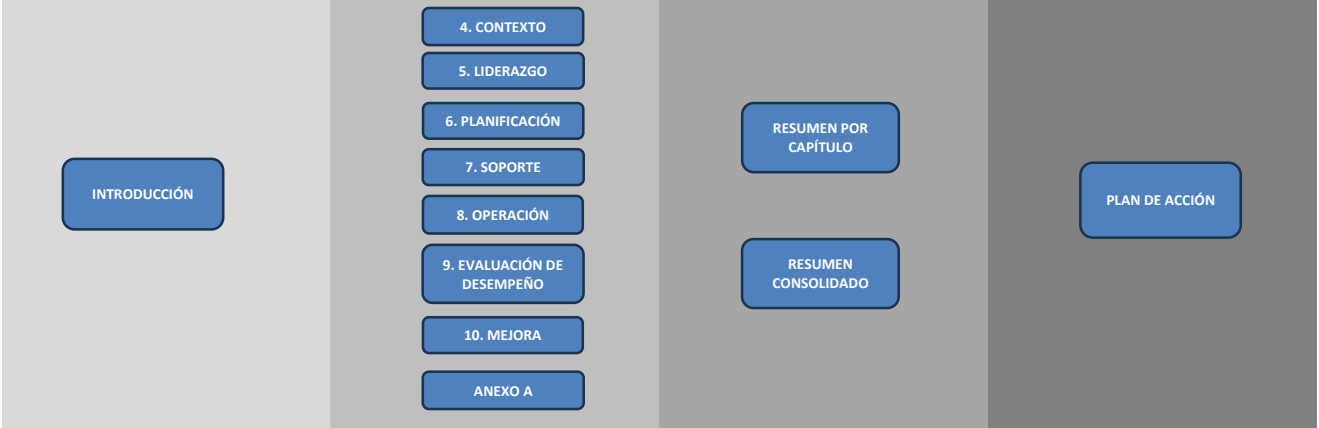


HERRRAMIENTA AUTODIAGNÓSTICO NTC ISO 9001:2015 E ISO/IEC 27001: 2022



Elaboró:
Yurany Pineda López
Paola Moreno Cely

Fuente: Centro Nacional de Memoria Histórica



INTRODUCCIÓN

HERRRAMIENTA AUTODIAGNÓSTICO NTC ISO 9001:2015 E ISO/IEC 27001: 2022

Se entiende por autodiagnóstico el conjunto de actividades realizadas por una misma organización para establecer el estado del arte de un sistema, proceso o actividad respecto a un parámetro previamente establecido.

Para este caso, su aplicación se centra en identificar la situación actual del Sistema Integrado de Gestión, respecto a los requerimientos de la NTC ISO 9001:2015 y la ISO/IEC 27001:2022.

Esta herramienta puede ser utilizada para desarrollar la primera etapa del ciclo de mejoramiento continuo, es decir el PLANEAR. No es lo mismo que llevar a cabo una auditoría, ya que el personal de la organización participa en el mismo diagnóstico, por lo cual no se cumplen los principios de la auditoría como objetividad, imparcialidad, autonomía e independencia.

Uno de los propósitos del auto diagnóstico es establecer un plan de implementación para organizaciones que apenas están implementando los dos estándares.

ESTRUCTURA:

En su primera parte, este documento cuenta con siete (7) hojas que hacen referencia a los capítulos 4 al 10 de la norma INTC ISO 9001: 2015, en donde se presenta una lista de chequeo de acuerdo con los requisitos que debe evaluarse.

En la segunda parte, una vez realizada la evaluación, contiene las hojas RESUMEN CONSOLIDADO y RESUMEN POR CAPÍTULO, en donde se encuentran los gráficos y la información del diagnóstico consolidada, por lo tanto, no se requiere diligenciar ni manipular dichas hojas, toda vez que los gráficos se generarán automáticamente de acuerdo a los resultados obtenidos en el diagnóstico.

DILIGENCIAMIENTO:

En el diligenciamiento y evaluación es importante aclarar los siguientes criterios:

NO APLICA= Marque con una "X", Cuando se ha excluido el requisito y este no afecta la capacidad ni la responsabilidad para cumplir requisitos por parte de la organización.

COMPLETO= Marque con una "X", en el caso de haber realizado TODAS las acciones requeridas, poseer evidencias suficientes y tener resultados eficaces de cumplimiento del requisito.

PARCIAL= Marque con una "X", en el caso de no haber realizado al menos una acción o actividad requeridas, poseer evidencias insuficientes y a pesar de obtener resultados, estos no son eficaces.

NINGUNO= Marque con una "X", en caso de no encontrar ninguna acción o actividad relacionada, no se poseen evidencias ni resultados relacionados con el requisito.

Nota: La evaluación es excluyente, por favor no marque con una "X" en más de 2 criterios, por ejemplo marcar X en completo y también en parcial.

De igual manera, se deberá relacionar evidencias o los aspectos desarrollados por la organización frente a los requisitos que se cumplen de manera completa o parcial, esto deberá relacionarse en la columna denominada **¿QUÉ TIENE ?**.

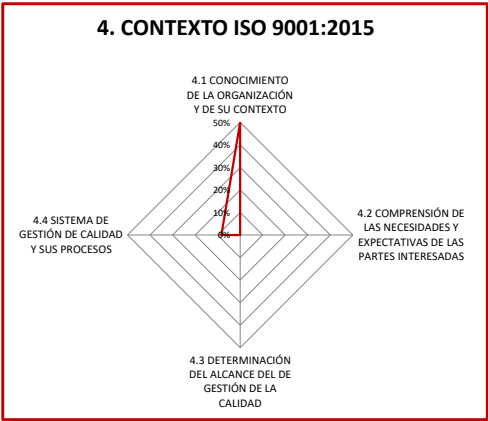
Mientras que en la columna **¿QUE NOS FALTA?** se relacionará las diferencias, brechas, evidencias posibles o aspectos a desarrollar por la organización frente a los requisitos que se cumplen de manera parcial o sin ninguna acción. Puede incluirse actividades, tareas, resultados esperados, el tiempo en el que se dene cumplir, procesos relacionados, así como responsables de las actividades para cerrar las brechas y la opción de relacionar un presupuesto si es necesario.

DIAGNÓSTICO NTC ISO 9001:2015 E ISO/IEC 27001: 2022												
		ISO 9001:2015				ISO 27001:2022						
4.CONTEXTO DE LA ORGANIZACIÓN (ISO 9001:2015)	4.CONTEXTO DE LA ORGANIZACIÓN (ISO 27001:2022)	NO APLICA	COMPLETO	PARCIAL	NINGUNO	NO APLICA	COMPLETO	PARCIAL	NINGUNO	QUÉ TIENE	QUÉ NOS FALTA	DOCUMENTACIÓN ASOCIADA
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO		50%				0%					
¿Se han determinado las cuestiones externas e internas pertinentes al propósito, dirección estratégica y que afectan los resultados del SGC?	La organización debe determinar las problemáticas externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.											
¿Se realiza seguimiento y revisión de la información sobre las cuestiones externas e internas?	NOTA: La determinación de estas cuestiones hace referencia a establecer el contexto externo e interno de la organización, considerado en el numeral 5.4,1 de la NTC-ISO 31000:2018											
			X						X	Cuenta con Misión, Visión y un canva inicial con la descripción de los servicios	No se evalúa la interiorización de la misión, visión y la política de calidad a los clientes internos Actas de seguimiento de la gestión estratégica, cumplir con las actividades programadas en el plan estratégico Política de Calidad que están disponibles en la página web y se socializa en las capacitaciones Cuenta con el Análisis FODA, matriz PESTAL, el modelo Canva.	
			0	1	0		0	0	1			
4.2 COMPRESIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	4.2 COMPRESIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS		0%				0%					
	La organización debe determinar:											
¿Se han determinado las partes interesadas además de los trabajadores que son pertinentes al SGC y la procedencia u origen de los componentes de sus productos o servicios?	a. Las partes interesadas que son relevantes al sistema de gestión de la seguridad de la información; y				X				X		Matriz de partes interesadas	Registro o lista de partes interesadas (clientes, empleados, autoridades, etc.)
¿Se han determinado las necesidades y expectativas de los trabajadores y de otras partes interesadas para el SGC?	b. Los requisitos relevantes de estas partes interesadas				X				X		Si se identifican las necesidades y las expectativas tanto de los clientes internos, como de las partes interesadas	Análisis de necesidades y expectativas de las partes interesadas (a veces llamado "mapa de partes interesadas")
¿Se realiza seguimiento y revisión de la información sobre las partes interesadas y sus requisitos pertinentes?	c. Cuales de estos requisitos pueden ser abordados a través del sistema de gestión de seguridad de la información											Matriz de partes interesadas (quiénes son, qué necesitan, cómo afectan o se ven afectados)
	NOTA Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios, y las obligaciones contractuales.				X				X		No se hace revisión y seguimiento porque no esta creada la matriz	Registro de seguimiento y cambios (si las necesidades de las partes interesadas varían con el tiempo)
			0	0	3		0	0	3			
4.3 DETERMINACIÓN DEL ALCANCE DEL DE GESTIÓN DE LA CALIDAD	4.3 DETERMINACIÓN DEL ALCANCE DEL DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		0%				0%					
	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.											
¿Se ha determinado los límites y la aplicabilidad del SGC para establecer su alcance?	Cuando se determina este alcance, la organización debe considerar:				X				X		Manual del SGI y establecer el alcance	
a) ¿Se consideran las cuestiones externas e internas?	a. Las problemáticas externas e internas referidas en el numeral 4.1, y				X				X		Se debe establecer desde el PESTAL y DOFA	Manual de calidad (si se utiliza).
b) ¿Se consideran los requisitos de las partes interesadas pertinentes incluyendo requisitos legales?	b. Los requisitos referidos en el numeral 4.2;				X				X		Identificación de partes interesadas Gerencia Estratégica	Documento específico llamado "Declaración de Alcance".
c,d) ¿Se consideran y se establecen las actividades, productos y servicios relacionadas con el trabajo, planificadas o realizadas por la organización?	c. las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones				X				X	Canva Inicial	Fortalecimiento del Canva	Dentro de la Política de Calidad o en un anexo.
¿El alcance del SGC se mantiene como información documentada y está disponible para las partes interesadas?	El alcance debe estar disponible como información documentada.				X				X		No se tiene establecido el alcance para SGC ya que no diseñando	Puede incluir: productos y servicios cubiertos, sitios, procesos, exclusiones justificadas.
¿Se cuenta con justificación para cualquier requisito que no es aplicable para el SGC?					X					El numeral 7.1.5 Recursos de Seguimiento y Medición no aplica para la empresa por su core del negocio	No se tiene documentado y por ende justificado el los requisitos que no son aplicables	Alcance documentado del SGSI (obligatorio). Generalmente incluye: Información sobre los activos, procesos, ubicaciones y límites físicos/lógicos.
¿Se aplican todos los requisitos de esta Norma Internacional si son aplicables en el alcance determinado del SGC?					X						No se tiene establecido el alcance para SGC ya que se está diseñando	Interrelación con otras partes de la organización. Interfaces y dependencias.
			0	0	7		0	0	5			Documento llamado típicamente "Declaración de Alcance del SGSI"

DIAGNÓSTICO NTC ISO 9001:2015 E ISO/IEC 27001: 2022												
		ISO 9001:2015				ISO 27001:2022						
4.CONTEXTO DE LA ORGANIZACIÓN (ISO 9001:2015)	4.CONTEXTO DE LA ORGANIZACIÓN (ISO 27001:2022)	NO APLICA	COMPLETO	PARCIAL	NINGUNO	NO APLICA	COMPLETO	PARCIAL	NINGUNO	QUÉ TIENE	QUÉ NOS FALTA	DOCUMENTACIÓN ASOCIADA
4.4 SISTEMA DE GESTIÓN DE CALIDAD Y SUS PROCESOS	4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		8%				0%					
¿Se ha establecido, implementado, se mantiene y mejora continuamente el SGC, incluidos los procesos e interacciones?	La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta norma.				X				X		Se quiere diseñar e implementado el SGI, a la fecha no se tiene nada diseñado No se tiene caracterizaciones	Mapa de procesos Procedimientos asociados a los procesos Caracterizaciones
¿Se han determinado los procesos, necesarios para el sistema de gestión de la calidad y su aplicación a través de la organización?					X						No se tiene mapa de procesos, sin embargo, no se encuentran limitados en un documento o explícitamente en el alcance	Caracterizaciones
¿Se han determinado las entradas requeridas y las salidas esperadas de estos procesos?					X						No se tiene determinado	Caracterizaciones
¿Se han determinado la secuencia e interacción de estos procesos?					X						No se tiene desarrollado un mapa de procesos	Caracterizaciones
¿Se han determinado y aplicado los criterios y los métodos necesarios para asegurarse de la operación eficaz y el control de estos procesos?					X						Se está estableciendo matriz de trazabilidad para algunos procesos, como Soporte Técnico que hace parte del Misional Sin embargo, no se ha desarrollado para todos los procesos o para los que se consideran necesarios	Caracterizaciones
¿Se han determinado los recursos necesarios para estos procesos y se asegura su disponibilidad?					X					Se cuenta con el personal para el diseño y la implementación, también se cuenta con la norma y se capacita a la Dir Adm	No se ha determinado recursos financieros	Caracterizaciones
¿Se han asignado las responsabilidades y autoridades para estos procesos?					X					si se tiene establecido que el Gerente General debe participar y aprobar los procedimientos que se desarrollen.	Se debe asignar a la Dir Adm con responsable de calidad	Caracterizaciones
¿Se han abordado los riesgos y oportunidades determinados de acuerdo con los requisitos del apartado 6.1.2?					X						No se ha establecido una matriz de riesgos y oportunidades para los procesos	Caracterizaciones
¿Se han evaluado estos procesos e implementado cualquier cambio necesario para asegurarse de que estos procesos logran los resultados previstos?					X						No se han evaluado los procesos que se han diseñado, ya que no se han implementando y tampoco comunicado	Caracterizaciones
¿Se han mejorado los procesos y el sistema de gestión de la calidad?					X						Mecanismo de mejora en los procesos	Caracterizaciones
4.4.2												Caracterizaciones
¿Se mantiene información documentada para apoyar la operación de sus procesos?					X						Documentar los procesos	Caracterizaciones
¿Se conserva la información documentada para tener confianza de que los procesos se realizan según lo planificado?			X							Se conserva la información creada a la fecha	Realizar procedimiento de información documentada Definir el mecanismo de control documental	Caracterizaciones
			1	0	11		0	0	1			

RESUMEN NUMERAL ISO 27001: 2022		ISO 9001
		% AVANCE
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	50%
4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	0%
4.3 DETERMINACIÓN DEL ALCANCE DEL DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	4.3 DETERMINACIÓN DEL ALCANCE DEL DE GESTIÓN DE LA CALIDAD	0%
4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	4.4 SISTEMA DE GESTIÓN DE CALIDAD Y SUS PROCESOS	8%
PROMEDIO DEL AVANCE	PROMEDIO DEL AVANCE	15%

RESUMEN NUMERAL ISO 9001:2015		ISO 27001
		% AVANCE
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	0%
4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	0%
4.3 DETERMINACIÓN DEL ALCANCE DEL DE GESTIÓN DE LA CALIDAD	4.3 DETERMINACIÓN DEL ALCANCE DEL DE GESTIÓN DE LA CALIDAD	0%
4.4 SISTEMA DE GESTIÓN DE CALIDAD Y SUS PROCESOS	4.4 SISTEMA DE GESTIÓN DE CALIDAD Y SUS PROCESOS	0%
PROMEDIO DEL AVANCE	PROMEDIO DEL AVANCE	0%





