organización interna	Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			12,1	100	INICIAL
NIVEL 3	A.6.1.1	Roles y responsabilidades en seguridad de la información	Control: Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	¿Se le da suficiente énfasis a la seguridad y al riesgo de la información?	50	8	100	INICIAL
				¿Hay apoyo de la administración?	1			
				¿Existe un foro de alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad?	1			
				¿Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas?	1			
				¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información?	1			
				¿Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información?	1			
				¿Hay coordinación dentro de la organización entre las unidades de negocio?	1			
NIVEL 3	A.6.1.2	Segregación de tareas	Control: Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	¿Son los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas?	1	1	100	INEXISTENTE
				¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea? Responsable | Accountable | Consulted | Informed	1			
				¿Existe una política que cubra la segregación de deberes?	1			
				¿Se realiza un seguimiento regular de las actividades y los registros de auditoría?	1			
NIVEL 3	A.6.1.3	Contacto con las autoridades	Control: Deben mantenerse los contactos apropiados con las autoridades pertinentes.	¿Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias?	1	1	100	INEXISTENTE
NIVEL 3	A.6.1.4	Contacto con grupos de interés especial	Control: Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.	¿Hay un contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad, tales como los capítulos locales de ISACA, ISC 2, ISSA, ISO27k?	50	25	100	REPETIBLE
				¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches?	0			
NIVEL 3	A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes?	50	25,5	100	REPETIBLE
				¿La etapa del proyecto incluye actividades apropiadas?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.6.2	Los dispositivos móviles y el teletrabajo	Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.			21,41666667	100	REPETIBLE
NIVEL 3	A.6.2.1	Política de dispositivos móviles	Control: Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	¿Existen política y controles seguridad relacionados con los usuarios móviles?	50	17,33333333	100	INICIAL
				¿Se distinguen los dispositivos personales de los empresariales?	1			
				¿Se emplean soluciones de MDM y soluciones MAM para controlar las aplicaciones, el acceso y el cifrado completo de disco?	1			
NIVEL 3	A.6.2.2	Teletrabajo	Control: Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	¿Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina?	1	25,5	100	REPETIBLE
				¿Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (Always-on-VPN), antivirus, copias de seguridad, parches, registro de seguridad y monitoreo, encriptación y continuidad del negocio?	50			
NIVEL 1	A.7	Seguridad relativa a los recursos humanos				13,25	100	INICIAL
NIVEL 2	A.7.1	Antes del empleo	Objetivo: Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.			21,41666667	100	REPETIBLE
NIVEL 3	A.7.1.1	Investigación de antecedentes	Control: La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.	¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección?	50	17,33333333	100	INICIAL
				¿Existen procesos de selección mejorados para los trabajadores en roles críticos?	1			
				¿Cómo se logra todo esto? ¿Hay un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH?	1			
NIVEL 3	A.7.1.2	Términos y condiciones del empleo	Control: Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.	¿Están claramente definidos los términos y condiciones de empleo?	50	25,5	100	REPETIBLE
				¿Se hace distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general?	1			
				¿Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles?	1			
				¿Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información?	50			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.7.2	Durante el empleo	Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.			17,33333333	100	INICIAL
NIVEL 3	A.7.2.1	Responsabilidades de gestión	Control: La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	¿Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia?	1	1	100	INEXISTENTE
				¿Se hace de forma regular y está a día?	1			
				¿El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados?	1			
				¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad?	1			
				¿Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización?	1			
NIVEL 3	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Control: Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	¿Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente?	1	1	100	INEXISTENTE
				¿Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores?	1			
				¿Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos?	1			
				¿Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos?	1			
				¿Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas?	1			
				¿Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento?	1			
				¿Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas?	1			
NIVEL 3	A.7.2.3	Proceso disciplinario	Control: Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores?	50	50	100	EFECTIVO
NIVEL 2	A.7.3	Finalización del empleo o cambio en el puesto de trabajo	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.			1	100	INEXISTENTE
NIVEL 3	A.7.3.1	Responsabilidades ante la finalización o cambio	Control: Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización?	1	1	100	INEXISTENTE
				¿Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 1	A.8	Gestión de activos				7,125	100	INICIAL
NIVEL 2	A.8.1	Responsabilidad sobre los activos	Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.			19,375	100	INICIAL
NIVEL 3	A.8.1.1	Inventario de activos	Control: La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.	¿Hay un inventario de activos de la información?	1	1	100	INEXISTENTE
				¿Contiene la siguiente información? • Datos digitales • Información impresa • Software • Infraestructura • Servicios de información y proveedores de servicios • Seguridad física • Relaciones comerciales • Las personas	1			
				¿Es suficientemente detallado y está estructurado adecuadamente?	1			
NIVEL 3	A.8.1.2	Propiedad de los activos	Control: Todos los activos que figuran en el inventario deben tener un propietario.	¿Los activos tienen propietario de riesgo?	1	1	100	INEXISTENTE
				¿Los activos tienen responsable técnico?	1			
NIVEL 3	A.8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.?	1	25,5	100	REPETIBLE
				¿Cubre el comportamiento del usuario en Internet y en las redes sociales?	1			
				¿Se permite el uso personal de los activos de la empresa?	100			
				En caso afirmativo, ¿Se controla / asegura esto?	0			
NIVEL 3	A.8.1.4	Devolución de activos	Control: Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	¿Existe un procedimiento para recuperar los activos tras una baja o despido?	50	50	100	EFECTIVO
NIVEL 2	A.8.2	Clasificación de la información	Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.			1	100	INEXISTENTE
NIVEL 3	A.8.2.1	Clasificación de la información	Control: La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	¿Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información?	1	1	100	INEXISTENTE
				¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad?	1			
				¿Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen?	1			
				¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados?	1			
NIVEL 3	A.8.2.2	Etiquetado de la información	Control: Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica?	1	1	100	INEXISTENTE
				¿Está sincronizado con la política de clasificación de la información?	1			
NIVEL 3	A.8.2.3	Manipulado de la información	Control: Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	¿Están los niveles de clasificación adecuadamente asignados a los activos?	1	1	100	INEXISTENTE

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.8.3	Manipulación de los soportes	Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.			1	100	INEXISTENTE
NIVEL 3	A.8.3.1	Gestión de soportes extraíbles	Control: Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles?	1	1	100	INEXISTENTE
				¿Los medios extraíbles están debidamente etiquetados y clasificados?	1			
				¿Los medios se mantienen y almacenan de forma adecuada?	1			
				¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?	1			
NIVEL 3	A.8.3.2	Eliminación de soportes	Control: Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.	¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios?	1	1	100	INEXISTENTE
				¿Se documenta la aprobación en cada etapa para la eliminación de los medios?	1			
				¿Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación?	1			
				¿Se tiene en cuenta los periodos de retención?	1			
				¿Los datos particularmente confidenciales se eliminan de forma segura (borrado criptográfico, desmagnetización o destrucción física)?	1			
NIVEL 3	A.8.3.3	Soportes físicos en tránsito	Control: Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	¿Se utiliza un transporte o servicio de mensajería confiable?	1	1	100	INEXISTENTE
				¿Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia?	1			
				¿Se verifica la recepción por el destino?	1			
NIVEL 1	A.9	Control de acceso				18,9844246	100	INICIAL
NIVEL 2	A.9.1	Requisitos de negocio para el control de acceso	Objetivo: Limitar el acceso a los recursos de tratamiento de la información y a la información .			7,125	100	INICIAL
NIVEL 3	A.9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	¿Existe una política de control de acceso?	1	1	100	INEXISTENTE
				¿Es consistente con la política de clasificación?	1			
				¿Hay una segregación de deberes apropiada?	1			
				¿Existe un proceso documentado de aprobación de acceso?	1			
				¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?	1			
NIVEL 3	A.9.1.2	Acceso a las redes y a los servicios de red	Control: Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado?	1	13,25	100	INICIAL
				¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados?	50			
				¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)?	1			
				¿La organización mide la identificación y los tiempos de respuesta ante incidentes?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.9.2	Gestión de acceso de usuario	Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.			7,712698413	100	INICIAL
NIVEL 3	A.9.2.1	Registro y baja de usuario	Control: Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	¿Se utiliza un ID de usuario únicos para cada usuario?	50	10,8	100	INICIAL
				¿Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido?	1			
				¿Existen una comunicación eficiente ente la Administración de Seguridad y Recursos Humanos?	1			
				¿Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes?	1			
				¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios?	1			
NIVEL 3	A.9.2.2	Provisión de acceso de usuario	Control: Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio?	1	1	100	INEXISTENTE
				¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones?	1			
				¿Existe un registro documental de la solicitud y aprobación de acceso?	1			
NIVEL 3	A.9.2.3	Gestión de privilegios de acceso	Control: La asignación y el uso de privilegios de acceso debe estar restringida y controlada.	¿Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios?	50	17,33333333	100	INICIAL
				¿Se ha establecido una caducidad para los ID de usuario con privilegios?	1			
				¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?	1			
NIVEL 3	A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Control: La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.?	1	15,14285714	100	INICIAL
				¿Se verifica rutinariamente si hay contraseñas débiles?	1			
				¿Se requiere confirmar la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas?	1			
				¿Se transmite dicha información por medios seguros?	1			
				¿Se generan contraseñas temporales suficientemente fuertes?	1			
				¿Se cambian las contraseñas por defecto de los fabricantes?	100			
				¿Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?	1			
NIVEL 3	A.9.2.5	Revisión de los derechos de acceso de usuario	Control: Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones?	1	1	100	INEXISTENTE
				¿Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios?	1			
				¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente?	1			
NIVEL 3	A.9.2.6	Retirada o reasignación de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	¿Existe un proceso de ajuste de derechos de acceso?	1	1	100	INEXISTENTE
				¿Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo?	1			
				¿Incluye el acceso físico a las instalaciones y el acceso lógico a la red?	1			
				En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.9.3	Responsabilidades del usuario	Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.			25,5	100	REPETIBLE
NIVEL 3	A.9.3.1	Uso de la información secreta de autenticación	Control: Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	¿Existe un proceso de cambio de contraseñas en caso de ser comprometida?	50	25,5	100	REPETIBLE
				¿Existen controles de seguridad relativas a las cuentas compartidas?	1			
NIVEL 2	A.9.4	Control de acceso a sistemas y aplicaciones	Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.			35,6	100	REPETIBLE
NIVEL 3	A.9.4.1	Restricción del acceso a la información	Control: Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	¿Existen controles de acceso adecuados?	50	75	100	GESTIONADO
				¿Se identifican los usuarios de forma individual individuales?	100			
NIVEL 3	A.9.4.2	Procedimientos seguros de inicio de sesión	Control: Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.	¿Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado?	1	1	100	INEXISTENTE
				¿Se utiliza autenticación multifactorial para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.?	1			
				¿Se registran los inicios de sesión exitosos?	1			
				¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?	1			
NIVEL 3	A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.	¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos?	100	100	100	OPTIMIZADO
				¿Las reglas tienen en cuenta lo siguiente? • Longitud mínima de la contraseña • Evitan la reutilización de un número específico de contraseñas • Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.) • Requiere el cambio forzado de contraseñas en el primer inicio de sesión • Esconde la contraseña durante la imputación	100			
NIVEL 3	A.9.4.4	Uso de utilidades con privilegios del sistema	Control: Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	¿Se verifica la necesidad comercial para otorgar el acceso según su roles y responsabilidades?	1	1	100	INEXISTENTE
				¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado?	1			
				¿Se tiene en cuenta la segregación de tareas?	1			
NIVEL 3	A.9.4.5	Control de acceso al código fuente de los programas	Control: Se debe restringir el acceso al código fuente de los programas.	¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios?	1	1	100	INEXISTENTE
				¿El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.?	1			
				¿Se almacenan y revisan los registros de acceso y cambios?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 1	A.10	Criptografía				8	100	INICIAL
NIVEL 2	A.10.1	Controles criptográficos	Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y /o integridad de la información.			8	100	INICIAL
NIVEL 3	A.10.1.1	Política de uso de los controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	¿Existe una política que cubra el uso de controles criptográficos?	1	1	100	INEXISTENTE
				¿Cubre lo siguiente? • Los casos en los que información debe ser protegida a través de la criptografía • Normas que deben aplicarse para la aplicación efectiva • Un proceso basado en el riesgo para determinar y especificar la protección requerida • Uso de cifrado para información almacenada o transferida • Los efectos de cifrado en la inspección de contenidos de software • Cumplimiento de las leyes y normativas aplicables	1			
				¿Se cumple con la política y requerimientos de cifrado?	1			
NIVEL 3	A.10.1.2	Gestión de claves	Control: Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)?	1	15	100	INICIAL
				¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas?	1			
				¿Se generan claves diferentes para sistemas y aplicaciones?	50			
				¿Se evitan claves débiles?	50			
				¿Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)?	1			
				¿Se hacen copias de respaldo de las claves?	1			
				¿Se registran las actividades clave de gestión?	1			
NIVEL 1	A.11	Seguridad física y del entorno				17,04960317	100	INICIAL
NIVEL 2	A.11.1	Áreas seguras	Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.			21,23809524	100	REPETIBLE
NIVEL 3	A.11.1.1	Perímetro de seguridad física	Control: Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.	¿Las instalaciones se encuentran en una zona de segura?	100	50,42857143	100	EFECTIVO
				¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)?	1			
				¿El techo exterior, las paredes y el suelo son de construcción sólida?	100			
				¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado?	50			
				¿Las puertas y ventanas son fuertes y con cerradura?	100			
				¿Se monitorea los puntos de acceso con cámaras?	1			
				¿Existe un sistema de detección de intrusos y se prueba periódicamente?	1			
NIVEL 3	A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)?	1	1	100	INEXISTENTE
				¿Hay procedimientos que cubran las siguientes áreas? • Cambio regular código de acceso • Inspecciones de las guardias de seguridad • Visitantes siempre acompañados y registrados en el libro de visitantes • Registro de movimiento de material • Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas)	1			
				¿Se utiliza autenticación multi-factor de autenticación (ej. Biométrico más el código PIN)?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

				¿Existe un registro de todas las entradas y salidas?	1			
NIVEL 3	A.11.1.3	Seguridad de oficinas, despachos y recursos	Control: Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.	¿Están los accesos (entrada y salida) de las instalaciones físicamente controladas (ej. Detectores de proximidad, CCTV)?	1	34	100	REPETIBLE
				¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos?	1			
				¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?	100			
NIVEL 3	A.11.1.4	Protección contra las amenazas externas y ambientales	Control: Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	¿Existen protecciones contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.?	100	34	100	REPETIBLE
				¿Existe un procedimiento de recuperación de desastres?	1			
				¿Se contemplan sitios remotos?	1			
NIVEL 3	A.11.1.5	El trabajo en áreas seguras	Control: Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.	¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo?	50	8	100	INICIAL
				¿Se hace un análisis para evaluar que los controles adecuados están implementados?	1			
				Controles de acceso físico	1			
				Alarmas de intrusión	1			
				Monitoreo de CCTV (verificar la retención y frecuencia de revisión)	1			
				Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación	1			
				Políticas, procedimientos y pautas	1			
NIVEL 3	A.11.1.6	Áreas de carga y descarga	Control: Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.	¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado?	0	0	100	INEXISTENTE
				¿Se verifica que el material recibido coincide con un número de pedido autorizado?	0			
				¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?	0			
NIVEL 2	A.11.2	Seguridad de los equipos	Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización n.			12,86111111	100	INICIAL
NIVEL 3	A.11.2.1	Emplazamiento y protección de equipos	Control: Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.	¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas?	1	13,25	100	INICIAL
				¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada?	1			
				¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales? • Agua / inundación • Fuego y humo • Temperatura, humedad y suministro eléctrico • Polvo • Rayos, electricidad estática y seguridad del personal	50			
				¿Se prueban estos controles periódicamente y después de cambios importantes?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 3	A.11.2.2	Instalaciones de suministro	Control: Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad?	1	1	100	INEXISTENTE
				¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente?	1			
				¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante?	1			
				¿Son probados con regularidad?	1			
				¿Hay una red de suministro eléctrico redundante?	1			
				¿Se realizan pruebas de cambio?	1			
				¿Se ven afectados los sistemas y servicios?	1			
				¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos?	1			
				¿Están ubicados apropiadamente?	1			
				¿Hay una capacidad adecuada de A / C para soportar la carga de calor?	1			
				¿Hay unidades redundantes, de repuesto o portátiles disponibles?	1			
				¿Hay detectores de temperatura con alarmas de temperatura?	1			
NIVEL 3	A.11.2.3	Seguridad del cableado	Control: El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.	¿Hay protección física adecuada para cables externos, cajas de conexiones?	1	13,25	100	INICIAL
				¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias?	1			
				¿Se controla el acceso a los paneles de conexión y las salas de cableado?	50			
				¿Existen procedimientos adecuados para todo ello?	1			
NIVEL 3	A.11.2.4	Mantenimiento de los equipos	Control: Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)?	100	34	100	REPETIBLE
				¿Hay programas de mantenimiento y registros / informes actualizados?	1			
				¿Se aseguran los equipos?	1			
NIVEL 3	A.11.2.5	Retirada de materiales propiedad de la empresa	Control: Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	¿Existen procedimiento relativos al traslado de activos de información?	1	13,25	100	INICIAL
				¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados?	50			
				¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo?	1			
				¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?	1			
NIVEL 3	A.11.2.6	Seguridad de los equipos fuera de las instalaciones	Control: Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	¿Existe una "política de uso aceptable" que cubra los requisitos de seguridad y "obligaciones" con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas?	1	1	100	INEXISTENTE
				¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras?	1			
				¿Existen controles para asegura todo esto?	1			
				¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 3	A.11.2.7	Reutilización o eliminación segura de equipos	Control: Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.	¿Se utiliza cifrado fuerte o borrado seguro?	1	1	100	INEXISTENTE
				¿Se mantienen registros adecuados de todos los medios que se eliminan?	1			
				¿La política y el proceso cubren todos los dispositivos y medios de TIC?	1			
NIVEL 3	A.11.2.8	Equipo de usuario desatendido	Control: Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.	¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción?	1	1	100	INEXISTENTE
				¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado?	1			
				¿Se protegen los bloqueos de pantalla con contraseña?	1			
				¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC?	1			
NIVEL 3	A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Control: Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas?	1	38	100	REPETIBLE
				¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos?	50			
				¿Se activa automáticamente tras de un tiempo inactivo definido?	1			
				¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?	100			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 1	A.12	Seguridad de las operaciones				7,160714286	100	INICIAL
NIVEL 2	A.12.1	Procedimientos y responsabilidades operacionales	Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.			7,125	100	INICIAL
NIVEL 3	A.12.1.1	Documentación de procedimientos operacionales	Control: Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.	¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.?	50	25,5	100	REPETIBLE
				¿Existe un conjunto completo de procedimientos de seguridad?	1			
				¿Los procesos son razonablemente seguros y están bien controlados?	50			
				¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal?	1			
				¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)?	50			
				¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?	1			
NIVEL 3	A.12.1.2	Gestión de cambios	Control: Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben ser controlados.	¿Existe una política de gestión de cambios?	1	1	100	INEXISTENTE
				¿Existen registros relacionados a la gestión de cambios?	1			
				¿Se planifican y gestionan los cambios?	1			
				¿Se evalúan los riesgos potenciales asociados con los cambios?	1			
				¿Los cambios están debidamente documentados, justificados y autorizados por la administración?	1			
NIVEL 3	A.12.1.3	Gestión de capacidades	Control: Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	¿Existe una política de gestión de capacidad?	1	1	100	INEXISTENTE
				¿Existen registros relacionados a la gestión de capacidad?	1			
				¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante?	1			
				¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?	1			
NIVEL 3	A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	Control: Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	¿Se segregan entornos de TIC de desarrollo, prueba y operacionales?	1	1	100	INEXISTENTE
				¿Cómo se logra la separación a un nivel de seguridad adecuado?	1			
				¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)?	1			
				¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos?	1			
				¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección?	1			
				¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros?	1			
				¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.12.2	Protección contra el software malicioso (malware)	Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.			25,75	100	REPETIBLE
NIVEL 3	A.12.2.1	Controles contra el código malicioso	Control: Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	¿Existen políticas y procedimientos asociados a controles antimalware?	1	25,75	100	REPETIBLE
				¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado?	1			
				¿Hay controles de antivirus de "escaneado en acceso" y "escaneo programático" en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT?	100			
				¿Se actualiza el software antivirus de forma automática?	100			
				¿Se general alertas accionables tras una detección?	1			
				¿Se toma acción de forma rápida y apropiada para minimizar sus efectos?	1			
				¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte?	1			
				¿Existe un mecanismo de escalación para incidentes graves?	1			
NIVEL 2	A.12.3	Copias de seguridad	Objetivo: Evitar la pérdida de datos			1	100	INEXISTENTE
NIVEL 3	A.12.3.1	Copias de seguridad de la información	Control: Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.	¿Existen políticas y procedimientos asociados a las copias de seguridad?	1	1	100	INEXISTENTE
				¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio?	1			
				¿Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.?	1			
				¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales?	1			
				¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido?	1			
				¿Se mantienen copias off-line para evitar una propagación de ransomware catastrófica?	1			
				¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar?	1			
				¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.12.4	Registros y supervisión	Objetivo: Registrar eventos y generar evidencias.			13,25	100	INICIAL
NIVEL 3	A.12.4.1	Registro de eventos	Control: Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	¿Existen políticas y procedimientos para el registro de eventos?	1	1	100	INEXISTENTE
				¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí?	1			
				¿Se registra lo siguiente? • cambios en los ID de usuario • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web	1			
				¿Existe un proceso para revisar y responder adecuadamente a las alertas de seguridad?	1			
NIVEL 3	A.12.4.2	Protección de la información del registro	Control: Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable?	50	50	100	EFECTIVO
				¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado?	50			
				¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención?	50			
				¿Existen copias de seguridad de los registros?	50			
NIVEL 3	A.12.4.3	Registros de administración y operación	Control: Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)?	1	1	100	INEXISTENTE
				¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?	1			
NIVEL 3	A.12.4.4	Sincronización del reloj	Control: Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente de tiempo precisa y acordada.	¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión?	1	1	100	INEXISTENTE
				¿Hay un tiempo de referencia definido (ej. Reloj atómicos, GPS o NTP)?	1			
				¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales?	1			
				¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.?	1			
				¿Existe una configuración de respaldo para la referencia de tiempo?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.12.5	Control del software en explotación	Objetivo: Asegurar la integridad del software en explotación.			1	100	INEXISTENTE
NIVEL 3	A.12.5.1	Instalación del software en explotación	Control: Se deben implementar procedimientos para controlar la instalación del software en explotación.	¿Existe una política acerca de la instalación de software?	1	1	100	INEXISTENTE
				¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción?	1			
				¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)?	1			
				¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.?	1			
				¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados?	1			
				¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas?	1			
				¿Existe un control de cambio y aprobación adecuado para la aprobación de software?	1			
NIVEL 2	A.12.6	Gestión de la vulnerabilidad técnica	Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.			1	100	INEXISTENTE
NIVEL 3	A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	¿Existe una política la gestión de vulnerabilidades técnicas?	1	1	100	INEXISTENTE
				¿Se escanean los sistemas para detectar vulnerabilidades de forma automatizada?	1			
				¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes?	1			
				¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC?	1			
				¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo?	1			
				¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución?	1			
				¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? ¿Los procesos para implementar parches urgentes son adecuados?	1			
				¿Se emplea una administración automatizada de parches?	1			
				¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?	1			
NIVEL 3	A.12.6.2	Restricción en la instalación de software	Control: Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados?	1	1	100	INEXISTENTE
				¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos?	1			
				¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.12.7	Consideraciones sobre la auditoria de sistemas de información	Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.			1	100	INEXISTENTE
NIVEL 3	A.12.7.1	Controles de auditoría de sistemas de información	Control: Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	¿Existe una política que requiera auditorias de seguridad de la información?	1	1	100	INEXISTENTE
				¿Existe un programa definido y procedimientos para auditoría?	1			
				¿Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales?	1			
				¿Se define el alcance de la auditoría en coordinación con la administración?	1			
				¿El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado?	1			
NIVEL 1	A.13	Seguridad de las comunicaciones				1	100	INEXISTENTE
NIVEL 2	A.13.1	Gestión de la seguridad de las redes	Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.			1	100	INEXISTENTE
NIVEL 3	A.13.1.1	Controles de red	Control: Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	¿Existen políticas de redes físicas e inalámbricas?	1	1	100	INEXISTENTE
				¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red?	1			
				¿Existe un mecanismo de registro i monitorización de la red y los dispositivos que se conectan ella?	1			
				¿Hay un sistema de autenticación para todos los accesos a la red de la organización?	1			
				¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos?	1			
				¿Los usuarios se autentican adecuadamente al inicio de sesión?	1			
				¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.?	1			
				¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?	1			
NIVEL 3	A.13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada?	1	1	100	INEXISTENTE
				¿Existe un monitoreo de servicios de red?	1			
				¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)?	1			
				¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red?	1			
				¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?	1			
NIVEL 3	A.13.1.3	Segregación en redes	Control: Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.	¿Existe una política de segmentación de red?	1	1	100	INEXISTENTE
				¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)?	1			
				¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados?	1			
				¿Hay controles adecuados entre ellos?	1			
				¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.13.2	Intercambio de información	Objetivo: Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa.			1	100	INEXISTENTE
NIVEL 3	A.13.2.1	Políticas y procedimientos de intercambio de información	Control: Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	¿Existen políticas y procedimientos relacionados con la transmisión segura de información?	1	1	100	INEXISTENTE
				¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.?	1			
				¿Está basado en la clasificación de la información?	1			
				¿Existen controles de acceso adecuados para esos mecanismos?	1			
				¿Se sigue el principio de confidencialidad y privacidad?	1			
				¿Existen un programa de concientización, capacitación y cumplimiento?	1			
NIVEL 3	A.13.2.2	Acuerdos de intercambio de información	Control: Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas?	1	1	100	INEXISTENTE
				¿Se mantiene una cadena de custodia para las transferencias de datos?	1			
NIVEL 3	A.13.2.3	Mensajería electrónica	Control: La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.?	1	1	100	INEXISTENTE
				¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)?	1			
				¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?	1			
NIVEL 3	A.13.2.4	Acuerdos de confidencialidad o no revelación	Control: Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación	¿Existen acuerdos de confidencialidad?	1	1	100	INEXISTENTE
				¿Han sido revisados y aprobados por el Departamento Legal?	1			
				¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)?	1			
				¿Han sido aprobados y firmados por las personas adecuadas?	1			
				¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 1	A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información				1,777777778	100	INICIAL
NIVEL 2	A.14.1	Requisitos de seguridad en los sistemas de información	Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.			3,333333333	100	INICIAL
NIVEL 3	A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Control: Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software?	1	1	100	INEXISTENTE
				¿Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo?	1			
				¿Son estos procedimientos obligatorios para todos los nuevos desarrollos y cambios en los sistemas existentes (ej. Actualizaciones de sistema operativo / aplicaciones en las actualizaciones, cambios de criptografía, etc.)	1			
				¿Se aplican estos controles para sistemas / software comercial, incluidos los productos “a medida” o personalizados?	1			
NIVEL 3	A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Control: La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.	¿La organización usa o proporciona aplicaciones web de comercio electrónico?	50	8	100	INICIAL
				¿Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio?	1			
				¿Contiene controles tales como validación de datos de entrada, validación de procesamiento, encriptación, autenticación de mensajes e irrenunciabilidad?	1			
				¿Se fuerza https?	1			
				¿Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)?	1			
				¿Se analizan y documentan las amenazas de forma rutinaria?	1			
				¿Existe una gestión de incidentes y cambios para tratarlos?	1			
NIVEL 3	A.14.1.3	Protección de las transacciones de servicios de aplicaciones	Control: La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.	¿Las transacciones se realizan y almacenan en un entorno interno seguro o expuesto a internet?	1	1	100	INEXISTENTE
				¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.?	1			
				¿Cumplen con todos los requisitos legales, regulatorios y de cumplimiento?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.14.2	Seguridad en el desarrollo y en los procesos de soporte	Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de lo s sistemas de información.			1	100	INEXISTENTE
NIVEL 3	A.14.2.1	Política de desarrollo seguro	Control: Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	¿Existe una política de desarrollo seguro que abarque la arquitectura de seguridad?	1	1	100	INEXISTENTE
				¿Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios?	1			
				¿Los métodos de desarrollo incluyen pautas de programación segura?	1			
				¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?	1			
NIVEL 3	A.14.2.2	Procedimiento de control de cambios en sistemas	Control: La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.	¿Existen políticas, procedimientos y registros relacionados de la gestión de cambios?	1	1	100	INEXISTENTE
				¿Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión?	1			
				¿Incluye un procedimiento para cambios de emergencia?	1			
				¿Se aplica los cambios significativos en equipos informáticos y de telecomunicaciones?	1			
				¿Los cambios en el sistema están debidamente documentados, justificados y autorizados por la administración?	1			
NIVEL 3	A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Control: Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.	¿Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado?	1	1	100	INEXISTENTE
				¿Hay registros de estas actividades?	1			
NIVEL 3	A.14.2.4	Restricciones a los cambios en los paquetes de software	Control: Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	¿Se hacen cambios a paquetes software adquiridos?	1	1	100	INEXISTENTE
				¿Se verifica que los controles originales no han sido comprometidos?	1			
				¿Se obtuvo el consentimiento y la participación del proveedor?	1			
				¿El proveedor continúa dando soporte tras los cambios?	1			
				¿Se exploró la posibilidad de obtener actualizaciones de programas estándar por parte de los proveedores?	1			
				¿Se hace una comprobación de compatibilidad con otro software en uso?	1			
NIVEL 3	A.14.2.5	Principios de ingeniería de sistemas seguros	Control: Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	¿Se siguen principios de SDLC que incluye controles de seguridad?	1	1	100	INEXISTENTE
				¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 3	A.14.2.6	Entorno de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	¿Se aíslan los entornos de desarrollo?	1	1	100	INEXISTENTE
				¿Quién es responsable de garantizar que el software nuevo / modificado no interrumpa otras operaciones?	1			
				¿Se realizan comprobaciones de antecedentes de los desarrolladores?	1			
				¿Tienen que cumplir con un NDA?	1			
				¿Se protegen los datos de prueba de la divulgación y dónde están almacenados?	1			
NIVEL 3	A.14.2.7	Externalización del desarrollo de software	Control: El desarrollo de software externalizado debe ser supervisado y controlado por la organización.	¿Se tienen en cuenta los siguientes aspectos cuando el desarrollo es lleva a cabo por un tercero? • Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual • Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba • Acceso al código fuente si el código ejecutable necesita ser modificado • Controles de prueba de seguridad de aplicaciones • Evaluación de vulnerabilidad y tratamiento	1	1	100	INEXISTENTE
NIVEL 3	A.14.2.8	Pruebas funcionales de seguridad de sistemas	Control: Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	¿Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados?	1	1	100	INEXISTENTE
				¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual?	1			
NIVEL 3	A.14.2.9	Pruebas de aceptación de sistemas	Control: Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red?	1	1	100	INEXISTENTE
				¿Las pruebas replican situaciones y entornos operativos realistas?	1			
				¿Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado?	1			
				¿Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo?	1			
				¿Se actualizan los controles de resiliencia y recuperación tras incidentes para reflejar los sistemas nuevos, modificados y retirados?	1			
NIVEL 2	A.14.3	Datos de prueba	Objetivo: Asegurar la protección de los datos de prueba			1	100	INEXISTENTE
NIVEL 3	A.14.3.1	Protección de los datos de prueba	Control: Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.	¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.?	1	1	100	INEXISTENTE
				¿Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas?	1			
				¿Existen registros de estas actividades?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 1	A.15	Relación con proveedores				1	100	INEXISTENTE
NIVEL 2	A.15.1	Seguridad en las relaciones con proveedores	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			1	100	INEXISTENTE
NIVEL 3	A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Control: Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.	¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI?	1	1	100	INEXISTENTE
				¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo?	1			
				¿Los contratos y acuerdos abordan lo siguiente? • Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada • Información / propiedad intelectual, y obligaciones / limitaciones derivadas • Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001 • Identificación de controles físicos y lógicos • Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio • Habilitación de seguridad de los empleados y concienciación • Derecho de auditoría de seguridad por parte de la organización	1			
				¿Existe una obligación contractual de cumplimento?	1			
				¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?	1			
NIVEL 3	A.15.1.2	Requisitos de seguridad en contratos con terceros	Control: Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura de Tecnología de la Información.	¿Los contratos o acuerdos formales con proveedores cubren lo siguiente? • Gestión de las relaciones, incluyendo riesgos • Cláusulas de confidencialidad vinculantes • Descripción de la información que se maneja y el método de acceder a dicha información • Estructura de la clasificación de la información a usar • La Inmediata notificación de incidentes de seguridad • Aspectos de continuidad del negocio • Subcontratación y restricciones en las relaciones con otros proveedores • Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, “robo de empleados”, etc.)	1	1	100	INEXISTENTE
NIVEL 3	A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Control: Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	¿Se validan los requisitos de seguridad de los productos o servicios adquiridos?	1	1	100	INEXISTENTE
				¿Se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros?	1			
				¿Se puede rastrear el origen del producto o servicio?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.15.2	Gestión de la provisión de servicios del proveedor	Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores			1	100	INEXISTENTE
NIVEL 3	A.15.2.1	Control y revisión de la provisión de servicios del proveedor	Control: Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor	¿Existe una monitorización de servicios y quien responsable de esta actividad?	1	1	100	INEXISTENTE
				¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia?	1			
				¿Se generan informes y / o métricas relacionadas a las reuniones y las decisiones tomadas?	1			
				¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría?	1			
				¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?	1			
NIVEL 3	A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Control: Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.	¿Se comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados?	1	1	100	INEXISTENTE
				¿Se actualizan los acuerdos relacionados con los cambios?	1			
NIVEL 1	A.16	Gestión de incidentes de seguridad de la información				1	100	INEXISTENTE
NIVEL 2	A.16.1	Gestión de incidentes de seguridad de la información y mejoras	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.			1	100	INEXISTENTE
NIVEL 3	A.16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	¿Existen políticas, procedimientos e ITT´s para la gestión de incidentes?	1	1	100	INEXISTENTE
				¿Qué cubre? • I plan de respuesta a incidentes • Puntos de contacto para la notificación de incidentes, seguimiento y evaluación • Monitoreo, detección y reporte de eventos de seguridad • Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio • Método de recolección de evidencias y pruebas forenses digitales • Revisión post-evento de seguridad y procesos de aprendizaje / mejora	1			
				¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre?	1			
NIVEL 3	A.16.1.2	Notificación de los eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	¿Se informan los eventos de seguridad de la información?	1	1	100	INEXISTENTE
				¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen?	1			
				¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución.	1			
				¿Se crean nuevos controles a partir de los informes de seguimiento ?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 3	A.16.1.3	Notificación de puntos débiles de la seguridad	Control: Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.	¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual?	1	1	100	INEXISTENTE
				¿Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo?	1			
NIVEL 3	A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Control: Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	¿Los empleados informan acerca de eventos relacionados a la seguridad de la información?	1	1	100	INEXISTENTE
				¿Se evalúan estos eventos para decidir si califican como incidentes?	1			
				¿Hay una escala de clasificación?	1			
				¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes graves?	1			
NIVEL 3	A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	¿Se recolecta, almacena y evalúa la evidencia?	1	1	100	INEXISTENTE
				¿Hay una matriz de escalación para usar según sea necesario?	1			
				¿Hay medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes?	1			
				¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?	1			
NIVEL 3	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Control: El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.	¿Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes?	1	1	100	INEXISTENTE
				¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias?	1			
				Además, ¿Se está utilizado para formación y concienciación?	1			
				¿La organización cuenta con un proceso de gestión de incidentes relativamente maduro?	1			
				¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?	1			
NIVEL 3	A.16.1.7	Recopilación de evidencias	Control: La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia.	¿La recolección de evidencias se hace de forma competente en la empresa o por terceros especializados y capacitados en esta área?	1	1	100	INEXISTENTE
				¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el rol?	1			
				¿Existen obligaciones relacionadas con la jurisdicción, las diferentes normas forenses y los requisitos legales asociados?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 1	A.17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio				9,166666667	100	INICIAL
NIVEL 2	A.17.1	Continuidad de la seguridad de la información	Objetivo: La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización.			1	100	INEXISTENTE
NIVEL 3	A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	¿Se encuentran establecidos los requisitos de continuidad del negocio?	1	1	100	INEXISTENTE
				¿Existe un plan de continuidad de negocio?	1			
				¿Existen un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos?	1			
				¿Se identifica el impacto potencial de los incidentes?	1			
				¿Se evalúan los planes de continuidad del negocio?	1			
				¿Se llevan a cabo ensayos de continuidad?	1			
NIVEL 3	A.17.1.2	Implementar la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa	¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción?	1	1	100	INEXISTENTE
				¿Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares?	1			
				¿La planificación de la continuidad es consistente e identifica las prioridades de restauración?	1			
				¿Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades?	1			
				¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos?	1			
NIVEL 3	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	¿Existe un método de pruebas del plan de continuidad?	1	1	100	INEXISTENTE
				¿Con qué frecuencia se llevan a cabo dichas pruebas?	1			
				¿Hay evidencia de las pruebas reales y sus resultados?	1			
				¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