		ISO 9001:2015				ISO 27001:2022				QUÉ TIENE?	QUÉ NOS FALTA?	DOCUMENTOS ASOCIADOS
5 LIDERAZGO (ISO 9001:2015)	5 LIDERAZGO (ISO 27001:2022)	NO APLICA	COMPLETO	PARCIAL	NINGUNO	NO APLICA	COMPLETO	PARCIAL	NINGUNO			
5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN		14%				13%					
¿La alta dirección tiene asignada la responsabilidad y autoridad para:	La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.			X				X		Manual de cargos	Actualización del manual de cargos para incluir funciones y responsabilidades frente al SGI	Manual de cargos y funciones actualizados
a) Asegurarse de que el SGC es conforme con los requisitos de esta Norma Internacional;	La alta dirección debe asignar la responsabilidad y autoridad para: a) asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma;				X				X		Tiene asignado a la directora administrativa y una profesional en SGSST que trabaja por horas para mantener al día los requisitos	
b) Asegurarse de que los procesos están generando y proporcionando las salidas previstas;	b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.				X				X		Indicadores de desempeño para medir si se están logrando dichas salidas Actas de revisión por la dirección con análisis de salidas por proceso. Acciones correctivas documentadas cuando no se cumplen las salidas. Auditorías internas que evidencien conformidad de los procesos.	
c) informar , en particular, a la alta dirección sobre el desempeño del sistema de gestión integrado, incluyendo el desempeño ambiental y sobre las oportunidades de mejora;	NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de la seguridad de la información dentro de la organización.				X				X		Actas de reuniones de revisión por la dirección. Informes de desempeño con indicadores clave de cada sistema Documentos de seguimiento de oportunidades de mejora identificadas.	
d) Asegurarse de que se promueve el enfoque al cliente en toda la organización;				X						Se promueve en reuniones, también desde la misión, visión, valores corporativos y la política de calidad	Documentar las capacitaciones	Gerencia Estratégica Berrut SAS (Misión, Visión, valores, política)
e) Asegurarse de que la integridad del SGC se mantiene cuando se planifican e implementan cambios en el SGC?					X						Aún no se realizan cambios, sin embargo, los documentos están versionados y adicional se cuenta en el documento un control de cambio, en el cual se indican que se hace y porque se hace	
¿La alta dirección se asegura que las responsabilidades y autoridades para los roles pertinentes se documenten, asignen, se comuniquen, se entiendan y se mantengan como información documentada en toda la organización?					X						Estas responsabilidades están incluidas en las caracterizaciones de procesos, donde se detalla quién hace qué, cómo y con qué recursos. Las descripciones de cargo también se han alineado con los requisitos del sistema, e incluyen responsabilidades relacionadas con calidad, medio ambiente y seguridad	F-ST-01 Caracterización de Proceso V1
		0	0	2	5	0	0	1	3			

RESUMEN NUMERAL ISO 27001: 2022		ISO 9001
		% AVANCE
5.1 LIDERAZGO Y COMPROMISO	5.1 LIDERAZGO Y COMPROMISO	15%
5.2 POLÍTICA	5.2 POLÍTICA	0%
5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	14%
PROMEDIO AVANCE	PROMEDIO AVANCE	10%

ISO 27001
% AVANCE
17%
0%
13%
10%



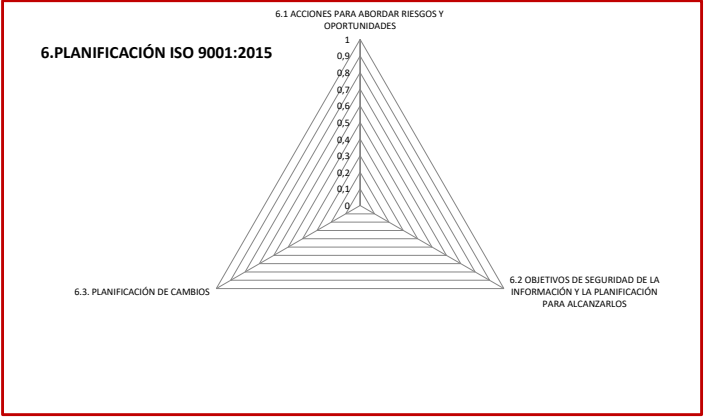
ISTICO NTC ISO 9001:2015 E ISO/IEC 27001: 2022												
		ISO 9001:2015				ISO 27001:2022						
6. PLANIFICACIÓN ISO 9001:2015	6. PLANIFICACIÓN ISO 27001:2022	NO APLICA	COMPLETO	PARCIAL	NINGUNO	NO APLICA	COMPLETO	PARCIAL	NINGUNO	¿QUÉ TIENE?	¿QUÉ NOS FALTA?	DOCUMENTOS ASOCIADOS
6.1 ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES	6.1 ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES		0%				0%					
6.1.1 Generalidades	6.1.1 Generalidades		0%				0%					
¿Al planificar el SGC se consideran las cuestiones externas e internas, los requisitos de las partes interesadas?	Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las problemáticas referidas en el numeral 4.1 y los requisitos a que se hace referencia en el numeral 4.2 y determinar los riesgos y oportunidades que es necesario tratar, con el fin de:				X				X	Vacio	Identificación de riesgos y oportunidades que puedan afectar la conformidad de productos/servicios o la satisfacción del cliente. Establecer un enfoque sistemático para identificar riesgos de seguridad de la información relacionados con la confidencialidad, integridad y disponibilidad. Documentar los criterios para aceptar el riesgo y evaluar su impacto.	Matriz de riesgos y oportunidades (a nivel de procesos o general). Metodología de análisis y evaluación de riesgos (propia o basada en ISO 31000/27005).
¿Se determinan los riesgos y oportunidades con el fin de lograr los resultados previstos,	a) asegurarse de que el sistema de gestión de la seguridad de la información pueda lograr sus resultados previstos;				X				X	Vacio	Evaluación del impacto de esos riesgos (no es obligatorio cuantificarlos, pero sí razonarlos). Establecer un enfoque sistemático para identificar riesgos de seguridad de la información relacionados con la	Matriz de riesgos y oportunidades (a nivel de procesos o general). Metodología de análisis y evaluación de riesgos (propia o basada en ISO 31000/27005).
Aumentar los efectos deseables, prevenir o reducir efectos no deseados y	b) prevenir o reducir efectos indeseados; y				X				X	Vacio	Establecer un enfoque sistemático para identificar riesgos de seguridad de la información relacionados con la	Metodología de análisis y evaluación de riesgos (propia o basada en ISO 31000/27005).
Lograr la mejora	c) lograr la mejora continua.				X				X	Vacio	Establecer un enfoque sistemático para identificar riesgos de seguridad de la información relacionados con la	Metodología de análisis y evaluación de riesgos (propia o basada en ISO 31000/27005).
	La organización debe planificar: d) las acciones para tratar estos riesgos y oportunidades; y	X							X	Vacio	Planificación de acciones para abordar esos riesgos y oportunidades. Establecer un enfoque sistemático para identificar riesgos de seguridad de la información relacionados con la confidencialidad, integridad y disponibilidad. Documentar los criterios para aceptar el riesgo y evaluar su impacto.	Matriz de riesgos y oportunidades (a nivel de procesos o general). Metodología de análisis y evaluación de riesgos (propia o basada en ISO 31000/27005).
	e) la manera de: 1. integrar e implementar estas acciones en sus procesos del sistema de gestión de la seguridad de la información,	X							X	Vacio	Establecer un enfoque sistemático para identificar riesgos de seguridad de la información relacionados con la confidencialidad, integridad y disponibilidad. Documentar los criterios para aceptar el riesgo y evaluar su impacto.	Metodología de análisis y evaluación de riesgos (propia o basada en ISO 31000/27005).
Evaluar la eficacia de estas acciones.	2. evaluar la eficacia de estas acciones.				X				X	Vacio	Integración de esas acciones en los procesos del SGC y su evaluación posterior. Realizar una evaluación de riesgos considerando amenazas, vulnerabilidades y consecuencias. Decidir sobre el tratamiento del riesgo (mitigar, aceptar, transferir o evitar). Conservar la información documentada de todo este proceso.	Vinculación de los riesgos a los objetivos del SGC o procesos clave. Seguimiento de acciones tomadas y evaluación de su eficacia. Informe de evaluación de riesgos, incluyendo activos, amenazas y consecuencias. Mapa o matriz de riesgos de SI. Plan de tratamiento del riesgo. Criterios para la aceptación del riesgo. Resultados y seguimiento del tratamiento (ej. implementación de controles). Referencia al Anexo A (Declaración de Aplicabilidad).
			0	0	5		0	0	7			
	6.1.2 APRECIACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN						0%					
	La organización debe definir y aplicar un proceso de apreciación de riesgos de la seguridad de la información que:											
	a) establezca y mantenga criterios de riesgo de la seguridad de la información que incluyan: 1) Los criterios de aceptación de riesgos; y 2) los criterios para ejecutar la apreciación de riesgos de la seguridad de la información;	X							X	Vacio	Seleccionar opciones de tratamiento del riesgo (mitigar, evitar, transferir, aceptar). Determinar los controles necesarios del Anexo A (u otros) para cada riesgo. Elaborar un plan de tratamiento del riesgo. Obtener la aprobación del propietario del riesgo.	Plan de tratamiento de riesgos (con responsables y tiempos). Declaración de aplicabilidad (SoA) actualizada. Documentación del análisis de efectividad de los controles implementados. Aprobaciones documentadas de los dueños de riesgos.
	b) asegure que las apreciaciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables;	X							X	Vacio	Seleccionar opciones de tratamiento del riesgo (mitigar, evitar, transferir, aceptar). Determinar los controles necesarios del Anexo A (u otros) para cada riesgo. Elaborar un plan de tratamiento del riesgo. Obtener la aprobación del propietario del riesgo.	Plan de tratamiento de riesgos (con responsables y tiempos). Declaración de aplicabilidad (SoA) actualizada. Documentación del análisis de efectividad de los controles implementados. Aprobaciones documentadas de los dueños de riesgos.

	c) identifique los riesgos de la seguridad de la información: 1. aplicar el proceso de apreciación de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información; e 2. identificar a los dueños de los riesgos;	x							x	Vacio	Seleccionar opciones de tratamiento del riesgo (mitigar, evitar, transferir, aceptar). Determinar los controles necesarios del Anexo A (u otros) para cada riesgo. Elaborar un plan de tratamiento del riesgo. Obtener la aprobación del propietario del riesgo.	Plan de tratamiento de riesgos (con responsables y tiempos). Declaración de aplicabilidad (SoA) actualizada. Documentación del análisis de efectividad de los controles implementados. Aprobaciones documentadas de los dueños de riesgos.
	d) analice los riesgos de la seguridad de la información: 1. Apreciar las consecuencias potenciales que resultaran si se materializaran los riesgos identificados en 6.1.2 c) a 1); 2. Apreciar la probabilidad realista de que ocurran los riesgos identificados en 6.1.2 c) 1); y 3. determinar los niveles de riesgo;	x							x	Vacio	Seleccionar opciones de tratamiento del riesgo (mitigar, evitar, transferir, aceptar). Determinar los controles necesarios del Anexo A (u otros) para cada riesgo. Elaborar un plan de tratamiento del riesgo.	Plan de tratamiento de riesgos (con responsables y tiempos). Declaración de aplicabilidad (SoA) actualizada. Documentación del análisis de efectividad de los controles implementados.
	e) evalúe los riesgos de seguridad de la información: 1. comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos en 6.1.2 a) y 2. priorizar los riesgos analizados para el tratamiento de riesgos.	x							x	Vacio	Seleccionar opciones de tratamiento del riesgo (mitigar, evitar, transferir, aceptar). Determinar los controles necesarios del Anexo A (u otros) para cada riesgo. Elaborar un plan de tratamiento del riesgo. Obtener la aprobación del propietario del riesgo.	Revisión periódica del estado de los tratamientos aplicados.
	La organización debe retener información documentada acerca del proceso de apreciación de riesgos de la seguridad de la información.	x							x	Vacio	Mantener la información documentada de todo el proceso.	Los documentos mencionados
			0	0	0			0	0	6		
	6.1.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN							0%				
	La organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para:											
	a) seleccionar las opciones apropiadas de tratamiento de riesgos de la seguridad de la información, teniendo en cuenta los resultados de la apreciación de riesgos;	x							x	vacio	Evaluar cada riesgo identificado (del numeral 6.1.2) y decidir: ¿Se acepta? ¿Se mitiga con un control? ¿Se transfiere (ej. seguros)? ¿Se evita?	Registro de decisiones por riesgo (mitigar, evitar, transferir, aceptar)
	b) determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la seguridad de la información; NOTA Las organizaciones pueden diseñar los controles necesarios, o identificarlos de cualquier fuente.	x							x	vacio	Seleccionar controles de seguridad apropiados para cada riesgo: Basados en el Anexo A (que contiene 93 controles organizados en 4 temas). O pueden ser controles adicionales definidos por la organización.	Lista de controles aplicables al SGSI
	c) comparar los controles determinados en 6.1.3 b) con los del Anexo A, y verificar que no se pasen por alto controles necesarios; NOTA 2. El Anexo A contiene una lista amplia de posibles controles de seguridad de la información.. Los usuarios de este documento pueden dirigirse al Anexo A, y asegurarse que no se pasen por alto los controles necesarios. NOTA 3 Los controles de seguridad de la información listados en el Anexo A no son exhaustivos y pueden ser necesarios controles de seguridad de la	x							x	vacio	Preparar y mantener actualizada la Declaración de Aplicabilidad (SoA): Indica qué controles del Anexo A son aplicables o no y por qué. Debe reflejar los resultados del análisis de riesgos.	Documento actualizado, con justificación por cada control (aplicabilidad y estado)
	d) producir una declaración de aplicabilidad que contenga: - los controles necesarios (véanse el numeral 6.1.3 b) y c)) y - la justificación de las inclusiones, - si es necesaria la implementación de controles de seguridad de la información o no, y - la justificación para la exclusión de los controles del Anexo A;	x							x	vacio	Preparar y mantener actualizada la Declaración de Aplicabilidad (SoA): Indica qué controles del Anexo A son aplicables o no y por qué. Debe reflejar los resultados del análisis de riesgos.	Documento actualizado, con justificación por cada control (aplicabilidad y estado)
	e) formular un plan de tratamiento de riesgos de la seguridad de la información; y	x							x	vacio	Desarrollar un plan de tratamiento del riesgo: Establece responsables, fechas, recursos y acciones para implementar los controles. Obtener aprobación formal del tratamiento de riesgos por parte del propietario del riesgo.	Documento actualizado, con justificación por cada control (aplicabilidad y estado)
	f) obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información.	x							x	vacio	Desarrollar un plan de tratamiento del riesgo: Establece responsables, fechas, recursos y acciones para implementar los controles. Obtener aprobación formal del tratamiento de riesgos por parte del propietario del riesgo.	Cronograma, responsables, estado de implementación Firmas, correos o minutos de reuniones de validación del tratamiento
	La organización debe retener información documentada acerca del proceso de tratamiento de riesgos de la seguridad de la información.	x							x	vacio	Mantener la información documentada de todo el proceso.	Política, procedimiento y/o registros del análisis y tratamiento de riesgos
	NOTA El proceso de apreciación y tratamiento de riesgos de la seguridad de la información que se presenta en esta Norma se alinea con los principios y directrices genéricas suministradas en la ISO 31000	x							x	vacio	Vacio	Vacio
			0	0	8							
	6.2 OBJETIVOS DE LA CALIDAD Y PLANIFICACION PARA LOGRARLOS							0%				
	La organización debe establecer los objetivos de seguridad de la información en las funciones v niveles relevantes.							0%				