NIVEL 2	A.17.2	Redundancias.	Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.			17,33333333	100	INICIAL
NIVEL 3	A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Control: Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga?	1	17,33333333	100	INICIAL
				¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí?	50			
				¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?	1			
NIVEL 1	A.18	Cumplimiento				4,43	100	INICIAL
NIVEL 2	A.18.1	Cumplimiento de los requisitos legales y contractuales	Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.			7,86	100	INICIAL
NIVEL 3	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.	¿Existe una política acerca del cumplimiento de requisitos legales? LOPD, GDPR, etc.	1	25,5	100	REPETIBLE
				¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables?	50			
				¿Hay una persona encargada de mantener, usar y controlar el registro?	50			
				¿Existen controles adecuados para cumplir con los requisitos?	1			
NIVEL 3	A.18.1.2	Derechos de Propiedad Intelectual (DPI)	Control: Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales	¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?	1	1	100	INEXISTENTE
NIVEL 3	A.18.1.3	Protección de los registros de la organización	Control: Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.	¿Existe una política que contemple lo siguiente? Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos.	1	10,8	100	INICIAL
				¿Se almacenan las firmas digitales de forma segura?	50			
				¿Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado?	1			
				¿Se verifica periódicamente la integridad de los registros?	1			
				¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo?	1			
NIVEL 3	A.18.1.4	Protección y privacidad de la información de carácter personal	Control: Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	¿Hay un mecanismo para instruir al personal en el manejo de información de carácter personal?	1	1	100	INEXISTENTE
				¿Hay un responsable de privacidad en la organización?	1			
				¿Es el responsable conocedor de la información de carácter personal que es recopilado, procesado y almacenados por la organización?	1			
NIVEL 3	A.18.1.5	Regulación de los controles criptográficos	Control: Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	¿Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico?	1	1	100	INEXISTENTE
				¿Estas actividades cumplen con los requisitos legales y reglamentarios?	1			

Adaptado de (Ministerio de Industria c. y., 2017)

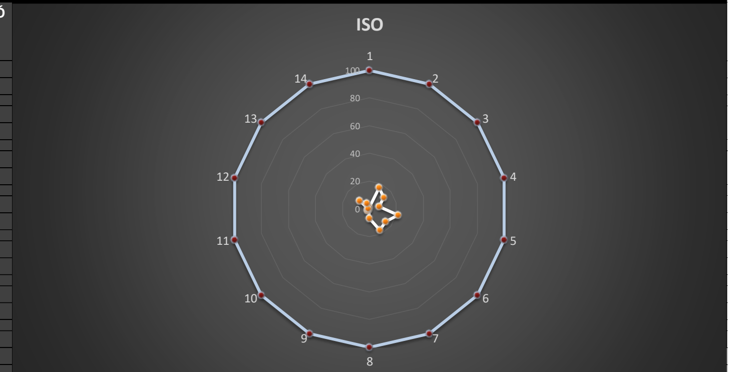
NIVEL 2	A.18.2	Revisiones de la seguridad de la información	Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.			1	100	INEXISTENTE
NIVEL 3	A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información?	1	1	100	INEXISTENTE
				¿Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos?	1			
				¿Están los objetivos y el alcance de auditoria autorizados por la gerencia?	1			
				¿Está adecuadamente controlado el acceso a las herramientas / software de auditoría del sistema de información?	1			
				¿Se documentan los hallazgos de auditoría y las actuaciones para solventarlos?	1			
NIVEL 3	A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Control: Los directivos deben asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable	¿Se garantizar que todos los procedimientos de seguridad dentro de un área de responsabilidad se llevan a cabo correctamente?	1	1	100	INEXISTENTE
				¿Se hace una verificación periódica?	1			
NIVEL 3	A.18.2.3	Comprobación del cumplimiento técnico	Control: Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares?	1	1	100	INEXISTENTE
				¿Las pruebas son realizadas por profesionales debidamente cualificados, competentes y confiables?	1			
				¿Se informa, analiza y utilizan los resultados de dichas pruebas?	1			
				¿La prioridad de tratamiento se basa en un análisis de riesgos?	1			
				¿Hay evidencias de medidas tomadas para abordar los problemas identificados?	1			

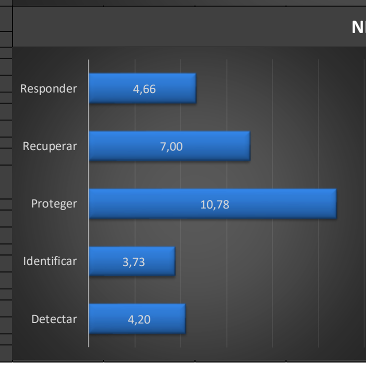
Adaptado de (Ministerio de Industria c. y., 2017)

ANEXO 2 DASHBOARD EVALUACION DIAGNOSTICO ISO /NIST

EVALUACION DIAGNOSTICO ISO / NIST

N	DOMINIO	PONDERACIÓN ACTUAL	OBJETIVO	CALIFICACIÓN DE DOMINIO
1	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	1,00	100,00	INEXISTENTE
	* Falta de Directrices de gestión de la seguridad de la información			
2	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	16,76	100,00	INICIAL
	* No se cuenta con un marco de gestión para controlar la operación del SGSI dentro de la organización.			
3	SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	13,25	100,00	INICIAL
	* Los empleados no conocen o no cumplen con sus responsabilidades en seguridad de la información.			
4	GESTIÓN DE ACTIVOS	7,13	100,00	INICIAL
	* Activos de información no identificados, falta de un nivel adecuado de protección.			
5	CONTROL DE ACCESO	18,98	100,00	INICIAL
	* Los controles de acceso a la información critica de la organización no de encuentran delimitados			
6	CRIPTOGRAFÍA	15,14	100,00	INICIAL
	* No se cuenta con controles de cifrado de la información critica de la organización.			
7	SEGURIDAD FÍSICA Y DEL ENTORNO	17,05	100,00	INICIAL
	* No se encuentran definidas perímetros de seguridad para las áreas que contienen activos de información críticos			
8	SEGURIDAD DE LAS OPERACIONES	7,16	100,00	INICIAL
	* Falta de registro de incidentes materializados, se debe controlar los cambios en el tratamiento de la información			
9	SEGURIDAD DE LAS COMUNICACIONES	1,00	100,00	INEXISTENTE
	* No se cuenta con protección de redes y recursos para el tratamiento de la información			
10	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	1,78	100,00	INICIAL
	* No se cuenta con licencias para cada software de la organización			
11	RELACIÓN CON PROVEEDORES	1,00	100,00	INEXISTENTE
	* No se encuentra documentados los riesgos asociados con el acceso a los activos de la organización por parte de los proveedores			
12	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	1,00	100,00	INEXISTENTE
	* No se cuentan con procedimientos para la gestión de incidentes			
13	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	9,17	100,00	INICIAL
	* El enfoque de continuidad del negocio no es el adecuado para el programa de SGSI			
14	CUMPLIMIENTO	4,43	100,00	INICIAL
	* Falta de análisis y aplicación de la normativa legal vigente.			
	Total general	8,20		





Responder	Capacidad de contener el impacto de un posible incidente de seguridad cibernética
Recuperar	Desarrollo e implementación de actividades apropiadas para mantener los planes de resiliencia y restablecer un servicio debido a un incidente de seguridad cibernética.
Proteger	Desarrollo e implementación de medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.
Identificar	Comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades.
Detectar	Desarrollo e implementación de actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética.

Adaptado de (Ministerio de Industria c. y., 2017) (Technology, 2018)

ANEXO 3 ACCIONES DE MEJORA DE LA EVALUACION DE DIAGNOSTICO

ACCIONES DE MEJORA		
Controles & Objetivos		**Acciones**
Políticas de seguridad de la información		Proporcionar orientación y apoyo al programa de SGSI a través de
	1	Elaboración de Política se SGSI que evidencia una estructura y jerarquía de administración de los activos de información críticos cubriendo riesgos y controles relevantes según la norma ISO
Organización de la seguridad de la información		Establecer un marco de gestión que permita administrar el programa de SGSI mediante
	1	Obtención del apoyo de la gerencia
	2	Elaboración de una política que permita definir roles y responsabilidades asignados de acuerdo con las capacidades y competencia del personal a través de una matriz RACI
	3	Definir un presupuesto para el SGSI
	4	Identificación de riesgos de la información y sus requisitos de seguridad a través de una política
Seguridad relativa a los recursos humanos		Asegurarse que los empleados entiendan sus obligaciones y responsabilidades según:
	1	Distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, etc.
	2	Evaluaciones que permitan identificar el entendimiento de las normas y políticas internas con realización al programa de SGSI
	3	Implementación de planes de concientización sobre la seguridad de la información que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos
	4	Definición de un proceso correctivo para incidentes de seguridad de la información
Gestión de activos		Identificar los activos de la organización tomando en cuenta lo siguiente
	1	Elaboración de un esquema estructurado para la identificación y clasificación de activos de información que no solo contenga la información de clientes sino un propietario del manejo de la información basado en la confidencialidad, integridad y disponibilidad
	2	Creación de una política del sobre el uso aceptable de los recursos tecnológicos.
	3	Definición de controles y procedimientos para el almacenamiento de la información respecto de la confidencialidad
	4	Borrado seguro
Control de acceso		Limitar el acceso a los recursos de tratamiento de la información y a la información a través de:
	1	Elaboración de política de control de acceso el cual deberá contener
		Segregación de documentación de aprobación de acceso, control y supervisión, sistemas de autenticación y evaluación del sistema de control de acceso
	2	Definición de atributos por usuario de acuerdo con las necesidades de cada área
	3	Implementar controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores.
Criptografía		Definir un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y /o integridad de la información mediante:
	1	Elaboración de política de controles criptográficos
	2	Verificación de cumplimiento
Seguridad física y del entorno		Prevenir el acceso físico no autorizado y mantenimiento de instalaciones utilizando
	1	Perímetros de seguridad
	2	Instalación de cámaras que permitan detección de intrusos
	3	Uso de sistemas biométricos o tarjetas de proximidad
	4	Registro de accesos
	5	Implementación de procedimiento de recuperación
	6	Verificación del sistema UPS así como su mantenimiento
	7	Uso de personal calificado para realizar mantenimiento de equipos e infraestructura
	8	Políticas de zona de trabajo limpia
Seguridad de las operaciones		Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información. Mediante:
	1	Procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.
	2	Política de gestión y control de cambios que evalúe riesgos potenciales
	3	Controles antimalware y controles de antivirus de "escaneado en acceso" y "escaneo programático" en todos los dispositivos.
	4	Adquisición de licencias de antivirus
	5	Política y procedimiento de copia de seguridad
	6	Monitoreo de eventos como permisos y controles de acceso o instalación de software
	7	Escaneo de los sistemas para detectar vulnerabilidades de forma automatizada
	8	Procedimientos para auditoria de sistemas
Seguridad de las comunicaciones		Asegurar la protección de la transmisión de la información a través de
	1	Elaboración de una política para control mantenimiento y supervisión del uso de las redes inalámbricas
	2	Implementación de sistemas de autenticación para los accesos a la red de la organización
	3	Monitoreo de los servicios de red
	4	Revisión periódica de Firewall
	5	Elaboración de procedimientos de transmisión segura de información manteniendo el principio de confidencialidad y privacidad
	6	Elaboración y revisión de acuerdos de confidencialidad por parte del departamento legal
Adquisición, desarrollo y mantenimiento de los sistemas de información		Garantizar que la seguridad de la información sea parte integral de los sistemas de información utilizando:
	1	Políticas, procedimientos para la adquisición de sistemas y software
	2	Procedimientos para analizar riesgos y requisitos funcionales y técnicos en la adquisición de sistemas y software
	3	Leyes vigentes
	4	Elaboración de controles de resiliencia y recuperación
Relación con proveedores		Asegurar la protección de los activos de la organización mediante
	1	Elaboración de políticas relacionados con la gestión de proveedores que involucran servicios de TI
	2	Monitorización e informes de los servicios recibidos
Gestión de incidentes de seguridad de la información		Asegurar un enfoque eficaz para la gestión de incidentes de seguridad de la información que incluya
	1	Políticas y procedimientos para la gestión de incidentes
	2	Verificación contractual acerca de la notificación de incidentes y prohibición de verificar, validar o explotar vulnerabilidades del software y hardware de la organización.
Aspectos de seguridad de la información para la gestión de la continuidad de negocio		Integrar la seguridad de la información a los sistemas de gestión de la continuidad de negocio de la organización mediante
	1	Elaboración de un plan de continuidad de negocio que identifique impacto, plazos de restauración del servicio, acuerdos de responsabilidad y procedimientos de recuperación
	2	Evaluación de servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí
Cumplimiento		Evitar incumplimientos de las obligaciones legales relativas a la seguridad de la información tomando en cuenta
	1	Ley Orgánica de Tratamiento de Datos Personales
	2	Manteniendo un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables
	3	Definición de encargado y responsable del cumplimiento de la Ley Orgánica de Protección de Datos Personales
	4	Procedimientos relativos a la adquisición y gestión de licencias
	5	Escaneos de vulnerabilidades de red y pruebas de Pentesting

Adaptado de (Ministerio de Industria c. y., 2017)