¿Se han establecido objetivos de la calidad alcanzables para las funciones y niveles pertinentes y los procesos necesarios para el SGC, teniendo en cuenta sus requisitos legales y otros requisitos asociados, y considerando sus riesgos y oportunidades?	Los objetivos de seguridad de la información deben: a) ser coherentes con la política de seguridad de la información;					X				X	vacio	Definir objetivos de calidad claros y medibles Definir objetivos específicos de seguridad Alinear los objetivos con el resultado del análisis de riesgos y el plan de tratamiento.	Documento con los objetivos de calidad Lista de objetivos de seguridad❗ Relación con política y riesgos❗
¿Son Medibles en términos de desempeño?	b) ser medibles (si es posible);					X				X	vacio	Definir objetivos de calidad claros y medibles. Indicadores de medición y seguimiento❗	Indicadores de medición y seguimiento❗ Indicadores o métricas asociados❗
¿ Tienen en cuenta los requisitos aplicables?	c) tener en cuenta los requisitos de la seguridad de la información aplicables, y los resultados de la apreciación y del tratamiento de los riesgos;					X				X	vacio	Definir objetivos de calidad claros y medibles. Definir objetivos específicos de seguridad Alinear los objetivos con el resultado del análisis de riesgos y el plan de tratamiento.	Planes de acción vinculados. Relación con política y riesgos❗
¿Son Pertinentes para la conformidad de los productos y servicios y para el aumento de la satisfacción del cliente?						X				X	vacio	Integrar los objetivos en la gestión operativa.	Planes de acción vinculados❗
¿Son Comunicados?	d) ser comunicados; y					X				X	vacio	Comunicar los objetivos	Evidencia de comunicación❗
¿Son Actualizados, según corresponda?	e) ser actualizados, según sea apropiado.					X				X	vacio	Actualizar los objetivos cuando sea necesario	Revisión o actualización de objetivos❗
¿Se mantiene información documentada sobre los objetivos de la calidad?	f) esta como información documentada					X				X	vacio	Mantener la información documentada de los objetivos	Evidencias de la comunicación
¿Son Objeto de seguimiento?	La organización debe retener información documentada sobre los objetivos de la seguridad de la información.					X				X	vacio	Monitorear y evaluar periódicamente su avance y eficacia.	Revisión o actualización de objetivos❗
En la planificación de cómo lograr sus objetivos de la calidad, la organización:	Cuando se hace la planificación para alcanzar los objetivos de la seguridad de la información, la organización debe determinar:					X				X	vacio	Definir objetivos de calidad claros y medibles Asignar responsables, recursos y cronogramas para lograrlos.	Documento con los objetivos de calidad❗ Indicadores de medición y seguimiento❗ Actas de revisión por la dirección Planes de implementación❗
¿ Determina qué se va a hacer?	g) lo que se va a hacer;					X				X	vacio	Definir objetivos de calidad claros y medibles Asignar responsables, recursos y cronogramas para lograrlos.	Documento con los objetivos de calidad❗ Indicadores de medición y seguimiento❗ Actas de revisión por la dirección Planes de implementación❗
¿ Determina qué recursos se requerirán?	h) que recursos se requerirán;					X				X	vacio	Definir objetivos de calidad claros y medibles Asignar responsables, recursos y cronogramas para lograrlos.	Documento con los objetivos de calidad❗ Indicadores de medición y seguimiento❗ Actas de revisión por la dirección Planes de implementación❗
¿ Determina quién será responsable?	i) quién será responsable;					X				X	vacio	Definir objetivos de calidad claros y medibles Asignar responsables, recursos y cronogramas para lograrlos.	Documento con los objetivos de calidad❗ Indicadores de medición y seguimiento❗ Actas de revisión por la dirección Planes de implementación❗
¿ Determina cuándo se finalizará?	k) cuando se finalizará; y					X				X	vacio	Definir objetivos de calidad claros y medibles Asignar responsables, recursos y cronogramas para lograrlos.	Documento con los objetivos de calidad❗ Indicadores de medición y seguimiento❗ Actas de revisión por la dirección Planes de implementación❗
¿ Determina cómo se evaluarán los resultados?	l) cómo se evaluarán los resultados.					X				X	vacio	Monitorear y evaluar periódicamente su avance y eficacia. Hacer seguimiento y evaluación periódica del avance.	Documento con los objetivos de calidad❗ Indicadores de medición y seguimiento❗ Actas de revisión por la dirección
			0	0	14			0	0	14			Evidencia de seguimiento y evaluación❗
6.3. PLANIFICACIÓN DE CAMBIOS	6.3. PLANIFICACIÓN DE CAMBIOS				0%					0%			
¿Se establecen procesos, se planifican y se controlan los cambios que pueden impactar el SGC para asegurar que se logren los resultados previstos?	Cuando la organización determine la necesidad de cambios en el sistema de gestión de seguridad de la información, los cambios deben ser llevados a cabo de manera planeada.					X				X	vacio	Identificar la necesidad de cambios (procesos, procedimientos, recursos, responsabilidades, etc.) Planificar los cambios, incluyendo análisis de impacto. Evaluar los cambios propuestos (en procesos, tecnologías, controles, políticas). Identificar riesgos de seguridad asociados al cambio. Planificar el cambio considerando impacto, continuidad, recursos y responsables. Controlar la implementación del cambio. Actualizar documentación afectada.	Registros de cambios planificados❗ Análisis de impacto documentado❗ Evaluación de riesgos del cambio❗ Planificación formal del cambio❗ Controles implementados para mitigar riesgos❗ Actualización de políticas/procedimientos❗
¿ Considera el propósito de los cambios y sus consecuencias potenciales?						X	X				vacio	Identificar la necesidad de cambios (procesos, procedimientos, recursos, responsabilidades, etc.) Planificar los cambios, incluyendo análisis de impacto.	Registros de cambios planificados❗ Análisis de impacto documentado❗
¿ Considera la integridad del sistema de gestión de la calidad?						X	X				vacio	Identificar la necesidad de cambios (procesos, procedimientos, recursos, responsabilidades, etc.) Planificar los cambios, incluyendo análisis de impacto.	Registros de cambios planificados❗ Análisis de impacto documentado❗
¿ Considera la disponibilidad de recursos?						X	X				vacio	Identificar la necesidad de cambios (procesos, procedimientos, recursos, responsabilidades, etc.) Planificar los cambios, incluyendo análisis de impacto.	Registros de cambios planificados❗ Análisis de impacto documentado❗
¿ Considera la asignación o reasignación de responsabilidades y autoridades?						X	X				vacio	Comunicar y coordinar los cambios con los responsables.	Evidencia de comunicación del cambio❗ Responsables asignados❗
¿Se controlan los cambios planificados y se revisan las consecuencias de los cambios no previstos, tomando acciones para mitigar cualquier efecto adverso, según sea necesario?						X	X				vacio	Ejecutar el cambio de forma controlada. Evaluar los efectos del cambio sobre el sistema de gestión de la calidad.	Seguimiento o verificación post-cambio❗
			0	0	6			0	0	1			

RESUMEN NUMERAL ISO 27001: 2022		ISO 9001:2015
		5
		% AVANCE
6.1 ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES	6.1 ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES	0%
6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y LA PLANIFICACIÓN PARA ALCANZARLOS	6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y LA PLANIFICACIÓN PARA ALCANZARLOS	0%
6.3. PLANIFICACIÓN DE CAMBIOS	6.3. PLANIFICACIÓN DE CAMBIOS	0%
PROMEDIO AVANCE	PROMEDIO AVANCE	0%

ISO 27001:2022
% AVANCE
0%
0%
0%
0%





DIAGNÓSTICO NTC ISO 9001:2015 E ISO/IEC 27001:2022												
		ISO 9001:2015				ISO 27001:2022						
7. SOPORTE (ISO 9001:2015)		7. SOPORTE (ISO 27001:2022)										
		NO APLICA	COMPLETO	PARCIAL	NINGUNO	NO APLICA	COMPLETO	PARCIAL	NINGUNO	¿QUE TENA?	¿QUÉ NOS FALTA?	DOCUMENTOS ASOCIADOS
7.1 RECURSOS		7.1 RECURSOS										
La organización debe determinar y proporcionar los recursos necesarios para:		La organización debe determinar y proporcionar los recursos necesarios para:										
¿Se ha determinado y proporcionado los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema (económicos, infraestructura y tecnológicos)?												
el establecimiento				X				X		A pesar de que no se cuenta con un presupuesto destinado para el sistema se hacen las respectivas acciones, como: SGI: Se paga semestralmente la maestría de la directora administrativa en Calidad y gestión integral para que pueda diseñar e implementar el SGI En Recursos necesarios para la ejecución de las funciones se suministra a todos los empleados computador, microsoft 365 licenciado que permite compartir los documentos para la revisión actualización de los procesos, adicionalmente contamos con forms para desarrollo de evaluaciones y encuestas, en el mismo Microsoft se cuenta con un CRM para el área comercial que permite registra las operaciones comerciales con los clientes Contamos con antivirus licenciado, contamos con servidores virtualizados donde se encuentra la plataforma de GLPI para la solicitud, seguimiento y trazabilidad de tickets	Presupuesto con un rubro destinado para el establecimiento, implementación, mantenimiento y mejora continua del SGI Identificar los recursos necesarios para cumplir los requisitos del SGI: humanos, tecnológicos, financieros, infraestructura y documentalario	Facturas de la adquisición de dotación Factura de compra de herramientas Cuenta de cobro y pago de la persona a cargo del SGSST Formato entrega de dotación Foto del antes y después del puesto de trabajo Factura del Semestre de la Maestría de Calidad y Gestión Integral Factura del pago de Microsoft 365 Matriz de recursos por proceso (RRHH, tecnológicos, financieros, etc.).
Las capacidades y limitaciones de los recursos internos existentes?		Implementación,						X		Se cuenta con recurso humano necesario,se estableció el perfil del cargo para que cumpla con esos requisitos. Se cuenta con herramientas de monitoreo y trazabilidad que permite dar seguimiento en algunos procesos.	Cronograma y planeación de actividades para desarrollar. Identificar los recursos necesarios para cumplir los requisitos del SGI: humanos, tecnológicos, financieros, infraestructura y documentalario	Matriz de recursos por proceso (RRHH, tecnológicos, financieros, etc.).
¿Qué se necesita obtener de los proveedores externos?		mantenimiento,							X	Contamos con el formato de evaluación de proveedores y contratistas y reevaluación del mismo, en el cual están establecidos los siguientes requisitos que deben cumplir: Rut, Cámara de comercio, Propuesta comercial, cedula del representante legal, Certificado Bancario, Certificado de la ARL Indicando la implementación del SG-SST con puntaje obtenido	Requisitos a exigir a todos los proveedores externos	F-CM-01 SELECCIÓN EVALUACION PROVEEDOR Y CONTRATISTA V1 Evidencia de la competencia y capacidad del proveedor. Evidencia de controles aplicados a la seguridad de la información. Compromisos legales y contractuales firmados. Requisitos técnicos o de calidad específicos de lo entregado. Compromisos de confidencialidad, continuidad del negocio y trazabilidad.
		mejora continua del sistema de gestión de la seguridad de la información.							X		Auditorías internas Revisiones por la dirección Análisis de incidentes de seguridad Evaluaciones de cumplimiento Resultados de pruebas o controles técnicos	Registro de objetivos y metas del SGI Informes de auditorías internas Registros de no conformidad Informes de revisión por la dirección Matriz de riesgos actualizada Informes de desempeño de controles Registros de capacitación y campañas Planes de mejora continua
			0	3	0		0	3	1			
7.1.2 PERSONAS												
¿Se han determinado y proporcionado las personas necesarias para la implementación eficaz de su SGC y para la operación y control de sus procesos?												
				X		Si, se cuenta con la persona a cargo del SGI al interior de la compañía y 2 personas externas estudiantes de la maestría. Hay suficientes personas competentes para la organización y se tienen documentados los perfiles de cargo. Se cuenta con organigrama.				Definir claramente los roles que impactan en la calidad y seguridad de la información (ej. Responsable SGSI, Responsable Calidad, TI, Procesos, etc.). Determinar necesidades de personal, según la complejidad de los procesos, riesgos identificados, objetivos estratégicos y tipo de controles a implementar. Ajustar recursos humanos según cambios, nuevos proyectos, nuevas amenazas, aumento de volumen de procesos o requerimientos de partes interesadas.	Organigrama actualizado Identificación de responsables del SGI, responsables de procesos, equipos de soporte clave. Matriz de roles y responsabilidades, documento que indique quién hace qué en cada parte del SGI, incluyendo temas de calidad y seguridad. Descripción de cargos (perfiles), perfil de cada cargo con funciones y competencias requeridas, especialmente en seguridad de la información. Registros de asignación de funciones, designación formal de responsables del SGSI, oficiales de seguridad, auditores internos, comité de seguridad, etc. Evidencia de cobertura operativa, que haya suficiente personal disponible para ejecutar los procesos críticos del SGI (turnos, backups, planes de continuidad).	
			0	1	0							
7.1.3 INFRAESTRUCTURA												
¿Se determina, proporciona y mantiene la infraestructura necesaria para la operación de sus procesos y lograr la conformidad de los productos y servicios.												
				X		Equipos de cómputo y comunicación para la operación técnica y administrativa. Herramientas tecnológicas para la gestión de tickets, soporte técnico y atención al cliente. Se cuenta con hardware, software, redes, sistemas de control de acceso, conectividad, servidores, sistemas. Se mantiene y da soporte a la infraestructura. No se cuenta con infraestructura física, el trabajo se realiza de manera virtual desde casa o en donde se encuentren los clientes. Se cuenta con un inventario de los equipos de computo y celulares que se suministra a los empleados				Determinar cómo esa infraestructura soporta los requisitos de calidad y seguridad, verificar si la infraestructura permite entregar productos conformes y proteger la información (confidencialidad, integridad, disponibilidad). Monitorear fallas, tiempos fuera de línea, incidentes de seguridad o calidad causados por infraestructura inadecuada.	Inventario de infraestructura, listado de activos físicos y tecnológicos relevantes para el SGI. Registros de mantenimiento (TI), planes y reportes de mantenimiento preventivo/correctivo de equipos, redes, servidores, UPS, etc. Reportes de fallas o interrupciones, registros de eventos que afectaron la operación por fallas de infraestructura. Licencias de software y configuraciones técnicas, validación de software legal, configuraciones de seguridad, backups, firewalls. Evaluación de suficiencia de infraestructura, análisis periódico de si la infraestructura cumple con las necesidades actuales del SGI. Procedimientos de respaldo, recuperación y redundancia especialmente para ISO 27001, se espera ver cómo se protege la continuidad de la infraestructura crítica.	
			0	1	0							
7.1.4 AMBIENTE PARA LA OPERACIÓN DE LOS PROCESOS												