ANEXO 4 EVALUACION DE TIPOS DE INFORMACION

A1			TIPOS DE INFORMACION																
Sujetos o Entidades de Información	Tipo de información	Definición	Criterios de Seguridad de la Información																Calificación Impacto
			Privacidad				Integridad				Disponibilidad				Confidencialidad				
			Pérdidas financieras	Interrupción de operaciones	Degradación Imagen instituc	Pérdidas / Destrucción / P	Pérdidas financieras	Interrupción de operaciones	Degradación Imagen instituc	Pérdidas / Destrucción / P	Pérdidas financieras	Interrupción de operaciones	Degradación Imagen instituc	Pérdidas / Destrucción / P	Pérdidas financieras	Interrupción de operaciones	Degradación Imagen instituc	Pérdidas / Destrucción / P	
Clientes	Identificación	Información que permita identificar al cliente, información tomada de CI o pasaporte																	
	Ubicabilidad	teléfono, correo electrónico, redes sociales.																	
	Bancaria	Información que permita conocer su comportamiento dentro del sistema bancario																	
	Financiera	Información que permita conocer activos, pasivos, patrimonio, ingresos y gastos, nivel de endeudamiento																	
	Laboral	Información que permita conocer su actual situación laboral así como su histórico																	
	TJ	Información que permita el debito de pagos por adquisición de productos																	
	Medica	Información que permita conocer el estado de salud del cliente																	
	Legal	Información que permita conocer la situación legal, juicios demandas personificación jurídica, tributos etc.																	
	Educación	Información que permita conocer el nivel educativo del cliente																	
	Hábitos y Hobbies	Información que permita conocer su el tratamiento de riesgo de acuerdo al nivel de exposición de riesgo																	
Prospecto	Identificación	Información que permita identificar al cliente, información tomada de CI o pasaporte																	
	Ubicabilidad	Información que permita ubicar o contactar al cliente																	
	Financiera	Información que permita conocer activos, pasivos, patrimonio, ingresos y gastos, nivel de endeudamiento																	
	Medica	Información que permita conocer el estado de salud del cliente																	
	Legal	Información que permita conocer la situación legal, juicios demandas personificación jurídica, tributos etc.																	
	Hábitos y Hobbies	Información que permita conocer su el tratamiento de riesgo de acuerdo al nivel de exposición de riesgo																	
Empleados	Identificación	Información que permita identificar al cliente, información tomada de CI o pasaporte																	
	Personal	Información que permita conocer, orientación sexual, raza/etnia, tendencias políticas, cargas familiares																	
	Ubicabilidad	Información que permita ubicar o contactar al cliente																	
	Bancaria	Información que permita conocer su comportamiento dentro del sistema bancario																	
	Financiera	Información que permita conocer activos, pasivos, patrimonio, ingresos y gastos, nivel de endeudamiento																	
	Laboral	Información que permita conocer su actual situación laboral así como su histórico																	
	Medica	Información que permita conocer el estado de salud del empleado																	
	Legal	Información que permita conocer la situación legal, demandas, juicios, personificación jurídica, tributos etc.																	
	Educación	Información que permita conocer el nivel educativo del empleado																	
	Ingresos	Información correspondiente a nivel de ingresos dentro la organización																	
Proveedores	Catálogo Productos &	comercializarse - Estándares de Calidad.																	
	Ubicabilidad	Información que permita conocer la dirección de oficinas y sucursales - Teléfono, fax, correo electrónico - Redes sociales, Market Place, Whatsapp Bussiness, etc.																	
	Tributaria	Contribuyente "Activo - Suspendido" - Razón Social - Nombre de Rep																	
	Legal	Información legal como: formulario Conozca a su Proveedor - Nombramientos de Rep. Legales - Constitución de la organización - Información de obligaciones del proveedor SRI-IESS-SUPER CIAS - Convenios de Confidencialidad - Referencias Comerciales - Estados Financieros.																	
	Bancaria	del Banco - Estado de la cuenta "Activa - Suspendida" - Código Swift.																	
Organización	Procesos																		
	Financiera	y gastos, nivel de endeudamiento																	
	Catálogo Productos & Precios	Información que permita conocer el portafolio de Bienes o servicios a comercializarse.																	
	Estratégica																		

ANEXO 5 ACTIVOS DE INFORMACION

Identificador	Nombre del Activo	Características del Activo					Identificación del Activo de Información	Formato	Procesos	Responsable	Tipo de Información	Criterio				Criticidad	Ubicación del Activo
		Genera	Crea	Transmite	Comparte	Almacena						P	I	D	C		
ACIF_0001	Computador Portátil Gerente Comercial	X	X	X	X	X	Carpeta Clientes Actuales	Archivos de Imagen - Archivo de Excel	Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Identificación de Clientes						Oficina Gerente Comercial
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Ubicabilidad de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Bancaria de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Financiera de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Laboral de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información TJ de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Medica de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Legal de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Educación de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Hábitos y Hobbies de Clientes						
							Carpeta Seguros Actual	Medio electrónico	Colocación de nuevos productos	Gerente Comercial	Información Catálogo Productos & Precios de Organización						
							Carpeta Seguros Actual	Medio electrónico	Colocación de nuevos productos / Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Catálogo Productos & Precios de Proveedores						
ACIF_0002	Computador Portátil Gerente General	X	X	X	X	X	Carpeta Seguros Actual	Medio electrónico	Colocación de nuevos productos	Gerente General	Información Ubicabilidad de Proveedores						Oficina Gerente General
							Carpeta Seguros Actual	Medio electrónico	Colocación de nuevos productos	Gerente General	Información Procesos de Organización						
							Desconocido		Administración General	Gerente General	Información Estratégica de Organización						
ACIF_0003	Computador Portátil Gerente Administrativo	X	X	X	X	X	Carpeta Empleados 2020 Actual	Medio electrónico	Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Identificación de Empleados						Oficina Gerente Administrativo
									Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Personal de Empleados						
									Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Ubicabilidad de Empleados						
									Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Bancaria de Empleados						
									Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Financiera de Empleados						
									Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Laboral de Empleados						
									Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Medica de Empleados						
									Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Legal de Empleados						
									Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Educación de Empleados						
									Contrataciones / Renovaciones / Liquidación del Personal / Nómina Outsourcing	Gerente Administrativo	Información Ingresos de Empleados						
ACIF_0004	Computador de Escritorio Supervisor	X	X	X	X	X	Carpeta Clientes Actuales	Archivos de Imagen - Archivo de Excel	Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Identificación de Clientes						Departamento de Afiliaciones
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Ubicabilidad de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Bancaria de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Financiera de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Laboral de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información TJ de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Medica de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Legal de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Educación de Clientes						
									Afiliación Inicial / Renovación / Siniestros	Gerente Comercial	Información Hábitos y Hobbies de Clientes						

ACIF_0005 ACIF_0006 ACIF_0007 ACIF_0008 ACIF_0009	Computador de Escritorio Equipo Operativo	X	X	X	X	X	Carpeta Prospectos	Digital - Archivo de Excel	Cotizaciones	Supervisor de Ventas	Información Identificación de Prospecto	Departamento de Afiliaciones
									Cotizaciones	Supervisor de Ventas	Información Ubicabilidad de Prospecto	
									Cotizaciones	Supervisor de Ventas	Información Financiera de Prospecto	
									Cotizaciones	Supervisor de Ventas	Información Medica de Prospecto	
									Cotizaciones	Supervisor de Ventas	Información Legal de Prospecto	
									Cotizaciones	Supervisor de Ventas	Información Hábitos y Hobbies de Prospecto	
							Carpeta Clientes Diarios	Archivos de Imagen - Archivo de Excel	Afiliación Inicial	Operador	Información Identificación de Clientes	
									Afiliación Inicial	Operador	Información Ubicabilidad de Clientes	
									Afiliación Inicial	Operador	Información Bancaria de Clientes	
									Afiliación Inicial	Operador	Información Financiera de Clientes	
									Afiliación Inicial	Operador	Información Laboral de Clientes	
									Afiliación Inicial	Operador	Información TJ de Clientes	
									Afiliación Inicial	Operador	Información Medica de Clientes	
									Afiliación Inicial	Operador	Información Legal de Clientes	
									Afiliación Inicial	Operador	Información Educación de Clientes	
									Afiliación Inicial	Operador	Información Hábitos y Hobbies de Clientes	
ACIF_0010	Celular Gerente Comercial			X	X	X	Carpeta Descargas	Archivos de Imagen - Archivo de Excel Texto Whatsapp	Afiliación Inicial / Siniestros	Gerente Comercial	Información Identificación de Clientes	Oficina Gerente Comercial
									Afiliación Inicial / Siniestros	Gerente Comercial	Información Ubicabilidad de Clientes	
									Afiliación Inicial / Siniestros	Gerente Comercial	Información Bancaria de Clientes	
									Afiliación Inicial / Siniestros	Gerente Comercial	Información Financiera de Clientes	
									Afiliación Inicial / Siniestros	Gerente Comercial	Información Laboral de Clientes	
									Afiliación Inicial / Siniestros	Gerente Comercial	Información TJ de Clientes	
									Afiliación Inicial / Siniestros	Gerente Comercial	Información Medica de Clientes	
									Afiliación Inicial / Siniestros	Gerente Comercial	Información Legal de Clientes	
									Afiliación Inicial / Siniestros	Gerente Comercial	Información Educación de Clientes	
									Afiliación Inicial / Siniestros	Gerente Comercial	Información Hábitos y Hobbies de Clientes	
ACIF_0011	Cloud Personal One Drive			X		X	Carpeta Clientes Actuales	Archivos de Imagen - Archivo de Excel	Respaldo & Back Up	Gerente Comercial	Información Identificación de Clientes	Cloud
									Respaldo & Back Up	Gerente Comercial	Información Ubicabilidad de Clientes	
									Respaldo & Back Up	Gerente Comercial	Información Bancaria de Clientes	
									Respaldo & Back Up	Gerente Comercial	Información Financiera de Clientes	
									Respaldo & Back Up	Gerente Comercial	Información Laboral de Clientes	
									Respaldo & Back Up	Gerente Comercial	Información TJ de Clientes	
									Respaldo & Back Up	Gerente Comercial	Información Medica de Clientes	
									Respaldo & Back Up	Gerente Comercial	Información Legal de Clientes	
									Respaldo & Back Up	Gerente Comercial	Información Educación de Clientes	
									Respaldo & Back Up	Gerente Comercial	Información Hábitos y Hobbies de Clientes	
ACIF_0012	Equipos Exteriores	X	X	X	X	X	Desconocido		Formulario conozca a su proveedor / Registro de facturas / Emisión de Comprobantes de Retención	Contador General / Outsourcing	Información Tributaria de Proveedores	Equipo informático Contador
							Desconocido		Formulario conozca a su proveedor	Contador General / Outsourcing	Información Legal de Proveedores	
							Desconocido		Pago a proveedores	Contador General / Outsourcing	Información Bancaria de Proveedores	
							Carpeta Datos Financiero Seguros ABC	Medio electrónico	Administración General	Contador General / Outsourcing	Información Financiera de Organización	

ANEXO 6 IDENTIFICACION DE AMENAZAS Y VULNERABILIDADES

Identificar posibles amenazas			Identificar posibles vulnerabilidades			Identificar vulnerabilidades reales
Fuente	**Descripción**	**Subtipo de Amenaza**	**Tipo**	**Ejemplo**	**Ejemplo de**	
Margerit	[N] Desastres naturales	[N.*] Desastres naturales	Hardware	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos	
	[I] De origen industrial	[I.1] Fuego	Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de me	x
		[I.2] Daños por agua	Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de me	x
		[I.*] Desastres industriales	Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de me	x
		[I.4] Contaminación electromagnética	Hardware	Sensibilidad a la radiación electromagnética	Radiación electromagnética	
		[I.5] Avería de origen físico o lógico	Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mant	x
		[I.6] Corte del suministro eléctrico	Hardware	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energi	x
			Lugar	Red energética inestable	Pérdida del suministro de energi	x
		[I.7] Condiciones inadecuadas de temperatura o humedad	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento	
		[I.11] Emanaciones electromagnéticas	Hardware	Sensibilidad a la radiación electromagnética	Radiación electromagnética	
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	Hardware	Ausencia de un eficiente control de cambios en la	Error en el uso	x
			Software	Interfaz de usuario compleja	Error en el uso	
			Software	Ausencia de documentación	Error en el uso	
			Software	Configuración incorrecta de parámetros	Error en el uso	x
			Software	Fechas incorrectas	Error en el uso	
			Personal	Entrenamiento insuficiente en seguridad	Error en el uso	x
			Personal	Uso incorrecto de software y hardware	Error en el uso	x
			Personal	Falta de conciencia acerca de la seguridad	Error en el uso	x
			Organización	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso	x
			Organización	Ausencia de procedimientos para la introducción del	Error en el uso	x
			Organización	Ausencia de registros en las bitácoras (logs) de	Error en el uso	
			Organización	Ausencia de procedimientos para el manejo de información	Error en el uso	x
			Organización	Ausencia de responsabilidades en la seguridad de la	Error en el uso	x
		[E.2] Errores del administrador	Organización	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos	
			Organización	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso	
		[E.23] Errores de mantenimiento / actualización de equipos (ha	Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mant	x
		[E.24] Caída del sistema por agotamiento de recursos	Software	Configuración incorrecta de parámetros	Error en el uso	x
			Personal	Uso incorrecto de software y hardware	Error en el uso	x
		[E.25] Pérdida de equipos	Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mant	x