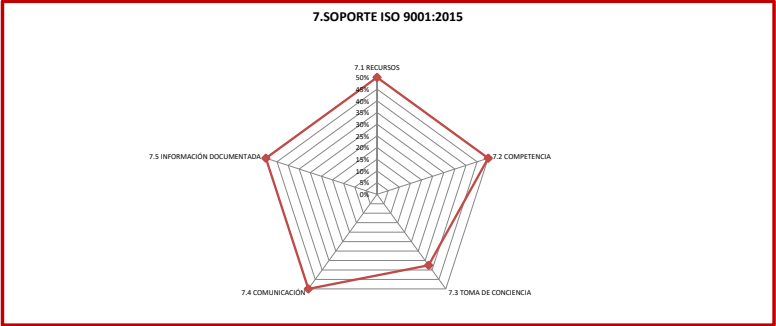
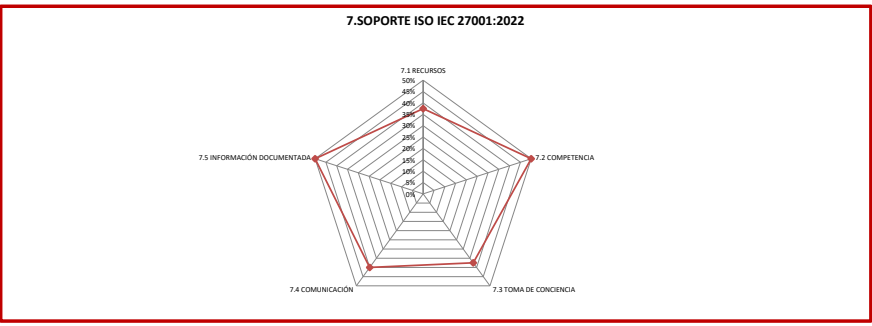
¿Se determina, proporciona y mantiene el ambiente necesario para la operación de sus procesos y para lograr la conformidad de los productos y servicios?											Condiciones físicas de trabajo: la compañía no cuenta con oficina, sin embargo suministramos escritorio y silla, según evaluación del puesto de trabajo Condiciones tecnológicas: los colaboradores cuentan con acceso a las herramientas digitales necesarias para cumplir sus funciones (correo, plataformas colaborativas, acceso remoto seguro, etc. En los valores de la compañía se promueve el trabajo en equipo "Gestión estratégica" Fotos de los encuentros Evaluación de capacitación SGSST Contamos con la batería psicológica	Asegurar que el ambiente no ponga en riesgo la seguridad de la información, evitar exposición a amenazas como accesos no autorizados, intrusiones, daños a infraestructura crítica o manipulación indebida de información. Verificar el ambiente en áreas críticas, asegurar que zonas donde se maneja información sensible tengan controles adecuados (ambiente físico seguro, limitado y controlado). Monitorear condiciones del ambiente, uso de registros de temperatura, humedad, sistemas de alarma, monitoreo de acceso, protocolos de orden y aseo, etc.	Política o procedimiento de ambiente de trabajo Controles de acceso Condiciones adecuadas en áreas de trabajo (limpieza, ergonomía, ventilación) Zonas seguras o restringidas para activos de información (servidores, archivos) Mantenimiento de condiciones ambientales críticas (UPS, aire acondicionado, sensores) Cultura organizacional que promueve orden, disciplina y confidencialidad
			0	1	0								
7.1.5.1 RECURSOS DE SEGUIMIENTO Y MEDICIÓN			0%						0%				
¿Se determina, proporciona y mantiene el ambiente necesario para la operación de sus procesos y para lograr la conformidad de los productos y servicios?		X								NO APLICA	NO APLICA	NO APLICA	
La organización se asegura que los recursos:		X								NO APLICA	NO APLICA	NO APLICA	
¿Son apropiados para el tipo específico de actividades de seguimiento y medición realizadas?		X								NO APLICA	NO APLICA	NO APLICA	
¿Se mantienen para asegurarse de la idoneidad continua para su propósito?		X								NO APLICA	NO APLICA	NO APLICA	
¿Se conserva la información documentada apropiada como evidencia de que los recursos de seguimiento y medición son idóneos para su propósito?		X								NO APLICA	NO APLICA	NO APLICA	
			0	0	0					NO APLICA	NO APLICA	NO APLICA	
7.1.5.2 TRAZABILIDAD DE LAS MEDICIONES			0%							NO APLICA	NO APLICA	NO APLICA	
¿Se calibran o verifican, o ambas , a intervalos especificados, o antes de su utilización, contra patrones de medición trazables a patrones de medición internacionales o nacionales?		X								NO APLICA	NO APLICA	NO APLICA	
¿Cuando no existen tales patrones, se conserva como información documentada la base utilizada para la calibración o la verificación?		X								NO APLICA	NO APLICA	NO APLICA	
¿Se identifican para determinar su estado?		X								NO APLICA	NO APLICA	NO APLICA	
¿Se protegen contra ajustes, daño o deterioro que pudieran invalidar el estado de calibración y los posteriores resultados de la medición?		X								NO APLICA	NO APLICA	NO APLICA	
¿Se determina si la validez de los resultados de medición previos se ha visto afectada de manera adversa cuando el equipo de medición se considere no apto para su propósito previsto?		X								NO APLICA	NO APLICA	NO APLICA	
			0	0	0								
7.1.6 CONOCIMIENTOS DE LA ORGANIZACIÓN			50%										
¿Se han determinado los conocimientos necesarios para la operación de sus procesos y para lograr la conformidad de los productos y servicios?				X						Contamos con los perfiles de cargo, donde se definen las competencias y conocimientos mínimos necesarios para cada rol La formación continua del personal, con énfasis en herramientas tecnológicas, el personal de soporte TI se capacita en Fortinet, Trellix, Kaspersky, Acronis, Microsoft enfocados a soporte técnico y el área comercial también se capacita en los mismo fabricantes pero enfocado a ventas. En cuanto a capacitación de atención al cliente, se trabajan actividades de habilidades blandas El seguimiento de fuentes externas, como normativas vigentes, guías de buenas prácticas ITIL, requerimientos del cliente y avances del sector IT. M-RH-01 MANUAL DE FUNCIONES Y PERFIL GERENTE GENERAL V1 M-RH-02 MANUAL DE FUNCIONES Y PERFIL DIRECTOR ADMINISTRATIVO V1 M-RH-03 MANUAL DE FUNCIONES Y PERFIL DIRECTOR COMERCIAL V1 M-RH-04 MANUAL DE FUNCIONES Y PERFIL EJECUTIVO B2B V1 La RH tiene MANUAL DE FUNCIONES Y PERFIL MANUAL DE PROCEDIMIENTOS	Procedimientos, instructivos y formatos, que permitan documentar y transferir el conocimiento Documentar las capacitaciones y su periodicidad que tienen que desarrollar en cuanto a los fabricantes de productos y servicios que ofrecemos, sin embargo, se ejecuta en los primeros 5 meses	Matriz de conocimientos críticos, identifica qué conocimiento es clave por proceso, quién lo posee y cómo se mantiene. Manuales, instructivos, guías internas, documentos accesibles al personal y actualizados (producción, TI, SGS, seguridad física). Sistema de gestión documental, donde esté organizado y controlado el conocimiento interno.	
¿Estos conocimientos se mantienen y se ponen a disposición en la medida en que sea necesario?				X						Capacitaciones de inducción y refuerzo, donde se transfiera conocimiento clave a nuevos colaboradores o en casos de cambio de proceso Gestión de la información en herramientas digitales, como bases de datos, historiales técnicos. Las sesiones de capacitación de inducción ya se graban, se entregan un manual de onboarding el cual señalan los temas vistos y firman de recepción de la información, también se evalúa a través de la plataforma Forms Se cuenta con un video del manejo de GLPI y manual necesarios para el desarrollo de sus funciones	Matriz de competencias, que identifica qué conocimientos se deben mantenerse actualizados por cada cargo Falta desarrollar reuniones periódicas por área, donde se puedan compartir actualizaciones, buenas prácticas y que se asegure que el equipo esté alineado y así mismo generar actas o informes para hacer seguimiento.	Planes de transferencia de conocimiento, en caso de reemplazos, rotación o proyectos especiales. Procedimientos de formación e inducción, donde se aborde conocimiento técnico, de calidad y seguridad.	
¿Cuando se abordan las necesidades y tendencias cambiantes, se consideran sus conocimientos actuales y determina cómo adquirir o acceder a los conocimientos adicionales necesarios y a las actualizaciones requeridas?				X						Análisis de contexto y partes interesadas, en donde se identifiquen cambios tecnológicos, regulatorios o del sector que puedan afectar nuestros servicios. Los fabricantes de las marcas que vendemos nos permiten estar actualizados, convocan a actividades para promover nuevas actualizaciones y en este tiempo el uso de la IA como herramienta a favor Cuando se requiere conocimiento especializado no disponible internamente, se recurre a consultoría externa, fabricantes que poseen el conocimiento requerido	Matriz de competencias, que se debe actualizar en función de nuevos requerimientos técnicos o estratégicos No se tiene documentando las capacitaciones que desarrolla los fabricantes, tampoco evidencia fotográfica o una lista de asistencia Matriz de brechas de conocimiento (antes y después de un cambio) Matriz de competencias por cargo ante nuevos servicio. Incluir conocimiento clave de calidad y seguridad, instrucciones de trabajo, configuración de controles, gestión de riesgos, lecciones aprendidas.	Acciones tomadas tras incidentes/no conformidades, que reflejen aprendizaje organizacional y actualización de procedimientos.	
			0	1	0								
7.2 COMPETENCIA	7.2 COMPETENCIA		50%						50%				
La organización debe:	La organización debe:												

<i>¿Se cuenta con la información documentada requerida por esta Norma Internacional?</i>	a) la información documentada requerida por esta Norma; y		x		x	Para el SGC se ha desarrollado documentos que nos permiten tener avances para la implementación. Para el sistema de la información se han desarrollado PDES que nos permiten desarrollar a nivel de Soporte T1 L-GC-01 LISTADO MAESTRO DE REGISTROS V1	Establecer una estructura documental del SGI, Manual (opcional), políticas, procedimientos, formatos, instructivos, registros. Unificar documentos comunes a ambos sistemas, por ejemplo: gestión de riesgos, control de cambios, auditoría, capacitación, compras.	Política del SGI (calidad + seguridad) Objetivos del sistema Procedimientos documentados? Planes de tratamiento de riesgos? Registros de auditoría? Control de cambios y versiones? Registro de acceso y control documental?
<i>¿Se cuenta con la información documentada que la organización determina como necesaria para la eficacia del SGC?</i>	b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.		x		x	La documentación que se ha desarrollado hasta al momento es porque se ha necesitado, decayendo a cada una de las áreas, está pendiente el desarrollo Área residual de apoyo Soporte T1 al interior de la compañía L-GC-01 LISTADO MAESTRO DE REGISTROS V1	Establecer una estructura documental del SGI, Manual (opcional), políticas, procedimientos, formatos, instructivos, registros. Unificar documentos comunes a ambos sistemas, por ejemplo: gestión de riesgos, control de cambios, auditoría, capacitación, compras.	Política del SGI (calidad + seguridad) Objetivos del sistema Procedimientos documentados? Planes de tratamiento de riesgos? Registros de auditoría? Control de cambios y versiones? Registro de acceso y control documental?
	NOTA: El alcance de la información documentada para un sistema de gestión de la seguridad de la información puede ser diferente de una organización a otra, debido a: a) el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios, b) la complejidad de los procesos y sus interacciones, y c) la competencia de las personas.				x	Se ha desarrollado procedimientos, manuales, formatos, listas, cronogramas según los procesos que se tienen a la fecha, se ha adelantado en su elaboración, falta comunicarlos y limitar su alcance de manejo	No se tiene establecido el alcance del SGI	Política del SGI (calidad + seguridad) Objetivos del sistema Procedimientos documentados? Planes de tratamiento de riesgos? Registros de auditoría? Control de cambios y versiones? Registro de acceso y control documental?
		0	2	0	0	2	0	
7.5.2 Creación y actualización	7.5.2 Creación y actualización							
Cuando se crea y actualiza información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:	Cuando se crea y actualiza información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:		100%		100%			
<i>¿Se asegura la identificación y descripción de la información documentada (por ejemplo, título, fecha, autor o número de referencia)?</i>	a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);		x		x	Los documentos que se han desarrollado cuentan con codificación (código, fecha, versión) cuenta con el título del documento y también cuenta con un control de cambios, adicionalmente con el logo de la compañía	Identificación de documentos, asignar código, título, fecha, versión, responsable, a todos los documentos del SGI	Registro de acceso y control documental?
<i>¿Se asegura el formato (por ejemplo, idioma, versión del software, gráficos) y los medios de soporte (por ejemplo, papel, electrónico)?</i>	b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);		x		x	Se cuenta con una lista de documentos elaborados hasta la fecha en el sistema se tiene la versión, la ubicación, en qué medio se tiene L-GC-01 LISTADO MAESTRO DE REGISTROS V1	Definir formato y medio adecuado, PDF, digital editable, impreso; repositorio en red, nube, SharePoint, etc., para todos los documentos del SGI	
<i>¿Se asegura la revisión y aprobación de la información documentada con respecto a la conveniencia y adecuación?</i>	c) la revisión y aprobación con respecto a la idoneidad y adecuación.		x		x	Para este caso los documentos tienen un "diagrama o cuadro" que está compuesto por quien elabora, revisa y aprueba, en el cual deben registrar	Establecer responsables de revisión y aprobación, todo documento debe ser verificado y autorizado antes de usarse	
		0	2	0	0	2	0	
7.5.3 Control de la información documentada	7.5.3 Control de la información documentada							

La información documentada requerida por el sistema de gestión de la calidad y por esta Norma internacional se debe controlar para asegurarse de que:	La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta Norma se debe controlar para asegurarse de que:			ISO				ISO				
a) ¿Se asegura que la información documentada esté disponible y sea idónea para su uso, donde y cuándo se necesite?	a) esté disponible y adecuada para su uso, donde y cuando se necesite; y			x				x		La documentación se encuentra disponible en el onedrive de la empresa, lista para compartir con todos los usuarios de la organización y con la limitación de acceso. En este momento sólo tiene acceso los líderes de cada área.	Definir los perfiles que se van a limitar los accesos y compartir la información con los usuarios	Lista maestra con estado de los documentos vigentes, obsoletos, en revisión.
b) ¿Se asegura que la información documentada esté protegida adecuadamente (contra pérdida de la confidencialidad, uso inadecuado o pérdida de integridad)?	b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).			x				x		La documentación solamente se encuentra disponible para la organización y limitada con permisos de acceso, en el cual se puede verificarlos controles de cambios y así mismo quién puede acceder a la información, si solo lo puede visualizar, o modificar. P-ST-03 Respaldo y Restauración de Datos V1	Tener backup de la información en otras plataformas como la nube, discos externos y servidores locales, y adicionalmente se tendría que estipular la frecuencia en que se hace los backup y quien tendría acceso a esa información A pesar de que se tiene el documento elaborado aún no se ha desarrollado su implementación y por tanto no se ha comunicado, adional a esto falta la adquisición de dichos recursos	
c) ¿Se definen actividades de distribución, acceso, recuperación y uso?	Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable: c) distribución, acceso, recuperación y uso;			x				x		La documentación se podría recuperar ya que la plataforma que lo almacena permite esa acción Se cuenta con un procedimiento que define el respaldo y restauración de los datos	No se tiene establecido un procedimiento en el cual especifique la distribución de la información, sin embargo, el área de soporte tiene definido de manera verbal su distribución, en cuanto a los accesos, esta está limitada de acuerdo a los cargos , pero no se cuenta documentado	Procedimiento de control documental, indica cómo se gestiona el ciclo de vida de los documentos. Registros de acceso o permisos (digitales), Logs, capturas, plataformas como SharePoint, Drive, NAS, etc.
d) ¿Se definen actividades de almacenamiento y preservación, incluida la preservación de la legibilidad?	d) almacenamiento y preservación, incluida la preservación de la legibilidad;			x				x		La información como documentos, procedimientos, cronogramas, etc, se encuentra almacenada en Share point y está se definió de manera verbal y toda la información referente a la compañía se debe almacenar allí La compañía no maneja documentos en físico, sino que todo se maneja de manera digital, lo que permite mantener legibilidad de los mismos, además que para la elaboración de documentos se tiene establecido como se deben elaborar P-ST-03 Respaldo y Restauración de Datos V1 P-SGI-01 PROCEDIMIENTO PARA LA ELABORACIÓN DE DOCUMENTOS V1	No se tienen establecidos un documento de almacenamiento donde se establezca que se debe almacenar y con que mecanismo se va a respaldar y la frecuencia del mismo. A pesar de que contamos con la plataforma GLPI no se cuenta con el backup de la información contenida No se cuenta con procedimiento para el almacenamiento Establecer reglas para almacenamiento y respaldo	Controles de respaldo y recuperación, procedimientos de backup, evidencias de pruebas de restauración.
e) ¿Se definen actividades de control de cambios (por ejemplo, control de versión)?	e) control de cambios (por ejemplo, control de versión); y			x				x		En el procedimiento para la elaboración de documentos se tiene establecido que para los documentos este tiene un control de cambios el cual contiene la siguiente información: Versión, la descripción y la fecha. P-SGI-01 PROCEDIMIENTO PARA LA ELABORACIÓN DE DOCUMENTOS V1	Controlar cambios y versiones de los documentos del SGI, toda modificación debe quedar registrada. Evitar el uso de versiones obsoletas.	
f) ¿Se definen actividades de conservación y disposición?	f) retención y disposición.			x				x		En el procedimiento para la elaboración de documentos, se ha definido una matriz de tiempos de conservación para cada tipo de documento (interno, externo y contable), estos también están sujetos a los requisitos legales o contractuales y están almacenados en Share Point. A pesar que no existe un documento de soporte, la información se encuentra clasificada, se protege mediante antivirus, contraseñas robustas para acceder al share point, doble autenticación. Con nuestros clientes se firman contratos de confidencialidad de la información y se establece el tiempo y con el personal interno en sus contratos se establece la confidencialidad de la información bajo cláusulas.	En el procedimiento que se tiene definido no tiene el alcance para seguridad de la información por ende no se desarrolla: clasificación de la información, protección, integridad, disponibilidad y confidencialidad durante el tiempo definido, adicionalmente se ve en la necesidad de dividir o desarrollar un procedimiento para este propósito No existe un formato para el registro de eliminación de documentos sensibles o información clasificada Definir tiempos de retención y disposición, ¿Cuánto tiempo conservar cada documento y cómo eliminarlo de forma segura.	Políticas de conservación y eliminación, basadas en requisitos legales, contractuales o normativos. Evidencia de destrucción segura de documentos, certificados, registros de eliminación (papel o digital).
g) ¿Se identifica y controla la información documentada de origen externo?	La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión de la seguridad de la información, se debe identificar y controlar, según sea adecuado.			x				x		Se cuenta con los contratos, en el cual está establecida su durabilidad y los responsables asignados. Se cuenta con manuales técnicos suministrados por los proveedores	No se cuenta con una matriz que permita el acceso a información de manera puntual con relación a los contratos No se cuenta con un listado o inventario del manuales No se cuenta con un listado de normas vigentes, donde se pueda evidenciar una breve descripción, la vigencia y otra información de valor a considerar Proteger la información sensible	
h) ¿Se protege contra modificaciones no intencionadas, la información documentada conservada como evidencia de la conformidad?	NOTA El acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.			x				x		Los registros son almacenados en repositorios digitales con control de acceso basado en roles (solo lectura para la mayoría de usuarios, permisos de edición restringidos)	No se realiza un respaldo automático periódico de los registros críticos, evitando la pérdida o corrupción accidental No se cuenta con una Política de clasificación de la información, matriz de activos, bitácoras de modificación o eliminación No se cuenta con backup adicionales, ni un cronograma cuál es la frecuencia de respaldo un documento donde se registre la trazabilidad (fecha, usuario, motivo), especialmente en documentos sujetos a control de versiones	
			0	0	0		0	0	0			

ISO 9001		
RESUMEN NUMERAL ISO 27001: 2022	RESUMEN NUMERAL ISO 9001:2015	% AVANCE
7.1 RECURSOS	7.1 RECURSOS	38%
7.2 COMPETENCIA	7.2 COMPETENCIA	50%
7.3 TOMA DE CONCIENCIA	7.3 TOMA DE CONCIENCIA	38%
7.4 COMUNICACIÓN	7.4 COMUNICACIÓN	50%
7.5 INFORMACIÓN DOCUMENTADA	7.5 INFORMACIÓN DOCUMENTADA	50%
PROMEDIO AVANCE	PROMEDIO AVANCE	46%

ISO 27001	
	% AVANCE
	38%
	50%
	38%
	40%
	50%
	43%



[illegible]