Identificar posibles amenazas			Identificar posibles vulnerabilidades			Identificar vulnerabilidades reales
Fuente	Descripción	Subtipo de Amenaza	Tipo	Ejemplo	Ejemplo de amenazas	
Margerit	[A] Ataques intencionados	[A.6] Abuso de privilegios de acceso	Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos	
			Software	Defectos bien conocidos en el software	Abuso de los derechos	x
			Software	Ausencia de "terminación de la sesión" cuando se abandona	Abuso de los derechos	
			Software	Disposición o reutilización de los medios de	Abuso de los derechos	
			Software	Ausencia de pistas de auditoria	Abuso de los derechos	
			Software	Asignación errada de los derechos de acceso	Abuso de los derechos	x
			Organización	Ausencia de procedimiento formal para el registro y	Abuso de los derechos	
			Organización	Ausencia de proceso formal para la revisión	Abuso de los derechos	x
			Organización	Ausencia o insuficiencia de disposiciones (con respecto a la	Abuso de los derechos	x
			Organización	Ausencia de procedimiento de monitoreo de los recursos de	Abuso de los derechos	x
			Organización	Ausencia de auditorías (supervisiones)	Abuso de los derechos	
			Organización	Ausencia de procedimientos de identificación y valoración de	Abuso de los derechos	x
			Organización	Ausencia de reportes de fallas en los registros de	Abuso de los derechos	
		[A.7] Uso no previsto	Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos	
			Software	Defectos bien conocidos en el software	Abuso de los derechos	x
			Software	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	
			Software	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos	
			Software	Ausencia de pistas de auditoria	Abuso de los derechos	
			Software	Asignación errada de los derechos de acceso	Abuso de los derechos	x
			Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos	
			Organización	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	x
			Organización	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos	x
			Organización	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos	x
			Organización	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos	
			Organización	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos	x
			Organización	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos	
		[A.11] Acceso no autorizado	Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos	
			Software	Defectos bien conocidos en el software	Abuso de los derechos	x
			Software	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	
			Software	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos	
			Software	Ausencia de pistas de auditoria	Abuso de los derechos	
			Software	Asignación errada de los derechos de acceso	Abuso de los derechos	x
			Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos	
			Organización	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	x
			Organización	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos	x
			Organización	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos	x
			Organización	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos	
			Organización	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos	x
			Organización	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos	

Identificar posibles amenazas			Identificar posibles vulnerabilidades			Identificar vulnerabilidades reales
Fuente	Descripción	Subtipo de Amenaza	Tipo	Ejemplo	Ejemplo de amenazas	
Margerit	[A] Ataques intencionados	[A.23] Manipulación de los equipos	Hardware	Ausencia de un eficiente control de cambios en la configuración	Error en el uso	x
			Software	Interfaz de usuario compleja	Error en el uso	
			Software	Ausencia de documentación	Error en el uso	
			Software	Configuración incorrecta de parámetros	Error en el uso	x
			Software	Fechas incorrectas	Error en el uso	
			Personal	Entrenamiento insuficiente en seguridad	Error en el uso	x
			Personal	Uso incorrecto de software y hardware	Error en el uso	x
			Personal	Falta de conciencia acerca de la seguridad	Error en el uso	x
			Organización	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso	x
			Organización	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso	x
			Organización	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso	
			Organización	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso	x
			Organización	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso	x
		[A.24] Denegación de servicio	Organización	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información	
			Organización	Ausencia de procedimiento de control de cambios	Incumplimiento en el mant	x
		[A.25] Robo	Hardware	Almacenamiento sin protección	Hurto de medios o documentos	x
			Hardware	Falta de cuidado en la disposición final	Hurto de medios o documentos	
			Hardware	Copia no controlada	Hurto de medios o documentos	
			Software	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos	
			Personal	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos	
			Lugar	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo	x
			Organización	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo	x
			Organización	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo	x
			Organización	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo	x
			Organización	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos	x
			Organización	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos	x
			Organización	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos	x
		[A.26] Ataque destructivo	Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de me	x

Identificar posibles amenazas			Identificar posibles vulnerabilidades			Identificar vulnerabilidades reales
Fuente	**Descripción**	**Subtipo de Amenaza**	**Tipo**	**Ejemplo**	**Ejemplo de amenazas**	
ANEXO C ISO 27005	Compromiso de la información	Hurto de medios o documentos	Hardware	Almacenamiento sin protección	Hurto de medios o documentos	x
			Hardware	Falta de cuidado en la disposición final	Hurto de medios o documentos	
			Hardware	Copia no controlada	Hurto de medios o documentos	
			Software	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos	
			Personal	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos	
			Organización	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos	x
			Organización	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos	x
			Organización	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos	x
		Hurto de equipo	Lugar	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo	x
			Organización	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo	x
			Organización	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo	x
			Organización	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo	x
		Divulgación	Hardware	Almacenamiento sin protección	Hurto de medios o documentos	x
			Software	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos	
			Red	Líneas de comunicación sin protección	Escucha encubierta	x
			Red	Tráfico sensible sin protección	Escucha encubierta	
		Manipulación con hardware	Software	Falla en la producción de informes de gestión	Uso no autorizado del equipo	
			Red	Conexiones de red pública sin protección	Uso no autorizado del equipo	x
			Personal	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	
			Organización	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo	x
			Organización	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo	
		Manipulación con software	Software	Descarga y uso no controlados de software	Manipulación con software	x
			Software	Ausencia de copias de respaldo	Manipulación con software	x
	Eventos naturales	Fenómenos meteorológicos	Hardware	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos	
	Pérdida de los servicios esenciales	Pérdida de suministro de energía	Hardware	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energi	x
			Lugar	Red energética inestable	Pérdida del suministro de energi	x

Identificar posibles amenazas			Identificar posibles vulnerabilidades			Identificar vulnerabilidades reales
Fuente	**Descripción**	**Subtipo de Amenaza**	**Tipo**	**Ejemplo**	**Ejemplo de amenazas**	
ANEXO C ISO 27005	Compromiso de las funciones	Error en el uso	Hardware	Ausencia de un eficiente control de cambios en la configuración	Error en el uso	x
			Software	Interfaz de usuario compleja	Error en el uso	
			Software	Ausencia de documentación	Error en el uso	
			Software	Configuración incorrecta de parámetros	Error en el uso	x
			Software	Fechas incorrectas	Error en el uso	
			Personal	Entrenamiento insuficiente en seguridad	Error en el uso	x
			Personal	Uso incorrecto de software y hardware	Error en el uso	x
			Personal	Falta de conciencia acerca de la seguridad	Error en el uso	x
			Organización	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso	x
			Organización	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso	x
			Organización	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso	
			Organización	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso	x
			Organización	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso	x
	Perturbación debida a la radiación	Radiación electromagnética	Hardware	Sensibilidad a la radiación electromagnética	Radiación electromagnética	
	Daño físico	Fuego	Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de me	x
		Daño por agua	Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de me	x
		Contaminación	Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de me	x
		Accidente importante	Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de me	x
		Destrucción del equipo o los medios	Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de me	x
			Personal	Procedimientos inadecuados de contratación	Destrucción de equipos o de medios.	
			Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipos o de me	x
		Polvo, corrosión, congelamiento	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento	
	Fallas técnicas	Falla del equipo	Organización	Ausencia de planes de continuidad	Falla del equipo	x
		Mal funcionamiento del equipo	Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mante	x
		Saturación del sistema de información	Red	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de inform	x
		Mal funcionamiento del software	Software	Software nuevo o inmaduro	Mal funcionamiento del software	
			Software	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	
			Software	Ausencia de control de cambios eficaz	Mal funcionamiento del software	x
		Incumplimiento en el mantenimiento del sistema de información	Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mante	x
			Organización	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mante	x
			Organización	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información	
			Organización	Ausencia de procedimiento de control de cambios	Incumplimiento en el mante	x

ANEXO 7 ANALISIS DE RIESGO

Vulnerabilidades reales		Riesgo inherente			Controles existentes	Planes de Acción
Tipo	Ejemplo	Riesgo	Probabilida	x Impacto		
Hardware	Ausencia de esquemas de reemplazo periódico.	ALTO	POCO PROBABLE	MAYOR	No se cuenta con planes de reemplazo de equipos, tampoco se cuenta con seguro de propiedad planta y equipo	Contratar seguro para hardware de la organización
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	ALTO	POSIBLE	MAYOR	El mantenimiento del equipos tecnológicos lo realiza personal externo de la organización que no conoce a fondo la criticidad de la información que maneja la empresa	Contratación formal de un servicio de outsourcing para el mantenimiento preventivo y correctivo de todos los equipos informáticos
Hardware	Susceptibilidad a las variaciones de voltaje	MODERADO	RARO	MAYOR	Se cuenta con reguladores de voltaje	Contratación formal de un servicio de outsourcing para el mantenimiento preventivo y correctivo de todos los equipos informáticos
Hardware	Ausencia de un eficiente control de cambios en la configuración	ALTO	POSIBLE	MAYOR	Ausencia de procedimiento de control de cambios	Elaboración e implementación de un procedimiento de control de cambios
Hardware	Almacenamiento sin protección	CRÍTICO	PROBABLE	MAYOR	No se cuenta con controles	Revisión de soportes de almacenamiento
Lugar	Red energética inestable	MODERADO	RARO	MAYOR	Se cuenta con reguladores de voltaje	Contratación formal de un servicio de outsourcing para el mantenimiento preventivo y correctivo de todos los equipos informáticos
Lugar	Ausencia de protección física de la edificación, puertas y ventanas	ALTO	POSIBLE	MAYOR	Se cuenta únicamente con cámaras de seguridad, no existe un monitoreo constante de evaluación de riesgos	Elaboración e implementación MANUAL DE PROCEDIMIENTOS PARA EL USO DE CÁMARAS DE SEGURIDAD Y VIGILANCIA
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	ALTO	POSIBLE	MAYOR	Se cuenta con control biométrico para inicio de actividades pero no para acceso a las instalaciones	Integración del sistema biométrico por huella dactilar para el inicio de sesión de los colaboradores una vez se ingrese a las oficinas, implementación del sistema biométrico de cámara web en laptops con el hardware necesario
Organización	Ausencia de políticas sobre el uso del correo electrónico	ALTO	POSIBLE	MAYOR	No se cuenta con política, no se cuenta con correo corporativo	Implementación de un sistemas de correo electrónico corporativo así como también la elaboración e implementación de una política corporativa de correo electrónico
Organización	Ausencia de procedimientos para la introducción del software en los sistemas operativos	ALTO	POSIBLE	MAYOR	No se cuenta con controles	Elaboración e implementación de un procedimiento de control de cambios
Organización	Ausencia de procedimientos para el manejo de información clasificada	ALTO	POSIBLE	MAYOR	Ausencia de procedimiento o política	Elaboración e implementación de Política de Uso y Manejo de Información Confidencial
Organización	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	ALTO	POSIBLE	MAYOR	No se cuenta con un organigrama de la organización, no se encuentran definidos responsabilidades de los cargos así como debes formales por cada colaborador que se encuentra bajo relación de dependencia.	Elaboración de Matriz RACI para su aprobación ante los accionistas
Organización	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	CRÍTICO	PROBABLE	MAYOR	No se encuentra con una política de control de accesos	Elaboración e implementación de Política de Control de accesos
Organización	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	ALTO	POCO PROBABLE	MAYOR	Servicios de terceros no cuentan con contratos formales	Verificación de todos los servicios de outsourcing
Organización	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	ALTO	POSIBLE	MAYOR	No se cuenta con procedimiento o política	Revisión de manuales de procedimientos existentes y verificar su correcta aplicación o actualización de acuerdo la a la Ley Orgánica de Protección de datos personales y marcos de referencia
Organización	Ausencia de procedimientos de identificación y valoración de riesgos	ALTO	POSIBLE	MAYOR	Ausencia de un procedimiento de administración de usuarios y privilegios	Elaboración e implementación de manual de procedimientos de Cuentas de Usuario
Organización	Ausencia de procedimiento de control de cambios	ALTO	POSIBLE	MAYOR	Ausencia de procedimiento de control de cambios	Elaboración e implementación de un procedimiento de control de cambios

Vulnerabilidades reales		Riesgo inherente			Controles existentes	Planes de Acción
Tipo	Ejemplo	Riesgo	Probabilida	x Impacto		
Organización	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	ALTO	POSIBLE	MAYOR	No se cuenta con política	Elaboración e implementación de una Política y procedimiento de procesos disciplinarios
Organización	Ausencia de política formal sobre la utilización de computadores portátiles	ALTO	POSIBLE	MAYOR	Ausencia de política de dispositivos móviles	Elaboración e implementación de una política de dispositivos móviles
Organización	Ausencia de control de los activos que se encuentran fuera de las instalaciones	ALTO	POSIBLE	MAYOR	Ausencia de política de dispositivos móviles	Elaboración e implementación de una política de dispositivos móviles
Organización	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	MODERADO	RARO	MAYOR	No se cuenta con una política	Elaboración e implementación de una Política de Escritorio y Pantalla Limpia
Organización	Ausencia de autorización de los recursos de procesamiento de la información	CRÍTICO	PROBABLE	MAYOR	Ausencia de un procedimiento de administración de usuarios y privilegios	Elaboración e implementación de manual de procedimientos de Cuentas de Usuario
Organización	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	CRÍTICO	PROBABLE	MAYOR	No se cuentan con mecanismos de monitoreo	Revisión y actualización de matriz de riesgos, revisión del procedimiento de contraseñas, revisión del procedimiento de destrucción de datos
Organización	Ausencia de revisiones regulares por parte de la gerencia	ALTO	POCO PROBABLE	MAYOR	La gerencia conoce parcialmente la gestión de SGSI	Capacitar a todo el personal acerca de la importancia de un sistema de SGSI
Organización	Ausencia de planes de continuidad	ALTO	POSIBLE	MAYOR	No se cuenta con un plan de resiliencia y continuidad del negocio	Elaboración e implementación de una plan resiliencia y continuidad del negocio
Personal	Entrenamiento insuficiente en seguridad	ALTO	POSIBLE	MAYOR	No se cuenta con controles	Capacitar a todo el personal acerca de la importancia de un sistema de SGSI
Personal	Uso incorrecto de software y hardware	ALTO	POSIBLE	MAYOR	No se cuenta con políticas controles o procedimientos	Análisis de manual de procedimientos de procesos y manual de procedimientos de las diferentes herramientas tecnológicas para el procesamiento de la información
Personal	Falta de conciencia acerca de la seguridad	ALTO	POSIBLE	MAYOR	No se cuenta con controles	Capacitar a todo el personal acerca de la importancia de un sistema de SGSI
Red	Líneas de comunicación sin protección	CRÍTICO	PROBABLE	MAYOR	Sistema de red no cuenta con una configuración avanzada de seguridad	Implementación de PROCEDIMIENTOS TÉCNICOS PARA GARANTIZAR SEGURIDAD EN LA RED Y LA INTEGRIDAD DEL SERVICIO
Red	Conexiones de red pública sin protección	CRÍTICO	PROBABLE	MAYOR	Ausencia de política de dispositivos móviles	Elaboración e implementación de una política de dispositivos móviles
Red	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	ALTO	POSIBLE	MAYOR	Sistema de red no cuenta con una configuración avanzada de seguridad	Implementación de PROCEDIMIENTOS TÉCNICOS PARA GARANTIZAR SEGURIDAD EN LA RED Y LA INTEGRIDAD DEL SERVICIO
Software	Configuración incorrecta de parámetros	CRÍTICO	PROBABLE	MAYOR	No se cuenta con parámetros definidos para la configuración de equipos	Contratación formal de un servicio de outsourcing para el mantenimiento preventivo y correctivo de todos los equipos informáticos
Software	Defectos bien conocidos en el software	ALTO	POSIBLE	MAYOR	Ausencia de evaluación de riesgos respecto del software	Revisión de manuales de procedimientos de las aplicaciones
Software	Asignación errada de los derechos de acceso	CRÍTICO	PROBABLE	MAYOR	Derecho de acceso solo tiene los niveles ejecutivos	Elaboración e implementación de manual de procedimientos de Cuentas de Usuario
Software	Descarga y uso no controlados de software	CRÍTICO	PROBABLE	MAYOR	No se cuenta con controles	Elaboración e implementación de manual de procedimientos de Cuentas de Usuario
Software	Ausencia de copias de respaldo	CRÍTICO	PROBABLE	MAYOR	Copias de seguridad a través de cuenta one drive personal del gerente general	Elaboración e implementación de Política de copias de seguridad o backup
Software	Ausencia de control de cambios eficaz	ALTO	POSIBLE	MAYOR	Ausencia de política de control de cambios	Elaboración e implementación de un procedimiento de control de cambios

ANEXO 8 ANEXO D ISO 27005

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
Hardware	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
Hardware	Sensibilidad a la radiación electromagnética	Radiación electromagnética
Hardware	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
Hardware	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
Hardware	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
Hardware	Almacenamiento sin protección	Hurto de medios o documentos
Hardware	Falta de cuidado en la disposición final	Hurto de medios o documentos
Hardware	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
Software	Defectos bien conocidos en el software	Abuso de los derechos
Software	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
Software	Disposición o reutilización de los medios de almacenamiento sin borrado aded	Abuso de los derechos
Software	Ausencia de pistas de auditoria	Abuso de los derechos
Software	Asignación errada de los derechos de acceso	Abuso de los derechos
Software	Software ampliamente distribuido	Corrupción de datos
Software	En términos de tiempo utilización de datos errados en los programas de aplica	Corrupción de datos
Software	Interfaz de usuario compleja	Error en el uso
Software	Ausencia de documentación	Error en el uso
Software	Configuración incorrecta de parámetros	Error en el uso
Software	Fechas incorrectas	Error en el uso
Software	Ausencia de mecanismos de identificación y autentificación, como la autentificació	Falsificación de derechos
Software	Tablas de contraseñas sin protección	Falsificación de derechos
Software	Gestión deficiente de las contraseñas	Falsificación de derechos
Software	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
Software	Software nuevo o inmaduro	Mal funcionamiento del software
Software	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
Software	Ausencia de control de cambios eficaz	Mal funcionamiento del software
Software	Descarga y uso no controlados de software	Manipulación con software
Software	Ausencia de copias de respaldo	Manipulación con software
Software	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
Software	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
Red	Líneas de comunicación sin protección	Escucha encubierta
Red	Tráfico sensible sin protección	Escucha encubierta
Red	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
Red	Punto único de falla	Falla del equipo de telecomunicaciones
Red	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
Red	Arquitectura insegura de la red	Espionaje remoto
Red	Transferencia de contraseñas en claro	Espionaje remoto
Red	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
Red	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
Personal	Procedimientos inadecuados de contratación	Destrucción de equipos o de medios.
Personal	Entrenamiento insuficiente en seguridad	Error en el uso
Personal	Uso incorrecto de software y hardware	Error en el uso
Personal	Falta de conciencia acerca de la seguridad	Error en el uso
Personal	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de datos
Personal	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
Personal	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los	Destrucción de equipos o de medios.
Lugar	Ubicación en un área susceptible de inundación	Inundación
Lugar	Red energética inestable	Pérdida del suministro de energía
Lugar	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
Organización	Ausencia de proceso formal para la revisión	Abuso de los derechos
Organización	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los con	Abuso de los derechos
Organización	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de inf	Abuso de los derechos
Organización	Ausencia de auditorías (supervisiones)	Abuso de los derechos
Organización	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
Organización	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
Organización	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
Organización	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
Organización	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
Organización	Ausencia de procedimiento formal para el control de la documentación del S	Corrupción de datos
Organización	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
Organización	Ausencia de procedimiento formal para la autorización de la información disponibl	Datos provenientes de fuentes no confiables
Organización	Ausencia de asignación adecuada de responsabilidades en la seguridad de la info	Negación de acciones
Organización	Ausencia de planes de continuidad	Falla del equipo
Organización	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
Organización	Ausencia de procedimientos para la introducción del software en los sistemas d	Error en el uso
Organización	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso
Organización	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
Organización	Ausencia de responsabilidades en la seguridad de la información en la descripc	Error en el uso
Organización	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la in	Procesamiento ilegal de datos
Organización	Ausencia de procesos disciplinarios definidos en el caso de incidentes de segu	Hurto de equipo
Organización	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
Organización	Ausencia de control de los activos que se encuentran fuera de las instalacione	Hurto de equipo
Organización	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
Organización	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
Organización	Ausencia de mecanismos de monitoreo establecidos para las brechas en l	Hurto de medios o documentos
Organización	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
Organización	Ausencia de procedimientos para la presentación de informes sobre las debilidade	Uso no autorizado del equipo
Organización	Ausencia de procedimientos del cumplimiento de las disposiciones con los derech	Uso de software falso o copiado

ANEXO 9 MATRIZ MARGER IT

Amenaza		[D] Datos / Información	[D] [conf] datos de configuración	[D] [log] registro de actividad	[K] Claves criptográficas	[S] Servicios	[SW] Software - Aplicaciones informáticas	[HW] Equipamiento informático (hardware)	[COM] Redes de comunicaciones	[Media] Soportes de información	[AUX] Equipamiento auxiliar	[L] Instalaciones	[P] Personal
		Tipo de Activo											
[N] Desastres naturales	[N.1] Fuego							D		D	D	D	
	[N.2] Daños por agua							D		D	D	D	
	[N.*] Desastres naturales							D		D	D	D	
[I] De origen industrial	[I.1] Fuego							D		D	D	D	
	[I.2] Daños por agua							D		D	D	D	
	[I.*] Desastres industriales							D		D	D	D	
	[I.3] Contaminación mecánica							D		D	D		
	[I.4] Contaminación electromagnética							D		D	D		
	[I.5] Avería de origen físico o lógico						D	D		D	D		
	[I.6] Corte del suministro eléctrico							D		D	D		
	[I.7] Condiciones inadecuadas de temperatura o humedad							D		D	D		
	[I.8] Fallo de servicios de comunicaciones								D				
	[I.9] Interrupción de otros servicios y suministros esenciales										D		
	[I.10] Degradación de los soportes de almacenamiento de la información									D			
	[I.11] Emanaciones electromagnéticas							C		C	C	C	
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	I C D			I C D	I C D	I C D	C		I C D			
	[E.2] Errores del administrador	D I C			D I C	D I C	D I C	D I C	D I C	D I C			
	[E.3] Errores de monitorización (log)			I									
	[E.4] Errores de configuración		I										
	[E.7] Deficiencias en la organización												D
	[E.8] Difusión de software dañino						D I C						
	[E.9] Errores de [re-]encaminamiento					C	C		C				
	[E.10] Errores de secuencia					I	I		I				
	[E.15] Alteración accidental de la información	I			I	I	I		I	I		I	
	[E.18] Destrucción de información	D			D	D	D		D	D		D	
	[E.19] Fugas de información	C			C	C	C		C	C		C	C
	[E.20] Vulnerabilidades de los programas (software)						I D C						
	[E.21] Errores de mantenimiento / actualización de programas (software)						I D						
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)							D		D	D		
	[E.24] Caída del sistema por agotamiento de recursos					D		D	D				
	[E.25] Pérdida de equipos							D C		D C	D C		
	[E.28] Indisponibilidad del personal												D
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)			I									
	[A.4] Manipulación de la configuración			I C A									
	[A.5] Suplantación de la identidad del usuario	C A I			C A I	C A I	C A I		C A I				
	[A.6] Abuso de privilegios de acceso	C I D			C I D	C I D	C I D	C I D	C I D				
	[A.7] Uso no previsto					D C I	D C I	D C I	D C I	D C I	D C I	D C I	
	[A.8] Difusión de software dañino						D I C						
	[A.9] [Re-]encaminamiento de mensajes					C	C		C				
	[A.10] Alteración de secuencia					I	I		I				
	[A.11] Acceso no autorizado	C I			C I	C I	C I	C I	C I	C I	C I	C I	
	[A.12] Análisis de tráfico								C				
	[A.13] Repudio			I		I							
	[A.14] Interceptación de información (escucha)								C				
	[A.15] Modificación deliberada de la información	I			I	I	I		I	I		I	
	[A.18] Destrucción de información	D			D	D	D			D		D	
	[A.19] Divulgación de información	C			C	C	C		C	C		C	
	[A.22] Manipulación de programas						C I D						
	[A.23] Manipulación de los equipos							C D		C D	C D		
	[A.24] Denegación de servicio					D		D	D				
	[A.25] Robo							D C		D C	D C		
	[A.26] Ataque destructivo							D		D	D	D	
	[A.27] Ocupación enemiga											D C	
	[A.28] Indisponibilidad del personal												D
	[A.29] Extorsión												C I D
	[A.30] Ingeniería social (picaresca)												C I D

ANEXO 10 ANEXO C ISO 27005

ANEXO C

EJEMPLOS DE AMENAZAS COMUNES

La siguiente tabla presenta ejemplos de amenazas comunes.
La lista se puede utilizar durante el proceso de valoración de las amenazas.
Estas pueden ser deliberadas, accidentales o ambientales (naturales) y pueden dar como resultado, por ejemplo, daño o pérdida de los servicios esenciales.
Los grupos de amenazas no están en orden de prioridad.