¿Se establecen criterios para la aceptación de los productos y servicios?					X						Se identificó que la organización realiza cotizaciones personalizadas según las necesidades del cliente y mantiene comunicación comercial mediante un CRM básico, lo que permite entender e incorporar ciertos requisitos explícitos durante el proceso de negociación. Además, se cuenta con una página web corporativa donde se describen los servicios que ofrece la empresa.	Procedimientos o formatos documentados que permitan estandarizar la recolección, verificación y validación de los requisitos antes de emitir una oferta formal.	Diseñar una plantilla de levantamiento de requisitos. Incluir revisión y aprobación interna previa a la cotización. Formalizar la aceptación de requisitos con el cliente mediante firma o validación por correo/documento
Cuando se determinan los requisitos para los productos y servicios que se van a ofrecer a los clientes, la organización se asegura de que:					X						La organización realiza cotizaciones personalizadas y mantiene comunicación con los clientes a través de su CRM. Sin embargo, no se identifican mecanismos formales para asegurar y documentar que, al determinar los requisitos, se verifiquen todos los aspectos exigidos por la norma, tales como: Requisitos del cliente están claramente definidos: Se abordan de manera informal, pero no existe una plantilla ni formato estandarizado que permita registrar de forma sistemática todos los requisitos.	Requisitos no establecidos por el cliente pero necesarios para el uso previsto o especificado: No se evidencia análisis formal que permita anticiparse a necesidades técnicas u operativas que el cliente no declare explícitamente. Requisitos legales y reglamentarios aplicables: No se identificó ningún mecanismo que garantice la verificación de requisitos normativos, contractuales o de cumplimiento aplicables a los servicios. La capacidad para cumplir con los requisitos definidos: No existe evidencia de un proceso formal de revisión técnica, operativa o de recursos antes de aceptar un contrato o compromiso.	
¿Los requisitos para los productos y servicios se definen, incluyendo: Cualquier requisito legal y reglamentario aplicable;					X						La organización define parcialmente los requisitos para productos y servicios, especialmente a través de las cotizaciones personalizadas y contratos firmados con los clientes. En dichos contratos, se identificó la inclusión de cláusulas de confidencialidad y tratamiento de datos, lo cual constituye una evidencia válida de atención a los requisitos legales relacionados con la protección de la información. Asimismo, se verificó que la organización cuenta con una política de tratamiento de datos publicada en su página web, alineada con los lineamientos de la legislación nacional vigente (Ley 1581 de 2012 y normas complementarias en Colombia), lo que fortalece el cumplimiento de requisitos legales frente a protección de datos personales.	Listas de chequeo, procedimientos o matrices formales para identificar y verificar el cumplimiento de otros requisitos legales o reglamentarios aplicables a productos o servicios específicos (por ejemplo: licencias de software, normas técnicas, continuidad del servicio, normativas del cliente por sector, etc.).	Desarrollar una matriz de requisitos legales por tipo de servicio o sector del cliente. Incluir revisión legal en la fase de diseño o cotización. Ampliar las cláusulas contractuales según el riesgo regulatorio del servicio.
Aquellos considerados necesarios por la organización;					X						Actualmente, la organización realiza cotizaciones personalizadas y establece condiciones en los contratos con los clientes, lo cual demuestra cierto nivel de análisis de requisitos más allá de lo solicitado directamente	Procedimiento o metodología formalizada que permita identificar y documentar requisitos adicionales que, aunque no sean expresamente requeridos por el cliente, la organización considere necesarios para asegurar la calidad o la seguridad del servicio. Tampoco se evidencian criterios internos que permitan justificar la inclusión de estos requisitos adicionales (por ejemplo: buenas prácticas técnicas, tiempos mínimos de entrega, exigencias internas de respaldo o continuidad, compatibilidad tecnológica, requisitos de seguridad, etc.).	
¿Pueda cumplir con las declaraciones acerca de los productos y servicios que ofrece?					X						La organización presenta sus productos y servicios a través de su página web, y realiza cotizaciones personalizadas acompañadas de contratos firmados, lo cual permite establecer un marco básico de cumplimiento de lo que se promete al cliente.	Identificar mecanismos documentados de revisión previa, ni registros que demuestren que las declaraciones comerciales (como tiempos de atención, niveles de servicio, cobertura técnica) han sido validadas técnicamente antes de ser ofrecidas. Tampoco se evidencia una metodología de análisis de capacidad operativa para confirmar que lo ofrecido puede cumplirse de manera consistente, ni un proceso que alinee lo prometido comercialmente con lo que puede ejecutar el equipo técnico u de soporte.	
8.2.3.1 Revisión de los requisitos para los productos y servicios				0	5	0							
					17%								
¿Se aseguran de tener la capacidad de cumplir los requisitos para los productos y servicios que se van a ofrecer a los clientes.?					X						La organización realiza un análisis previo de viabilidad y capacidad para la prestación de servicios y entrega de productos, el cual contempla variables como el anticipo del cliente, la asignación de recursos técnicos, y la disponibilidad de personal. Este análisis es gestionado a nivel de dirección y forma parte del proceso interno de toma de decisiones antes de comprometerse contractualmente.	Aunque esta revisión existe, no está formalizada en un formato estandarizado, ni es accesible para otras áreas, lo que dificulta su trazabilidad, mejora y evaluación en futuras auditorías internas. Se recomienda: Formalizar este análisis mediante un formato estándar. Definir criterios objetivos de capacidad técnica, económica y operativa. Incluir esta revisión como parte obligatoria del flujo comercial.	
¿Se revisa antes de comprometerse a suministrar productos y servicios a un cliente, que incluye:					X						La organización realiza una validación previa de viabilidad antes de cerrar acuerdos comerciales, que contempla variables operativas y condiciones contractuales clave. Esta revisión es gestionada directamente por la alta dirección, con base en criterios no documentados formalmente ni estructurados en formatos accesibles.	Evidencia documentada que permita verificar que dicha revisión incluye de manera sistemática los tres aspectos exigidos por la norma: Requisitos definidos por el cliente: Parcialmente cubiertos en cotizaciones y contratos. Requisitos no establecidos por el cliente pero necesarios para el uso previsto: No se evidencia análisis técnico formal que contemple esta dimensión. Capacidad de la organización para cumplir con los requisitos: Se evalúa de forma interna, pero sin registros ni formatos estandarizados. Aspectos conformes (limitados): Existen validaciones previas a la emisión de contratos y cotizaciones. Se documentan condiciones clave (como tiempos o alcance) en los contratos. Mecanismo formal o sistemático para registrar, verificar o documentar los requisitos relacionados con actividades posteriores a la entrega, como: instalación o configuración técnica. Soporte postventa o mantenimiento. Garantías. Indicadores de seguimiento o puntos de control definidos con el cliente. Tampoco se identifican fichas de requisitos o formatos donde se centralice toda esta información por cliente, lo que limita la trazabilidad y el cumplimiento consistente de las expectativas acordadas.	
¿Los requisitos especificados por el cliente, incluyendo los requisitos para las actividades de entrega y las posteriores a la misma?					X						La organización documenta ciertos requisitos del cliente a través de cotizaciones personalizadas y contratos, los cuales incluyen condiciones de pago, alcance del servicio y entrega de productos. También se realizan actas de entrega firmados por el cliente, lo que constituye evidencia válida del cumplimiento del proceso de entrega.	Procedimiento documentado ni con un formato específico que permita identificar y revisar los requisitos no solicitados directamente por el cliente, pero que son fundamentales para que el servicio o producto funcione adecuadamente. Si bien se cuenta con experiencia técnica en el equipo de trabajo y con ciertos criterios que se aplican de manera operativa, no se evidencia que estos requisitos adicionales se analicen de manera sistemática o se documenten antes de comprometerse con el cliente. Esto representa un riesgo de omitir aspectos críticos como: Compatibilidad técnica. Condiciones mínimas de infraestructura del cliente. Requisitos operativos u de seguridad separados para un uso funcional.	
¿Los requisitos no establecidos por el cliente, pero necesarios para el uso especificado o previsto, cuando sea conocido?						X							
¿Los requisitos especificados por la organización?						X							procedimientos, políticas, formatos
¿Los requisitos legales y reglamentarios aplicables a los productos y servicios?						X						Proceso estructurado para identificar, revisar y cumplir con todos los requisitos legales y reglamentarios aplicables a los productos y servicios. Esto representa un riesgo de incumplimiento, especialmente ante clientes de sectores regulados. Mecanismo formal ni documentado para revisar y registrar las diferencias que puedan existir entre los requerimientos inicialmente expresados por el cliente (por ejemplo, durante la cotización o consulta) y los finalmente establecidos en el contrato o pedido. Aunque estas situaciones se manejan operativamente por el equipo comercial y la alta dirección, no se evidencian registros de validación de cambios, actas de conformidad o versiones comparativas entre lo solicitado y lo acordado, lo que conlleva asegurar trazabilidad y cumplimiento con este requisito.	procedimientos, políticas, formatos
¿Las diferencias existentes entre los requerimientos del contrato o pedido y los expresados previamente?						X							procedimientos, políticas, formatos

¿La competencia, incluyendo cualquier calificación requerida de las personas?						X							En la organización no se evidencian mecanismos formales que aseguren que los proveedores externos o contratistas sean informados sobre los requisitos de competencia o calificación exigidos para las personas que prestan los servicios contratados (por ejemplo, técnicos, operadores de instalación, personal de soporte subcontratado). Aunque en la práctica se trabaja con proveedores de confianza y se espera que el personal asignado cuente con la experiencia necesaria, no se comunican explícitamente los requisitos de competencia (certificaciones, experiencia mínima, formación específica), ni se solicita evidencia de los mismos antes de la prestación del servicio. Tampoco se encontró documentación que indique: Qual competencias deben tener las personas que intervienen en nombre del proveedor. Que esta información se comunique de manera estructurada (ej. cláusula en contrato, anexo técnico). <i>Que se considere evidencia de que el proveedor cumple con estas exigencias</i>	Documentos de actividades críticas (experiencia, certificaciones, etc) Registro de informes y experiencia del proveedor	
¿Las interacciones del proveedor externo con la organización?						X							En la organización, no se evidencia un mecanismo formal y estructurado para comunicar a los proveedores externos cómo deben interactuar con Berrut durante la prestación del servicio, ejecución del contrato o entrega del producto. Las interacciones ocurren de forma operativa, a través de correos, llamadas o conversaciones directas, pero no están estandarizadas ni definidas previamente en términos de: Canales oficiales de comunicación, Responsables designados por ambas partes, Momentos de interacción requeridos (ej. informes, avances, entregas, validaciones). <i>Documentación o reportes a presentar en cada fase.</i>		
¿El control y el seguimiento del desempeño del proveedor externo a aplicar por parte de la organización?						X							La organización cuenta con un procedimiento y un formato de evaluación de proveedores, lo cual representa una base documental para controlar el desempeño de terceros. Sin embargo, no se evidenció que dicha información se comunique a los proveedores externos, ni en los contratos ni en correos electrónicos formales. Tampoco se encontraron registros de: Indicadores de desempeño comunicados al proveedor (ej. cumplimiento de tiempos, calidad, soporte posventa). Retroalimentaciones estructuradas o informes de desempeño compartidos. Notificaciones o advertencias documentadas en caso de bajo desempeño. En la práctica, las decisiones sobre continuar o no con un proveedor se basan en la experiencia directa del equipo y en la satisfacción general, sin trazabilidad.		
¿Las actividades de verificación o validación que la organización, o su cliente, pretende llevar a cabo en las instalaciones del proveedor externo?						X							<i>Alinea al criterio comunicado.</i> Actualmente, la organización no cuenta con evidencia documentada que indique que se comuniquen actividades de verificación o validación a realizar en las instalaciones del proveedor externo, ni por parte de Berrut ni de sus clientes. Aunque en algunos casos se realizan visitas técnicas o validaciones funcionales antes de recibir productos o servicios, estas actividades: No están documentadas como parte de un plan de verificación. No se informan previamente al proveedor como un requisito o parte del proceso. No se registran como parte del control formal. Tampoco se evidencian cláusulas contractuales, anexos técnicos o correos que establezcan este tipo de interacciones presenciales como parte de los términos de referencia.		
				0	2	5									
8.5 PRODUCCIÓN Y PROVISIÓN DEL SERVICIO						32%									
8.5.1 Control de la producción y de la provisión del servicio						28%									
¿Se implementa la producción y provisión del servicio bajo condiciones controladas?						X							En la organización, la provisión de servicios (particularmente en soporte TI interno y externo) se realiza de manera funcional, pero no en un marco formal de condiciones controladas según lo requerido por la norma. Aunque se cuenta con: Una plataforma de tickets (GLP) que permite seguimiento a las solicitudes de soporte. Planes de trabajo puntuales para mantenimientos correctivos cuando estos se requieren. <i>Informes técnicos que se elaboran al finalizar ciertas actividades.</i>	No se cuenta con procedimientos estandarizados que regulen la provisión del servicio, ni con instrucciones de trabajo, criterios de aceptación documentados, ni registros sistemáticos que aseguren trazabilidad del cumplimiento bajo condiciones controladas.	
Las condiciones controladas incluyen, cuando aplica: La disponibilidad de información documentada que defina: Las características de los productos a producir, los servicios a prestar, o las actividades a desempeñar y los resultados a alcanzar?						X							En la organización, no se cuenta con información documentada estandarizada que defina formalmente las características de los productos, los servicios prestados o los resultados que deben alcanzarse en cada actividad. Aunque se maneja un sitio web con información comercial de productos y servicios, cotizaciones personalizadas y contratos que definen condiciones de entrega y alcance, no se identificaron procedimientos, instrucciones técnicas o fichas de servicio que detallen de forma sistemática: Las características técnicas o funcionales mínimas de cada servicio. Los objetivos o resultados esperados por tipo de actividad (ej. resolución de incidente, instalación, mantenimiento, etc.). <i>Criterios de aceptación, acciones a tomar y validaciones intermedias.</i>		
La disponibilidad y el uso de los recursos de seguimiento y medición adecuados;						X							En Berrut, existen herramientas que permiten cierto nivel de seguimiento y medición, especialmente en el área de soporte TI, tales como: La plataforma GLP, que permite registrar tickets, medir tiempos de respuesta y resolución, y generar reportes mensuales. La herramienta Centreon, que monitorea en tiempo real el estado de la red, los servidores, los respaldos, entre otros aspectos críticos.	Sin embargo, no se cuenta con una metodología formal ni con registros sistemáticos que evidencien que estos recursos se usan de manera estructurada como parte del sistema de gestión de calidad, ni para establecer indicadores, límites, alertas o verificaciones regulares de desempeño. Tampoco se evidencian recursos de medición aplicados en otras áreas como comercial, compras, recursos humanos o gestión estratégica, ni unificación de criterios de seguimiento de desempeño en la prestación del servicio.	Indicadores de trazabilidad Formatos de soporte técnico Informes
La implementación de actividades de seguimiento y medición en las etapas apropiadas para verificar que se cumplen los criterios para el control de los procesos o sus salidas, y los criterios de aceptación para los productos y servicios;						X							En Berrut, se realizan algunas actividades operativas que permiten monitorear procesos y verificar resultados, principalmente en soporte TI. Esto incluye: El uso de GLP para registrar tickets, hacer seguimiento a tiempos de respuesta, y verificar el cierre. El uso de Centreon para monitorear en tiempo real el estado de infraestructura crítica (redes, backups, servidores). Sin embargo, no se cuenta con criterios de control formalmente definidos ni con criterios de aceptación documentados por tipo de servicio. Tampoco se identifican etapas de verificación predefinidas ni responsables asignados que realicen una validación sistemática y registrada. En los procesos comerciales, de compras, recursos humanos y gestión estratégica, no se encontraron evidencias de seguimiento y medición estructurada, ni de etapas establecidas para validar el cumplimiento del proceso o el resultado.		