Tipo	Amenazas		Origen		
			D (deliberadas)	A (accidentales)	E (ambientales)
Daño físico	Fuego	A, D, E	D	A	E
	Daño por agua	A, D, E	D	A	E
	Contaminación	A, D, E	D	A	E
	Accidente importante	A, D, E	D	A	E
	Destrucción del equipo o los medios	A, D, E	D	A	E
	Polvo, corrosión, congelamiento	A, D, E	D	A	E
Eventos naturales	Fenómenos climáticos	E			E
	Fenómenos sísmicos	E			E
	Fenómenos volcánicos	E			E
	Fenómenos meteorológicos	E			E
	Inundación	E			E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D	D	A	
	Pérdida de suministro de energía	A, D, E	D	A	E
	Falla en el equipo de telecomunicaciones	A, D	D	A	
Perturbación debida a la radiación	Radiación electromagnética	A, D, E	D	A	E
	Radiación térmica	A, D, E	D	A	E
	Impulsos electromagnéticos	A, D, E	D	A	E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D	D		
	Espionaje remoto	D	D		
	Escucha encubierta	D	D		
	Hurto de medios o documentos	D	D		
	Hurto de equipo	D	D		
	Recuperación de medios reciclados o desechados	D	D		
	Divulgación	A, D	D	A	
	Datos provenientes de fuentes no confiables	A, D	D	A	
	Manipulación con hardware	D	D		
	Manipulación con software	A, D	D	A	
	Detección de la posición	D	D		
Fallas técnicas	Falla del equipo	A		A	
	Mal funcionamiento del equipo	A		A	
	Saturación del sistema de información	A, D	D	A	
	Mal funcionamiento del software	A		A	
	Incumplimiento en el mantenimiento del sistema de información	A, D	D	A	
Acciones no autorizadas	Uso no autorizado del equipo	D	D		
	Copia fraudulenta del software	D	D		
	Uso de software falso o copiado	A, D	D	A	
	Corrupción de los datos	D	D		
	Procesamiento ilegal de los datos	D	D		
Compromiso de las funciones	Error en el uso	A		A	
	Abuso de derechos	A, D	D	A	
	Falsificación de derechos	D	D		
	Negación de acciones	D	D		
	Incumplimiento en la disponibilidad del personal	A, D, E	D	A	E

ANEXO 11 MODELO OPERACIONAL BASE

Clasificación de Dominios ISO		NIST				
		PROTEGER	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
Procesos Estratégicos	A.5 Políticas de seguridad de la información	A.5.1.1				
Procesos Estratégicos	A.6 Organización de la seguridad de la información	A.6.1.1 A.6.1.1 A.	A.6.1.2 A.6.1.1 A.6.1.2 A.6.1.5	A.6.1.1	A.6.1.1 A.6.1.3 A.6.1.4	A.6.1.4
Procesos Tácticos	A.8 Gestión de activos	A.8.1.1	A.8.2.2 A.8.1.4 A.8.2.1 A.8.2.3			
Procesos Tácticos	A.9 Control de acceso		A.9.1.2 A.9.1.1 A.9.1.2 A.9.2.1			
Procesos Tácticos	A.15 Relación con proveedores	A.15.1.1 A.15.1.1	A.15.1.1 A.15.2.1	A.15.2.1		
Procesos Tácticos	A.18 Cumplimiento	A.18.1.1 A.18.2.3	A.18.1.4 A.18.1.3	A.18.1.4 A.18.2.2		
Procesos Operativos	A.7 Seguridad relativa a los recursos humanos	A.7.2.1	A.7.1.1 A.7.2.1 A.7.1.1 A.7.1.1	A.7.2.2	A.7.2.2	
Procesos Operativos	A.10 Criptografía		A.10.1.1			
Procesos Operativos	A.11 Seguridad física y del entorno	A.11.2.6 A.11.1.4	A.11.1.1 A.11.1.4 A.11.1.4 A.11.1.2	A.11.1.1 A.11.1.2		
Procesos Operativos	A.12 Seguridad de las operaciones	A.12.5.1 A.12.1.3	A.12.2.1 A.12.1.3 A.12.1.2 A.12.4.1	A.12.1.1 A.12.2.1 A.12.1.2 A.12.4.1	A.12.4.1 A.12.2.1 A.12.4.3	
Procesos Operativos	A.13 Seguridad de las comunicaciones	A.13.2.1 A.13.2.:	A.13.1.1 A.13.1.1 A.12.6.2 A.13.1.1	A.13.1.1 A.13.1.2		
Procesos Operativos	A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información		A.14.1.2 A.14.1.2 A.14.1.1 A.14.1.3	A.14.2.7 A.14.2.8		
Procesos Operativos	A.16 Gestión de incidentes de seguridad de la información	A.16.1.6	A.16.1.1 A.16.1.3	A.16.1.1 A.16.1.2 A.16.1.4 A.16.1.3	A.16.1.4 A.16.1.1 A.16.1.6 A.16.1.5	A.16 Ges A.16 Ges
Procesos Operativos	A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	A.17.1.1 A.17.1.3	A.17.2.1 A.17.1.1 A.17.1.2			

ANEXO 12 MODELO OPERACIONAL RESUMIDO

Clasificación de Dominios ISO	NIST																					
	IDENTIFICAR					PROTEGER						DETECTAR			RESPONDER					RECUPERAR		
	ID.AM Gestión de activos	ID.BE Entorno empresarial	ID.GV Gobernanza	ID.RA Evaluación de riesgos	ID.SC Gestión del riesgo de la cadena de suministro	PR.AC Gestión de identidad y control de acceso	PR.AT Conciencia y capacitación	PR.DS Seguridad de datos	PR.IP Procesos y procedimientos de protección de la informació	PR.MA Mantenimiento	PR.PT Tecnología protectora	DE.AE Anomalías y eventos	DE.CM-2 Vigilancia continua de seguridad	DE.DP Procesos de detección	RS.CO Comunicaciones	RC.IM Mejoras	RS.AN Análisis	RS.MI Mitigación	RS.RP Planificación de respuesta	RC.CO Comunicaciones	RC.IM Mejoras	RC.RP Planificación de recuperación
Procesos Estratégicos			A.5 Políticas de seguridad de la información																			
	A.6 Organización de la seguridad de la información		A.6 Organización de la seguridad de la información	A.6 Organización de la seguridad de la información		A.6 Organización de la seguridad de la información	A.6 Organización de la seguridad de la información	A.6 Organización de la seguridad de la información	A.6 Organización de la seguridad de la información					A.6 Organización de la seguridad de la información	A.6 Organización de la seguridad de la información					A.6 Organización de la seguridad de la información		
Procesos Tácticos	A.8 Gestión de activos							A.8 Gestión de activos	A.8 Gestión de activos		A.8 Gestión de activos											
						A.9 Control de acceso		A.9 Control de acceso			A.9 Control de acceso											
		A.15 Relación con proveedores	A.15 Relación con proveedores		A.15 Relación con proveedores					A.15 Relación con proveedores			A.15 Relación con proveedores									
			A.18 Cumplimiento	A.18 Cumplimiento		A.18 Cumplimiento			A.18 Cumplimiento					A.18 Cumplimiento								
Procesos Operativos			A.7 Seguridad relativa a los recursos humanos			A.7 Seguridad relativa a los recursos humanos	A.7 Seguridad relativa a los recursos humanos	A.7 Seguridad relativa a los recursos humanos	A.7 Seguridad relativa a los recursos humanos					A.7 Seguridad relativa a los recursos humanos	A.7 Seguridad relativa a los recursos humanos							
								A.10 Criptografía														
	A.11 Seguridad física y del entorno	A.11 Seguridad física y del entorno				A.11 Seguridad física y del entorno		A.11 Seguridad física y del entorno	A.11 Seguridad física y del entorno	A.11 Seguridad física y del entorno	A.11 Seguridad física y del entorno		A.11 Seguridad física y del entorno									
	A.12 Seguridad de las operaciones	A.12 Seguridad de las operaciones		A.12 Seguridad de las operaciones			A.12 Seguridad de las operaciones	A.12 Seguridad de las operaciones	A.12 Seguridad de las operaciones		A.12 Seguridad de las operaciones	A.12 Seguridad de las operaciones	A.12 Seguridad de las operaciones				A.12 Seguridad de las operaciones	A.12 Seguridad de las operaciones				
	A.13 Seguridad de las comunicaciones					A.13 Seguridad de las comunicaciones		A.13 Seguridad de las comunicaciones			A.13 Seguridad de las comunicaciones	A.13 Seguridad de las comunicaciones										
						A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información		A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información		A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información		A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información								
				A.16 Gestión de incidentes de seguridad de la información					A.16 Gestión de incidentes de seguridad de la información			A.16 Gestión de incidentes de seguridad de la información		A.16 Gestión de incidentes de seguridad de la información	A.16 Gestión de incidentes de seguridad de la información	A.16 Gestión de incidentes de seguridad de la información	A.16 Gestión de incidentes de seguridad de la información	A.16 Gestión de incidentes de seguridad de la información	A.16 Gestión de incidentes de seguridad de la información		A.16 Gestión de incidentes de seguridad de la información	A.16 Gestión de incidentes de seguridad de la información
		A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio			A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio			A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio		A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio											

ANEXO 13 MODELO OPERACIONAL LITERALES

		Identificar					Proteger						Detectar			Responder					Recuperar		
	Clasificación de Dominios ISO	Gestión de activos	Entorno empresarial	Gobernanza	Evaluación de riesgos	Gestión del riesgo de la cadena de suminis	Gestión de identidad y control de acces	Conciencia y capacitación	Seguridad de datos	Procesos y procedimientos de protección de la informació	Manteni miento	Tecnología protectora	Anomalías y eventos	Vigilancia continua de segurid	Procesos de detecc	Análisis	Comunica ciones	Mejoras	Mitigación	Planifica ción de respue	Comunica ciones	Mejoras	Planifica ción de recuperac ión
Procesos Estratégicos	A.5 Políticas de seguridad de la información			A.5.1.1																			
	A.6 Organización de la seguridad de la información	A.6.1.1		A.6.1.1	A.6.1.4		A.6.1.2 A.6.2.1 A.6.2.2	A.6.1.1	A.6.1.2	A.6.1.5					A.6.1.1		A.6.1.1 A.6.1.3 A.6.1.4				A.6.1.4		
Procesos Tacticos	A.8 Gestión de activos	A.8.1.1							A.8.2.2 A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3	A.8.1.4 A.8.2.3 A.8.3.1 A.8.3.2		A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.1 A.8.3.3											
	A.9 Control de acceso	A.8.1.2 A.8.2.1					A.9.1.2 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.6 A.9.3.1 A.9.4.1 A.9.4.2 A.9.4.3 A.9.4.4 A.9.4.5		A.9.1.1 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5			A.9.1.2											
	A.15 Relación con proveedores		A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2	A.15.1.1		A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2					A.15.1.1 A.15.2.1			A.15.2.1									
	A.18 Cumplimiento			A.18.1.1 A.18.1.2 A.18.1.3 A.18.1.4 A.18.1.5	A.18.2.3		A.18.1.4			A.18.1.3 A.18.2.2 A.18.2.3					A.18.1.4 A.18.2.2 A.18.2.3								
Procesos Operativos	A.7 Seguridad relativa a los recursos humanos			A.7.2.1			A.7.1.1	A.7.2.1 A.7.2.2	A.7.1.1 A.7.1.2 A.7.3.1	A.7.1.1 A.7.1.2 A.7.2.1 A.7.2.2 A.7.2.3 A.7.3.1					A.7.2.2		A.7.2.2						
	A.10 Criptografía								A.10.1.1														
	A.11 Seguridad física y del entorno	A.11.2.6	A.11.1.4 A.11.2.2 A.11.2.3				A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.5 A.11.2.6 A.11.2.7 A.11.2.8		A.11.1.4 A.11.1.5 A.11.2.1 A.11.2.4 A.11.2.5 A.11.2.7	A.11.1.4 A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.7	A.11.1.2 A.11.2.4 A.11.2.5 A.11.2.6	A.11.2.9		A.11.1.1 A.11.1.2									
	A.12 Seguridad de las operaciones	A.12.5.1	A.12.1.3		A.12.6.1			A.12.2.1	A.12.1.3 A.12.1.4 A.12.2.1 A.12.5.1	A.12.1.2 A.12.3.1 A.12.5.1 A.12.6.1		A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1	A.12.1.1 A.12.1.2 A.12.4.1	A.12.2.1 A.12.4.1 A.12.4.3 A.12.5.1 A.12.6.1 A.12.6.2		A.12.4.1 A.12.4.3			A.12.2.1 A.12.6.1				
	A.13 Seguridad de las comunicaciones	A.13.2.1 A.13.2.2					A.13.1.1 A.13.1.3 A.13.2.1		A.13.1.1 A.13.1.3 A.13.2.1 A.13.2.3 A.13.2.4	A.12.6.2		A.13.1.1 A.13.2.1	A.13.1.1 A.13.1.2										
	A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información						A.14.1.2 A.14.1.3		A.14.1.2 A.14.1.3 A.14.2.4	A.14.1.1 A.14.2.1 A.14.2.2 A.14.2.3 A.14.2.4 A.14.2.5		A.14.1.3		A.14.2.7	A.14.2.8								
	A.16 Gestión de incidentes de seguridad de la información				A.16.1.6					A.16.1.1 A.16.1.3 A.16.1.6			A.16.1.1 A.16.1.4 A.16.1.7		A.16.1.2 A.16.1.3 A.16.1.6	A.16.1.4 A.16.1.5 A.16.1.6 A.16.1.7	A.16.1.1 A.16.1.2	A.16.1.6	A.16.1.5	A.16.1.5		A.16 Ges	A.16 Ges
	A.17 Aspectos de seguridad de la información para la gestión de la continuidad		A.17.1.1 A.17.1.2 A.17.2.1			A.17.1.3			A.17.2.1	A.17.1.1 A.17.1.2 A.17.1.3		A.17.1.2 A.17.2.1											