El uso de la infraestructura y el entorno adecuados para la operación de los procesos;												La organización dispone de infraestructura básica adecuada para la operación de sus procesos, en especial para los servicios de soporte TI interno y externo. Esta infraestructura incluye: Equipos de cómputo operativos, Servidores y redes bajo monitoreo con Centreon, UPS adquiridos por los clientes para proteger infraestructura crítica. Uso de OneDrive para respaldo de documentos, Plataformas como GLP y CRM básico que apoye procesos clave. Además, algunos contratos con clientes establecen condiciones mínimas para garantizar el entorno operativo (como respaldo de energía, backups, monitoreo).	Sin embargo, no se evidencian registros o controles sistemáticos que verifiquen la adecuación y mantenimiento preventivo de la infraestructura, ni se ha definido un entorno físico, tecnológico o de trabajo deseado por proceso.		
La designación de personas competentes, incluyendo cualquier calificación requerida;												En la organización se identificó que la designación de personal técnico operativo se realiza con base en el conocimiento práctico y la experiencia de los colaboradores, lo cual ha demostrado ser funcional para el desarrollo de las actividades. Se cuenta con manuales de funciones para cargos como Analista IT y Auxiliar Técnica, sin embargo, dichos documentos requieren actualización, particularmente en lo relacionado con las competencias requeridas, criterios de calificación y responsabilidades actuales. Adicionalmente, se evidenció que la empresa gestiona formación técnica con apoyo de sus mayoristas, quienes brindan capacitaciones orientadas a certificaciones en las marcas que comercializa. Esta iniciativa representa una fortaleza importante en la gestión del conocimiento técnico.	No obstante, no se cuenta con una matriz de competencias, registros sistemáticos de la formación recibida, ni evidencia formal que vincule dicha formación con la validación o designación del personal para funciones específicas. Actualmente, no se documenta la evaluación de competencias antes de asignar un rol, ni se conserva información que permita demostrar que el personal designado cumple con las calificaciones mínimas requeridas.	actualización de perfil profesional matriz de competencias Registro de formación técnica	
La validación y revalidación periódica de la capacidad para alcanzar los resultados planificados de los procesos de producción y de prestación del servicio, cuando las salidas resultantes no puedan verificarse mediante actividades de seguimiento o medición posteriores;												En la organización, no se identificó evidencia de que se realicen procesos formales de validación ni revalidación periódica de la capacidad de los procesos cuando los resultados no pueden verificarse completamente mediante medición posterior. Si bien existen herramientas como GLP para seguimiento de tickets y Centreon para monitoreo técnico, estas no cubren todos los procesos ni garantizan la trazabilidad completa de los resultados esperados en cada caso. Por ejemplo: En soporte TI, no se definen claramente los resultados planificados por tipo de intervención, y no hay criterios documentados de aceptación o verificación funcional sistemática. En proyectos o configuraciones críticas, no se evidencia que se valide por adelantado que el procedimiento técnico o recurso asignado puede garantizar el cumplimiento de requisitos, ni que se haga una revalidación periódica del mismo. Tampoco existen registros de validación previa a la prestación del servicio, especialmente en servicios personalizados o críticos, donde el error no se puede detectar fácilmente después (por ejemplo, configuraciones mal aplicadas, backups incompletos, falta de continuidad del servicio).			
La implementación de acciones para prevenir los errores humanos;												En Berrut, no se identificaron acciones sistemáticas o estructuradas que tengan como propósito específico la prevención de errores humanos. Actualmente, el control de errores depende en gran medida de la experiencia individual del personal, el conocimiento técnico adquirido en la práctica y la revisión informal de actividades. Aunque existen herramientas operativas como: GLP para seguimiento de tickets, Centreon para monitoreo técnico, Formación técnica ocasional brindada por mayoristas, Y actos de entrega de productos firmados por los clientes, no se evidencian medidas diseñadas específicamente para prevenir errores humanos, tales como: Listas de verificación (checklists), Procedimientos paso a paso validados, Verificaciones cruzadas (doble revisión), Lecciones aprendidas o análisis de errores previos, Automatización de tareas repetitivas o críticas. Además, no se conserva registro de no conformidades causadas por error humano, ni de acciones preventivas implementadas con base en incidentes pasados.			
La implementación de actividades de liberación, entrega y posteriores a la entrega.												En la organización se identificaron prácticas parciales que evidencian actividades de liberación y entrega, especialmente en la venta de productos, donde se utiliza un acta de entrega firmado por el cliente, que incluye: Fecha de entrega, Cantidades, Descripción del producto, Firma de quien entrega y de quien recibe.	En cuanto a los servicios, como soporte TI, instalación o mantenimiento, no se evidenció un procedimiento formal para la liberación del servicio ni un criterio definido para su cierre y aceptación. Tampoco se realizan actividades sistemáticas posteriores a la entrega, tales como: Confirmación de satisfacción del cliente, Verificación de resultados del servicio, Seguimiento técnico post-servicio (salvo lo que se registra en GLP, de forma operativa). En los contratos, sí se establecen condiciones generales sobre entregas, pero no hay formatos ni protocolos estandarizados para gestionar la liberación y verificar el cumplimiento de lo pactado, salvo el ticket cerrado o el acta en venta.	Definir procedimientos o instructivos Estandarizar formatos	
					0	5	4								
8.5.2. Identificación y trazabilidad								50%							
¿Se utilizan los medios apropiados para identificar las salidas, cuando es necesario, para asegurar la conformidad de los productos y servicios?												En Berrut, si se utilizan algunos medios para identificar las salidas de productos y servicios, aunque de forma parcial y no estandarizada. En particular: En la venta de productos físicos, se genera un acta de entrega, que identifica: Lo que se entrega, Cantidades, Fecha, Cliente que lo recibe. Esta acta funciona como medio de identificación de la salida, y es firmada por ambas partes. En el caso de servicios de soporte técnico, el sistema GLP permite generar tickets que contienen información sobre la atención prestada, incluyendo: Fecha y hora, Descripción del incidente o solicitud, Técnico asignado, Estado del ticket (cerrado o abierto). No obstante, los tickets no siempre describen con precisión el producto final entregado (ej. configuración, instalación específica, estado de salud).	En servicios más complejos (ej. instalación de redes, mantenimiento, configuración de servidores), no se identificó un formato de salida ni un documento que certifique la conformidad del servicio prestado. Tampoco se usa una ficha técnica, informe de ejecución, checklist de verificación, o acta de aceptación técnica por parte del cliente.	Acta de entrega en productos físicos Contratos y cotizaciones como referencias para la solicitud checklist técnico, validación por cliente, informe de entrega	

¿Se identifica el estado de las salidas con respecto a los requisitos de seguimiento y medición a través de la producción y prestación del servicio?				X					<p>En Berrut, existen mecanismos parciales que permiten conocer el estado de los servicios o productos en relación con los requisitos establecidos, pero estos no están formalmente estructurados ni estandarizados.</p> <p>En productos: Se utiliza un acta de entrega firmada por el cliente, que indica que el producto fue recibido conforme en cuanto a cantidad y tipo. No obstante, no se documenta si se cumplieron todos los requisitos técnicos o funcionales prometidos, ni se verifica explícitamente el estado del producto respecto a parámetros de calidad u otros requisitos.</p> <p>En servicios: A través de la plataforma GLP, se puede verificar el estado del ticket (abierto, en proceso, cerrado), lo que permite tener una imagen clara del estado de la atención.</p> <p>En Berrut, se identificaron acciones parciales relacionadas con trazabilidad, aplicables principalmente en la entrega de productos físicos, pero no se implementa un sistema formal de trazabilidad integral para servicios o configuraciones técnicas.</p> <p>En productos: Se elabora un acta de entrega firmada por el cliente, donde se indica: Fecha, Cantidad, Descripción del producto.</p> <p>Sin embargo, no se incluye en todos los casos la identificación única del producto (ej. número de serie, código de equipo, ID de software/licenciado), salvo cuando el cliente lo solicita expresamente o el tipo de producto lo exige.</p> <p>En servicios: A través de la plataforma GLP, se puede rastrear: (i) historial del ticket, (ii) técnico asignado, (iii) fecha de atención y cierre, (iv) Descripción del incidente.</p> <p>A pesar de esto, la trazabilidad está limitada a eventos operativos y no está vinculada a una salida única con criterios técnicos estandarizados. Tampoco se conserva documentación estructurada de configuraciones, entregables digitales o decisiones técnicas documentadas.</p>	<p>Sin embargo: No se evidencian registros de validación técnica del servicio antes del cierre. No se documentan los criterios de aceptación (que requisitos debía cumplir la solución). No se realiza una medición o validación explícita del resultado entregado versus lo requerido.</p>		
¿Se controla la identificación única de las salidas cuando la trazabilidad sea un requisito, y se conserva la información documentada necesaria para permitir la trazabilidad.				X					<p>En Berrut, se identificaron acciones parciales relacionadas con trazabilidad, aplicables principalmente en la entrega de productos físicos, pero no se implementa un sistema formal de trazabilidad integral para servicios o configuraciones técnicas.</p> <p>En productos: Se elabora un acta de entrega firmada por el cliente, donde se indica: Fecha, Cantidad, Descripción del producto.</p> <p>Sin embargo, no se incluye en todos los casos la identificación única del producto (ej. número de serie, código de equipo, ID de software/licenciado), salvo cuando el cliente lo solicita expresamente o el tipo de producto lo exige.</p> <p>En servicios: A través de la plataforma GLP, se puede rastrear: (i) historial del ticket, (ii) técnico asignado, (iii) fecha de atención y cierre, (iv) Descripción del incidente.</p> <p>A pesar de esto, la trazabilidad está limitada a eventos operativos y no está vinculada a una salida única con criterios técnicos estandarizados. Tampoco se conserva documentación estructurada de configuraciones, entregables digitales o decisiones técnicas documentadas.</p>	<p>Para elementos como respaldo de información, instalaciones o configuración de servidores, no se lleva un control documental que permita identificar de forma única lo que se hizo, cómo se hizo y quién lo hizo, salvo lo que pueda recuperarse operativamente desde GLP o Centreon, sin estructura formal.</p>		
			0	3	0							
8.5.3. Preservación			50%									
¿Se preservan las salidas durante la producción y prestación del servicio, en la medida necesaria para asegurarse de la conformidad con los requisitos?				X					<p>En Berrut, se evidencian acciones parciales que contribuyen a la preservación de las salidas, tanto en productos como en servicios. No obstante, no existe un enfoque formal, documentado ni estandarizado para asegurar la preservación en todos los procesos críticos.</p> <p>En productos: Se conserva el estado físico de los productos durante su entrega mediante embalaje adecuado. Se utiliza un acta de entrega firmada por el cliente, que da trazabilidad a la entregado, lo cual apoya la conformidad con los requisitos.</p> <p>En servicios: La empresa utiliza UPS (sistemas de alimentación ininterrumpida) para proteger los servidores durante cortes de energía, lo cual preserva la continuidad y la integridad de los servicios críticos hasta que se pueda realizar un apagado controlado. Se hacen copias de seguridad (backups) para proteger la información de los clientes. Se utiliza OneDrive como almacenamiento de respaldo.</p>	<p>Sin embargo, no se identifican procedimientos documentados que definan cómo se debe preservar la integridad, identificación o seguridad de entregables digitales, configuraciones técnicas o servicios prestados mientras están en ejecución. Tampoco se conserva evidencia sistemática de validaciones técnicas (intermedias, condiciones de almacenamiento lógico o físico, ni mecanismos de preservación de datos mientras se realiza el servicio.</p>	<p>Procedimientos ante desastres política de back up procedimiento de almacenamiento Acta de entrega de productos y/o servicios Indicadores de trazabilidad Informes y análisis de la información</p>	
			0	1	0							
8.5.4. Propiedad perteneciente a los clientes o proveedores			33%									
¿Se asegura el cuidado de la propiedad perteneciente a los clientes o a proveedores externos mientras esté bajo el control de la organización o esté siendo utilizado por la misma?				X					<p>Se identifican prácticas operativas que evidencian el cuidado parcial de la propiedad del cliente, principalmente en infraestructura física o digital, aunque no existe un procedimiento documentado que lo formalice.</p> <p>Evidencias positivas: La empresa implementa el uso de UPS en los servidores de los clientes, lo cual permite mantener la continuidad de energía en caso de cortes, preservando la integridad de la información y los equipos. Se utilizan copias de seguridad (backups) y almacenamiento en OneDrive, lo que protege la información de los clientes que está bajo el control temporal de Berrut. En muchos casos, las configuraciones técnicas, servidores o equipos instalados en el cliente son tratados bajo condiciones de seguridad operativa, aunque sin trazabilidad escrita. En algunos contratos se incluyen cláusulas de confidencialidad y manejo de datos, lo que implica un reconocimiento formal de responsabilidad.</p>	<p>Aspectos pendientes: No existe un registro que identifique formalmente la propiedad del cliente o proveedor externo bajo custodia, ni un control que indique su localización, estado, responsable, ni trazabilidad. No se evidencian acciones documentadas en caso de daño, pérdida o deterioro de dicha propiedad. No hay evidencia de capacitación del personal sobre el manejo de propiedad del cliente. Tampoco se define cómo se gestiona la propiedad intangible (ej. accesos, credenciales, licencias temporales) cuando se entrega por parte del cliente o proveedor.</p>		
¿Se identifica, verifica, protege y salvaguarda la propiedad de los clientes o de los proveedores externos suministrada para su utilización o incorporación dentro de los productos y servicios?				X					<p>Existen prácticas operativas que demuestran cuidado parcial de la propiedad del cliente y de proveedores externos, principalmente en entornos de soporte técnico e infraestructura, pero no hay una metodología formal ni un sistema documentado de gestión de dicha propiedad.</p> <p>Ejemplos de aplicación en la organización: Uso de UPS que garantiza la continuidad de energía y evita daños en servidores del cliente (protección de activos físicos). Backups y uso de OneDrive, que permiten salvaguardar la información del cliente durante la ejecución del servicio. En algunos contratos se incluyen cláusulas de confidencialidad y protección de datos, lo que indica la intención de cuidar los activos digitales del cliente.</p>	<p>No se encontró evidencia de que se identifique o registre formalmente cada elemento propiedad del cliente o proveedor cuando este es utilizado en un servicio. No se hace una verificación al recibir un equipo, acceso o archivo, ni se registra su estado inicial. Tampoco hay evidencia de controles físicos o digitales adicionales para resguardar datos confidenciales más allá de la buena práctica del equipo técnico.</p>		
¿Cuando la propiedad de un cliente o de un proveedor externo se pierda, deteriore o de algún otro modo se considere inadecuada para su uso, se informa de esto al cliente o proveedor externo y conservar la información documentada sobre lo ocurrido?				X					<p>En la auditoría se evidenció que Berrut no ha documentado ningún procedimiento formal para la notificación, tratamiento y registro de incidentes relacionados con la propiedad del cliente o de proveedores externos. Tampoco se identificaron registros históricos que evidencien la ocurrencia de un evento de pérdida, daño o deterioro, ni acciones documentadas frente a estos casos. Aunque en la práctica el equipo técnico demuestra compromiso con la protección de activos del cliente (a través del uso de UPS, backups y prácticas seguras), no existe un protocolo que establezca: Cómo se debe actuar ante el deterioro o pérdida de equipos o datos. A quién debe notificarse formalmente. Qué registros deben generarse (bitácora del incidente, comunicación al cliente, medidas correctivas). Este vacío representa un riesgo reputacional, contractual y de cumplimiento normativo, ya que no se garantiza trazabilidad ni evidencia de acción responsable frente a la propiedad ajena.</p>			
			0	2	1							
8.5.5 Actividades posteriores a la entrega			29%									

¿Se cumplen los requisitos para las actividades posteriores a la entrega asociadas con los productos y servicios?													<p>se evidencian acciones dispersas que corresponden a actividades posteriores a la entrega, principalmente en los servicios de soporte TI y la atención a productos, pero no se identificó una política, procedimiento ni estructura formal que integre dichas actividades como parte del ciclo de prestación del servicio.</p> <p>Casos positivos:</p> <p>Se realiza soporte técnico post-entrega a través de la plataforma GUP, donde los clientes pueden generar solicitudes incluso después de la entrega inicial de un producto o servicio.</p> <p>Se tiene implementado un procedimiento de atención de quejas, el cual canaliza insatisfacciones que podrían estar relacionadas con la entrega.</p> <p>En el área comercial, las interacciones con clientes quedan registradas en el CRM, lo cual puede servir de base para seguimiento posterior si se estructura adecuadamente.</p> <p>Se realizan backups y monitoreo de red (Centreon) que pueden considerarse parte de una actividad de soporte post-entrega, sobre todo cuando hay acuerdos de continuidad.</p>	<p>Limitaciones encontradas:</p> <p>No existen criterios documentados ni compromisos contractuales claros sobre el alcance de las actividades post-entrega (tiempos de atención, criterios de satisfacción, actualizaciones, garantías).</p> <p>No se implementan actividades de seguimiento proactivo (llamadas de satisfacción, encuestas, verificación técnica del desempeño entregado).</p> <p>No se conserva información documentada que evidencie que las actividades post-entrega cumplieron requisitos acordados o expectativas del cliente.</p> <p>Los informes técnicos generados post-servicio no se validan con el cliente, y están solo en el correo del director técnico, sin trazabilidad.</p>		
¿Al determinar el alcance de las actividades posteriores a la entrega que se requieren, la organización considerar													<p>la determinación del alcance de las actividades posteriores a la entrega no se realiza de forma estructurada, ni se tienen criterios definidos que contemplen los factores establecidos en la norma ISO 9001:2015. Sin embargo, existen elementos prácticos que pueden ser aprovechados como base para establecer un sistema formal.</p> <p>Prácticas actuales observadas:</p> <p>Soporte técnico posterior a la entrega a través de la plataforma GUP, con posibilidad de gestionar solicitudes, fallas o ajustes posteriores a la prestación inicial del servicio.</p> <p>Contratos personalizados y cotizaciones en los que se pactan ciertos niveles de atención o respuesta tras la entrega, aunque sin detallar formalmente la vida útil, requisitos legales o consecuencias no deseadas.</p> <p>Copias de seguridad (backups) y uso de UPS para preservar información y continuidad de operaciones, especialmente en infraestructura entregada al cliente.</p> <p>Atención de quejas a través de un procedimiento establecido.</p> <p>Interacción con clientes a través de CRM básico, donde se podrían integrar datos de retroalimentación, aunque no se explora con ese fin actualmente.</p>	<p>Elementos ausentes o no estructurados:</p> <p>No se consideran de forma documentada los requisitos legales o reglamentarios específicos aplicables a la fase post-entrega (por ejemplo, garantías de software, tiempos de respuesta, condiciones del soporte).</p> <p>No se analiza formalmente la vida útil de los productos o servicios, ni su relación con el alcance de soporte o mantenimiento.</p> <p>No se gestiona de forma activa la retroalimentación del cliente, ni positiva ni negativa, más allá de las quejas esporádicas.</p> <p>No se contempla de forma preventiva el riesgo de consecuencias no deseadas si el soporte o servicio post-entrega es insuficiente o inexistente.</p>		
Los requisitos legales y reglamentarios?													<p>no realiza un análisis formal ni documentado de los requisitos legales o reglamentarios aplicables a la fase post-entrega, y tampoco los tiene como un criterio explícito para definir los servicios o actividades posteriores a la entrega de productos o servicios.</p> <p>Si bien algunos contratos incluyen cláusulas de confidencialidad y tratamiento de datos personales, que se alinean con la Ley 1581 de 2012 (protección de datos personales en Colombia), no se identificaron cláusulas específicas sobre obligaciones post-venta como garantías, soporte técnico reglamentado, mantenimiento obligatorio o tiempos de atención regulados.</p> <p>Tampoco se encontró un procedimiento de revisión legal que considere: Normas del régimen de comercio electrónico, Responsabilidad civil por fallas del servicio, Leyes aplicables a software, hardware o continuidad del negocio, Requisitos sectoriales si el cliente pertenece a un sector regulado (por ejemplo, salud, financiero o gubernamental).</p>			
Las consecuencias potenciales no deseadas a sus productos y servicios?													<p>No realiza un análisis formal ni sistemático de las consecuencias no deseadas que podrían derivarse del uso, falla o mal funcionamiento de sus productos o servicios una vez entregados.</p> <p>Aunque el equipo técnico posee un alto conocimiento operativo y responde con agilidad ante fallas, no existen registros, procedimientos ni herramientas documentadas que permitan identificar o anticipar escenarios de riesgo para el cliente después de la entrega. Tampoco se vinculan estas consecuencias con criterios para definir el tipo o nivel de soporte post-entrega requerido.</p>			
La naturaleza , el uso y la vida útil prevista de sus productos y servicios?													<p>no aplica de forma documentada ni estructurada un análisis sobre la naturaleza, uso o vida útil prevista de sus productos y servicios como base para definir las actividades post-entrega.</p> <p>Si bien el equipo técnico posee conocimiento práctico sobre el comportamiento y durabilidad esperada de ciertos componentes tecnológicos y servicios prestados, este conocimiento no se traslada a una política, procedimiento o contrato que establezca.</p>			
Los requisitos del cliente?													<p>No obstante, sí se identifican prácticas comerciales y técnicas que evidencian cierta personalización basada en el cliente, como: las cotizaciones personalizadas, en las cuales se adaptan los servicios o entregables a las necesidades específicas del cliente. La existencia de contratos que formalizan acuerdos individuales, incluyendo tiempos de entrega, alcances, componentes de soporte y condiciones de pago.</p> <p>La plataforma GUP, que permite recibir solicitudes de soporte técnico incluso después de finalizar el proyecto o instalación.</p> <p>El uso de un CRM básico donde se documenta parte de la interacción comercial, aunque no se emplea como insumo para definir servicios post-entrega.</p> <p>Un procedimiento para atención de quejas, que permite canalizar insatisfacciones posteriores a la entrega, aunque sin integrarse al proceso de mejora o rediseño de soporte.</p>	<p>no cuenta con un procedimiento formal para recopilar, analizar o integrar los requisitos específicos del cliente relativos a la etapa posterior a la entrega como parte del diseño de sus servicios.</p> <p>Una recolección sistemática de requisitos post-entrega durante la preventa o la firma de contrato.</p> <p>Que se analicen formalmente los niveles de soporte deseados por el cliente (por ejemplo, soporte 24/7, mantenimientos programados, garantías extendidas).</p> <p>Que se documente la trazabilidad entre lo que el cliente solicita y lo que finalmente se ofrece o entrega.</p>		
La retroalimentación del cliente?													<p>Prácticas existentes observadas:</p> <p>Se cuenta con un procedimiento para la atención de quejas, lo que permite identificar insatisfacciones puntuales posteriores a la entrega.</p> <p>La plataforma GUP permite registrar y gestionar solicitudes técnicas post-entrega, y contiene información útil sobre problemas recurrentes o tiempos de atención, aunque no se analiza como retroalimentación formal.</p> <p>Algunas interacciones comerciales quedan documentadas en el CRM, lo que podría reflejar satisfacción o solicitudes de mejora, pero no se sistematiza ni se convierte en mejora estructural.</p>	<p>no cuenta con un proceso sistemático para recolectar, analizar y utilizar la retroalimentación del cliente como insumo para definir sus actividades post-entrega. Si bien se atienden quejas o comentarios cuando el cliente los manifiesta, no existe una metodología proactiva que permita capitalizar esta información para mejorar el soporte posterior.</p> <p>Limitaciones evidenciadas:</p> <p>No se aplica ninguna encuesta o mecanismo de evaluación formal de satisfacción del cliente.</p> <p>No hay reuniones o seguimientos post-entrega que recojan de forma directa la percepción del cliente.</p> <p>No se hace seguimiento a la experiencia del cliente tras la entrega del servicio o producto.</p> <p>La información que se obtiene por medios informales (llamadas, tickets, correos) no se documenta ni consolida como insumo para mejorar el servicio post-entrega.</p>		
				0	4	3										
8.5.6 Control de cambios						0%										

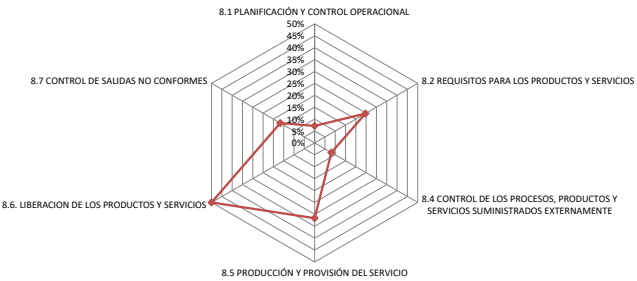
¿Se revisa y controlan los cambios para la producción o la prestación del servicio, en la extensión necesaria para asegurarse de la continuidad en la conformidad con los requisitos?					X						<p>Hallazgos relevantes:</p> <p>En casos puntuales, como ajustes de personal técnico o cambios en la solución entregada al cliente, se toman decisiones directamente por la alta dirección o los líderes técnicos, pero sin dejar trazabilidad ni evaluación previa del impacto del cambio.</p> <p>No se identificó ningún formato, acta o registro que evidencie:</p> <p>Qué cambio se solicitó o aplicó,</p> <p>Quién lo aprobó,</p> <p>Qué riesgo o impacto podría tener,</p> <p>Cómo se comunicó al cliente o al personal afectado.</p> <p>La información técnica se encuentra dispersa, muchas veces sólo en el correo del director o en los tickets de la plataforma GLP, sin consolidación ni trazabilidad.</p> <p>Esto puede generar riesgos operativos importantes, como:</p> <p>Falta de alineación entre el producto entregado y los requisitos contractuales,</p> <p>Pérdida de control en la trazabilidad técnica del servicio,</p> <p>Fallos en la continuidad del servicio ante cambios no documentados,</p> <p>Desconocimiento por parte del cliente o del equipo de soporte frente a los cambios implementados.</p>	
¿Se conserva información documentada que describa los resultados de la revisión de los cambios, las personas que autorizan el cambio y de cualquier acción necesaria que surja de la revisión?					X						<p>En la práctica, se realizan modificaciones a configuraciones, personal asignado, planes de trabajo o componentes técnicos, pero estos cambios no se documentan formalmente.</p> <p>No se hallaron evidencias de:</p> <p>Actos o correos estructurados que aprueben el cambio,</p> <p>Evaluación del impacto del cambio,</p> <p>Registro de quién autorizó el cambio ni de qué se hizo después.</p> <p>La información asociada a los cambios puede quedar en correos personales, dentro de tickets en GLP o en el conocimiento tácito del equipo técnico, sin trazabilidad.</p>	
			0	0	2							
8.6. LIBERACION DE LOS PRODUCTOS Y SERVICIOS			50%									
¿Se implementan disposiciones planificadas, en las etapas adecuadas, para verificar que se cumplen los requisitos de los productos y servicios?					X						<p>Para soporte TI, la plataforma GLP permite registrar la atención de tickets, su estado, descripción de actividades y cierre, lo que permite inferir un cumplimiento mínimo de requisitos funcionales.</p> <p>Para ventas de productos, si bien no se almacena ni libera inventario internamente, se generan actas de entrega firmadas por el cliente, lo que constituye evidencia de conformidad parcial.</p>	<p>En mantenimientos, se elabora un plan de trabajo por actividad, que incluye tiempos, actividades y validación de ejecución. Sin embargo, no se define si se verificó contra los requisitos acordados con el cliente, ni hay formato estandarizado para esta liberación.</p> <p>En servicios de implementación o configuración, no se encontró evidencia de checklists técnicos ni validaciones documentadas previas al cierre o entrega.</p>
¿Los productos y servicios son liberados al cliente hasta que se hayan completado satisfactoriamente las disposiciones planificadas?,					X						<p>En productos físicos, el mayorista entrega directamente al cliente, pero Ferrari genera actas de entrega firmadas, lo que constituye una evidencia de aceptación. Sin embargo, no incluyen criterios técnicos de conformidad ni firma interna de liberación.</p> <p>En el servicio de soporte, la plataforma GLP permite cerrar tickets y ver su estado, pero no hay evidencia de revisión técnica previa a la liberación del servicio.</p> <p>Para mantenimientos, se elabora un plan de trabajo que indica actividades realizadas y su cumplimiento, aunque no está vinculado a criterios de verificación específicos ni contiene validación técnica documentada.</p>	<p>No se realiza una verificación técnica documentada antes de entregar servicios o soluciones al cliente.</p> <p>No hay evidencia de que un responsable técnico autorice formalmente la liberación.</p> <p>El cliente no valida de manera formal que lo entregado cumple con lo pactado, más allá de la firma de entrega física.</p>
¿Los productos y servicios son liberados al cliente cuando son aprobado de otra manera por una autoridad pertinente y, cuando sea aplicable, por el cliente?					X						<p>En algunos casos, se entrega el servicio o producto con base en la experiencia del equipo técnico, aunque no se haya verificado completamente el cumplimiento de todas las actividades planificadas.</p> <p>No se identificaron registros de aprobaciones formales por parte de responsables técnicos o del cliente ante desviaciones o entregas condicionadas.</p> <p>El cliente firma el acta de entrega en algunos casos, pero esto no sustituye ni documenta la aceptación explícita de una entrega fuera de los criterios de aceptación.</p>	<p>No existe un formato o evidencia escrita de que una autoridad pertinente haya aprobado una liberación excepcional.</p> <p>El cliente no aprueba formalmente la entrega anticipada o bajo condición.</p> <p>No hay análisis de impacto ni justificación técnica registrada.</p>
¿Se conserva información documentada sobre la liberación de los productos y servicios?					X						<p>Para productos vendidos, se firma un acta de entrega por parte del cliente, la cual incluye:</p> <p>Fecha de entrega,</p> <p>Elementos entregados,</p> <p>Nombre de quien recibe y entrega.</p> <p>Sin embargo, no incluye criterios de aceptación ni autorización técnica interna.</p> <p>Para servicios (soporte, mantenimiento):</p> <p>Se elaboran informes de actividades,</p> <p>Se utilizan planes de trabajo que registran lo ejecutado,</p> <p>Pero estos no son validados por el cliente ni firmados por personal técnico como evidencia de liberación.</p> <p>En plataforma GLP,</p> <p>Se puede verificar si un ticket fue atendido y cerrado,</p> <p>Pero no se conserva evidencia formal del cumplimiento contra requisitos ni quién autorizó el cierre.</p>	<p>No se conserva evidencia técnica explícita de cumplimiento de los requisitos.</p> <p>No hay firma o trazabilidad de quién autoriza la liberación (servicio o producto).</p> <p>No se consolidan los registros en un sistema o carpeta centralizada.</p>
¿La información documentada incluye evidencia de la conformidad con los criterios de aceptación?					X							
¿La información documentada incluye la trazabilidad a las personas que autorizan la liberación?					X						<p>En el acta de entrega de productos:</p> <p>Aparece quién entrega y quién recibe,</p> <p>Pero no queda claro si quien entrega también verifica técnicamente la conformidad del producto ni se registra formalmente como autorizador.</p> <p>En servicios de soporte o mantenimiento:</p> <p>Se genera un informe o plan de trabajo,</p> <p>No incluye firma o validación del técnico que autoriza la liberación del servicio.</p> <p>En la plataforma GLP:</p> <p>Se puede identificar el usuario que cierra el ticket,</p> <p>Esto da una trazabilidad técnica parcial,</p> <p>Pero no se registra si esa persona tiene rol de aprobación ni si validó criterios de aceptación.</p>	<p>No hay control ni estandarización de quién aprueba técnicamente cada entrega.</p> <p>La trazabilidad no está integrada a los formatos o sistemas de manera explícita.</p> <p>No se conserva evidencia documentada de esta autorización.</p>
			0	6	0							
8.7 CONTROL DE SALIDAS NO CONFORMES			17%									

¿Se asegura que se identifiquen y controlan las salidas que no sean conformes con sus requisitos para prevenir su uso o entrega no intencionada?				X						<p>Cuando un cliente detecta una falla, se puede generar un ticket en GLP, y el equipo técnico da respuesta.</p> <p>En algunos casos, se evidenció que el área técnica toma acciones correctivas inmediatas, pero no se conserva evidencia formal como no conformidad.</p>	<p>No se identificó un sistema de registro, análisis y seguimiento de salidas no conformes, ni un responsable designado para su gestión.</p> <p>Tampoco hay evidencia de evaluación del impacto, contención, o comunicación interna formal cuando ocurre una desviación.</p>	
¿Se toman las acciones adecuadas basándose en la naturaleza de la no conformidad y en su efecto sobre la conformidad de los productos y servicios?					X						<p>En soporte TI, las fallas técnicas suelen ser resueltas por el equipo directamente desde GLP, pero no se realiza análisis formal del tipo de no conformidad ni de su impacto operativo o contractual.</p> <p>No hay distinción entre una falla crítica (ej. pérdida de respaldo, corte de servicio) y una falla menor (ej. error en reporte, atención demorada).</p> <p>No se documentan acciones de tipo:</p> <ul style="list-style-type: none"> Corrección inmediata vs. acción correctiva estructural, Notificación al cliente sobre impacto, Asignación de la culpa o no cumplimiento contractual o legal. <p>En la operación diaria, cuando un cliente detecta una falla post-entrega (ej. servicio incompleto, instalación deficiente, backup infectivo), se atiende directamente por el equipo técnico o comercial, pero:</p> <ul style="list-style-type: none"> No se registra como no conformidad, No se analiza la causa raíz, No se genera documentación formal del tratamiento ni se evidencia la validación del cliente. 	
¿Esto se aplica también a los productos y servicios no conformes detectados después de la entrega de los productos, durante o después de la provisión de los servicios?				X						<p>Existe un procedimiento formal para rechazos y devoluciones de productos físicos, lo cual es un punto fuerte parcial.</p>		
¿Las salidas no conformes se tratan de una o más de las siguientes maneras: Corrección?				X						<p>Si se realizan correcciones cuando se detecta una no conformidad, especialmente en el contexto de soporte TI y servicios técnicos. Estas correcciones suelen llevarse a cabo de forma rápida y directa por el personal técnico.</p>	<p>No obstante:</p> <ul style="list-style-type: none"> No se registra formalmente que se trató como una no conformidad. No se conserva evidencia de la validación técnica de la corrección ni de la aceptación por parte del cliente. No se documenta si la corrección fue suficiente o si se repitió la no conformidad. 	
Separación, contención, devolución o suspensión de provisión de productos y servicios?					X						<p>No existe un proceso documentado formal para aplicar separación o suspensión, si se toman decisiones operativas para pausar entregas técnicas o resolver situaciones antes de continuar con la provisión del servicio o entrega del producto.</p> <p>No se documentan como parte de una gestión formal de no conformidades.</p> <p>No hay un criterio definido para cuando detener, devolver o pausar.</p> <p>No existe evidencia sistemática de estas decisiones (bitácora, autorización, trazabilidad).</p>	
Informando al cliente?					X					<p>Se evidenció que, en la práctica, algunas no conformidades son comunicadas al cliente de forma verbal o por correo, especialmente en soporte técnico o cuando hay demoras o fallas viables.</p>	<p>Sin embargo:</p> <ul style="list-style-type: none"> No hay un procedimiento que regule cómo y cuándo debe informarse al cliente sobre una no conformidad. No hay registros que evidencien qué se informó, cuándo y quién lo autorizó. En casos críticos (ej. backup no ejecutado, interrupción del servicio), no siempre se informa proactivamente si el cliente no lo detecta primero. 	
Obteniendo autorización para su aceptación bajo concesión?					X						<p>No cuenta con un procedimiento formal ni registro para gestionar concesiones.</p> <p>En la práctica, si un servicio se entrega parcialmente o con alguna limitación, se busca resolverlo o se coordina una solución directa con el cliente, pero:</p> <ul style="list-style-type: none"> No se solicita formalmente autorización del cliente para aceptar una salida fuera de especificación. No se deja evidencia de que el cliente aceptó voluntariamente la no conformidad, ni bajo qué condiciones. No se evalúa el impacto posterior de haber entregado un producto o servicio bajo concesión. 	
¿Se verifica la conformidad con los requisitos cuando se corrigen las salidas no conformes?					X						<p>Se evidenció que cuando ocurre una no conformidad operativa (ej. error técnico, instalación incompleta, fallo de backup), el personal técnico procede a corregirla y en muchos casos realiza una verificación funcional informal (ej. "funcionó después de reconfigurar"), pero:</p> <ul style="list-style-type: none"> No existe una verificación formal y registrada que asegure que se cumplen todos los requisitos definidos inicialmente. No hay un paso sistemático para validar la corrección antes de cerrar el ticket, proyecto o entrega. Tampoco se conserva evidencia documentada de que la conformidad fue establecida. 	
¿Se conserva información documentada que describa la no conformidad?					X						<p>Las no conformidades técnicas o errores de servicio son tratadas a través del sistema de tickets GLP.</p> <p>Los tickets incluyen descripción del problema, asignación, y solución aplicada.</p> <p>Sin embargo, GLP no se usa como repositorio de no conformidades estructuradas, sino solo como herramienta operativa.</p> <p>No existe un registro formal separado que clasifique estos eventos como "no conformidades" del sistema de gestión.</p> <p>No se conservan documentos con:</p> <ul style="list-style-type: none"> Identificación formal de la no conformidad, Trazabilidad del tratamiento, Evidencia de corrección o validación, Aprobación por parte de un responsable. 	
¿Se conserva información documentada que Describa las acciones todas;				X						<p>actúa técnicamente ante no conformidades (especialmente en soporte TI y provisión de servicios), las acciones tomadas no se documentan de forma estructurada. Esto incluye:</p> <ul style="list-style-type: none"> Correcciones operativas hechas directamente por el técnico, Coordinaciones con cliente para resolver fallos, Sustitución de dispositivos o reconfiguración de dispositivos. 	<p>No se registra el detalle de qué acciones se realizaron, en qué fecha, quién las ejecutó, y cuál fue su impacto.</p> <p>Las acciones que se ejecutan no están formalmente vinculadas a un análisis de causa ni a una validación de efectividad.</p> <p>En casos donde hay devolución de productos o reclamos, las acciones tomadas no se consolidan en un historial accesible para revisión o auditoría.</p>	
¿Se conserva información documentada que Describa todas las concesiones obtenidas;					X						<p>Se han presentado casos donde el cliente acepta ciertas desviaciones menores (por ejemplo, una entrega parcial de equipos, una configuración no 100% ajustada al alcance inicial, o una postergación acordada). Sin embargo:</p> <ul style="list-style-type: none"> No se documentan como concesiones. No se define un procedimiento para registrar, validar o aprobar este tipo de eventos. No se conserva evidencia estructural de que el cliente aceptó conscientemente una no conformidad bajo ciertas condiciones. Tampoco se identifica quién autorizó esta aceptación por parte de la responsabilidad. 	
¿Se conserva información documentada que identifique la autoridad que decide la acción con respecto a la no conformidad.					X						<p>Cuando ocurre una no conformidad técnica o operativa (por ejemplo, un error en un servicio, una devolución de equipo, una queja), las acciones se ejecutan directamente por parte del técnico o responsable operativo, y en muchos casos:</p> <ul style="list-style-type: none"> No queda documentado quién autorizó la decisión tomada. No se tiene evidencia de validación o aprobación por un líder, gerente o encargado del SGC. <p>Las decisiones se comunican en ocasiones por correo o verbalmente, pero sin registro formal ni firma digital/documental.</p>	
			0	4	8							

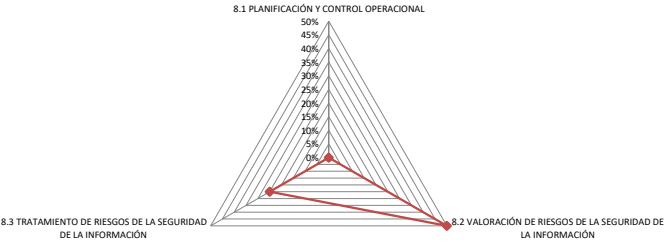
RESUMEN NUMERAL ISO 27001: 2022		ISO 9001
		AVANCE
8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL	8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL	7%
8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	8.2 REQUISITOS PARA LOS PRODUCTOS Y SERVICIOS	25%
8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	8.3 DISEÑO Y DESARROLLO DE LOS PRODUCTOS	na
	8.4 CONTROL DE LOS PROCESOS, PRODUCTOS Y SERVICIOS SUMINISTRADOS EXTERNAMENTE	8%
	8.5 PRODUCCIÓN Y PROVISIÓN DEL SERVICIO	32%
	8.6 LIBERACIÓN DE LOS PRODUCTOS Y SERVICIOS	50%
	8.7 CONTROL DE SALIDAS NO CONFORMES	17%
PROMEDIO AVANCE	PROMEDIO AVANCE	23%

ISO 27001
%
AVANCE
0%
50%
25%
25%

8. OPERACIÓN ISO 9001:2015



8. OPERACIÓN ISO 27001:2022



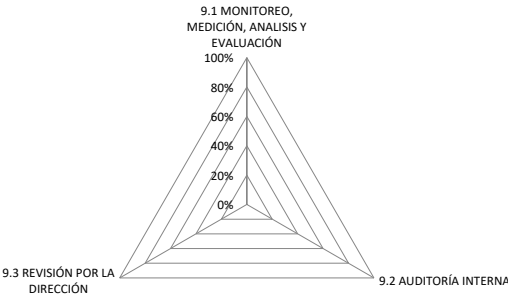
DIAGNÓSTICO NTC ISO 9001:2015 E ISO/IEC 27001: 2022												
		ISO 9001:2015				ISO 27001:2022						
9 EVALUACIÓN DEL DESEMPEÑO ISO 9001:2015	9 EVALUACIÓN DEL DESEMPEÑO ISO 27001:2022	NO APLICA	COMPLETO	PARCIAL	NINGUNO	NO APLICA	COMPLETO	PARCIAL	NINGUNO	¿QUÉ TIENE?	¿QUÉ NOS FALTA?	DOCUMENTOS ASOCIADOS
9.1 MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	9.1 MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN				0%				0%			
¿Se ha determinado qué necesita seguimiento y medición?	La organización debe determinar: a) a qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información;				X				X		Se debe dejar documentado en algún instrumento: a que se le va hacer seguimiento, incluido procesos y controles. Métodos de seguimiento, análisis, evaluación cuando se realizará la medición y seguimiento, quien ejecutará las acciones de seguimiento y medición, cuando se realizara el análisis y evaluación de los resultados .	Indicadores de gestion
¿Se han determinado los métodos de seguimiento, medición, análisis y evaluación necesarios para asegurar resultados válidos?	b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos; NOTA Para ser considerados válidos, los métodos seleccionados deberían producir resultados comparables y reproducibles.				X				X			
¿Se ha determinado cuándo se lleva a cabo el seguimiento y la medición?	c) cuándo se debe llevar a cabo el seguimiento y la medición;				X				X			
¿Se ha determinado cuándo se analiza, evalúan y comunican los resultados del seguimiento y la medición?	d) quién debe llevar a cabo el seguimiento y la medición;				X				X			
¿Se evalúa el desempeño y la eficacia del SGC?	e) cuando se deben analizar y evaluar los resultados del seguimiento y la medición;				X				X			
¿Se conserva información documentada apropiada como evidencia de los resultados del seguimiento, medición, análisis y evaluación?	f) quién debe analizar y evaluar estos resultados.				X				X			
¿Se analizan y evalúan los datos y la información apropiados que surgen por el seguimiento y la medición?	La información documentada debe ser retenida como evidencia de los resultados.				x				x			
¿ Evaluar la conformidad de los productos y servicios?	La organización debe evaluar el desempeño y efectividad del sistema de gestión de seguridad de la Información.				X				X			
¿ Evaluar el grado de satisfacción del cliente?					x				x			
¿ Evaluar el desempeño y la eficacia del sistema de gestión de la calidad?					X							
¿ Evaluar si lo planificado se ha implementado de forma eficaz?					X							
¿ Evaluar la eficacia de las acciones tomadas para abordar los riesgos y oportunidades?					X							
¿ Evaluar el desempeño de los proveedores externos?					X							
¿ Evaluar la necesidad de mejoras en el sistema de gestión de la calidad?					X							
			0	0	14		0	0	8			
9.2 AUDITORÍA INTERNA	9.2 AUDITORÍA INTERNA				0%				8%			
9.2.1 Generalidades	9.2.1 Generalidades				0%				17%			
¿Se llevan a cabo auditorías internas a intervalos planificados (con una periodicidad por lo menos una vez al año) para proporcionar información acerca de si:	La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información:				x				x		Esta actividad se debe programar una vez se cuente con la implementación del sistema, incluyendo la parte documental y socialización al interior de la entidad, con el fin de ir validando el avance en esta materia.	*Manual del Sistema de Gestión de Seguridad de la Información "
¿El SGC es conforme con:	a) es conforme con: 1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y 2) los requisitos de esta Norma;				X				X			
Los requisitos propios de la organización para su SGC incluyendo política y objetivos;	b) esta implementado y mantenido efectivamente				X			X				
Los requisitos de esta Norma Internacional;					X							
¿El SGC se implementa y mantiene eficazmente?					X							
			0	0	5		0	1	2			
9.2.2 Programa de auditoría interna	9.2.2 Programa de auditoría interna				0%				0%			
¿Se planifica, establece, implementa y mantiene uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes, que deben tener en consideración la importancia de los procesos involucrados, los cambios que afecten a la organización y los resultados de las auditorías previas? ¿el programa cubre todas las áreas, proceso, proyectos y elementos del sistema realizadas?	La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Cuando los programas de auditoría se establezcan en la organización debe considerar la importancia de los procesos involucrados y los resultados de las auditorías previas;				X				X		**Manual del Sistema de Gestión de Seguridad de la Información "" SIP -MA-002 Vr, 2 de 2021 (Numeral 9.3.1 Evaluación del Desempeño), se describe un ítem ""Auditoría Interna"", se indica que se debe realizar anualmente, pero no describe quien debe realizar esta actividad; sin embargo, en el último año no se ha realizado alguna auditoría sobre el asunto. *Procedimiento ""Auditoría Interna"" Esta actividad se debe programar una vez se cuente con la implementación del sistema, incluyendo la parte documental y socialización al interior de la entidad, con el fin de ir validando el avance en esta materia. Si bien el proceso de Control Interno tiene establecido un Programa de Auditoría Interna, para esta vigencia se tiene contemplado es un Diagnóstico de Implementación, para futuros ejercicios se debe	*Manual del Sistema de Gestión de Seguridad de la Información " * Procedimiento "Auditoría Interna"
¿Las auditorías son planificadas ?	La organización debe: a) definir los criterios y el alcance de cada auditoría;				X				X			
¿Se definen los criterios de la auditoría y el alcance para cada auditoría?	b) seleccionar auditores y llevar a cabo auditorías para asegurarse la objetividad y la imparcialidad del proceso de auditoría.				X				X			
¿Se seleccionan los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría? ¿las auditorías son ejecutadas por personal que no tenga responsabilidad directa con la actividad que se esté auditando?	c) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y				X				X			
¿Se aseguran de que los resultados de las auditorías se informen a la dirección pertinente?	d) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.				X				X			

¿Se realizan las correcciones y tomar las acciones correctivas y preventivas adecuadas sin demora injustificada?					X												
¿Se conserva información documentada como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías?					X												
	NOTA Para mayor información consultar las normas NTC-ISO 19011 y NTC-ISO 27007		0	0	7		0	0	5								
9.3 REVISIÓN POR LA DIRECCIÓN	9.3 REVISIÓN POR LA DIRECCIÓN		0%				0%										
9.3.1 Generalidades	9.3.1 Generalidades		0%				0%										
¿La alta dirección revisa el SGC, de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación, eficacia y alineación continuas con la dirección estratégica de la organización?	La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y efectividad.				X				X								En el ejercicio de revisión, no se obtuvo evidencia de que esto se haya realizado, por lo que se debe implementar estas revisiones con el fin de validar el compromiso de la Alta Dirección con este sistema.
			0	0	1		0	0	1								* Manual del Sistema de Gestión de Seguridad de la Información " SIP -MA-002 Vr, 2 de 2021 (Numeral 9.3.1 Evaluación del Desempeño), se describe un ítem "Revisión por la Dirección", * Manual del Sistema Integrado de Gestión - Código SIP-MA-001 versión 10 de fecha 26/04/2024.-
9.3.2 Entradas de la revisión por la dirección	9.3.2 Entradas de la revisión por la dirección		0%				0%										
¿ Incluye el estado de las acciones de las revisiones por la dirección previas?	La revisión por la dirección debe incluir consideraciones sobre: a) el estado de las acciones con relación a las revisiones previas por la dirección;				X				X								
¿Incluye los cambios en: *Las cuestiones externas o internas que sean pertinentes, *Las necesidades y expectativas de las partes interesadas, incluidos requisitos legales y otros, *Los aspectos ambientales significativos y *Los riesgos y oportunidades ?	b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;				X				X								
¿ Incluye la información sobre el desempeño y la eficacia del SGC incluidas las tendencias relativas a:	c) cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el sistema de seguridad de la información.				X				X								
El grado en que se han logrado los objetivos de la calidad	d) retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias relativas a:				X				X								
Los incidentes , no conformidades, acciones correctivas, preventivas y mejora continua?	1. no conformidades y acciones correctivas;				X				X								
Los resultados de seguimiento y medición;	2. seguimiento y resultados de las mediciones;				X				X								
Los resultados de las auditorías;	3. resultados de la auditoría; y																
La satisfacción del cliente y la retroalimentación de las partes interesadas pertinentes, incluidas las quejas;	4. cumplimiento de los objetivos de la seguridad de la información;				X				X								
El desempeño de los procesos y conformidad de los productos y servicios;	e) retroalimentación de las partes interesadas;				X				X								
El desempeño de los proveedores externos;	f) resultados de la apreciación de riesgos y estado del plan de tratamiento de riesgos; y				X				X								
¿ Incluye la eficacia de las acciones tomadas para abordar los riesgos y las oportunidades?	g) las oportunidades de mejora continúa.				X				X								
¿ Incluye la adecuación de los recursos?					X				X								
¿ Incluye las oportunidades o recomendaciones de mejora?					X				X								
			0	0	12		0	0	10								
9.3.3 Salidas de la revisión por la Dirección	9.3.3 Resultados de la revisión por la Dirección		0%				0%										
¿Las salidas de la revisión por la dirección incluyen las decisiones y acciones relacionadas con:	Los resultados de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información.				X				X								Se debe dejar documentada, las decisiones tomadas y las oportunidades de mejora y en general los resultados obtenidos de la revisión.
¿Las decisiones relacionadas con las oportunidades de mejora continua?	Información documentada debe ser retenida como evidencia de los resultados de las revisiones por la dirección.				X				X								
¿Cualquier necesidad de cambio en el SGC (incluyendo política y objetivos)?					X												
¿Las necesidades de recursos?					X												
¿Se conserva información documentada como evidencia de los resultados de las revisiones por la dirección y está disponible para consulta?					X												
			0	0	5		0	0	2								

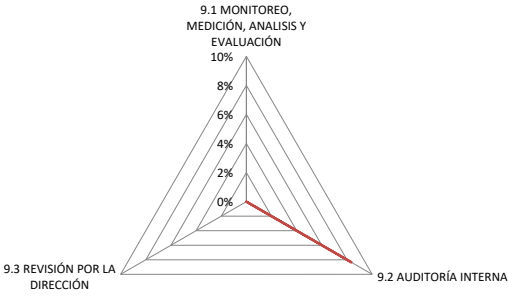
RESUMEN NUMERAL ISO 9001:2015		ISO 9001
		% AVANCE
9.1 MONITOREO, MEDICIÓN, ANALISIS Y EVALUACIÓN	9.1 MONITOREO, MEDICIÓN, ANALISIS Y EVALUACIÓN	0%
9.2 AUDITORÍA INTERNA	9.2 AUDITORÍA INTERNA	0%
9.3 REVISIÓN POR LA DIRECCIÓN	9.3 REVISIÓN POR LA DIRECCIÓN	0%
PROMEDIO AVANCE	PROMEDIO AVANCE	0%

ISO 27001
% AVANCE
0%
8%
0%
3%

9 EVALUACIÓN DEL DESEMPEÑO ISO 9001:2015



9 EVALUACIÓN DEL DESEMPEÑO ISO 27001:2022





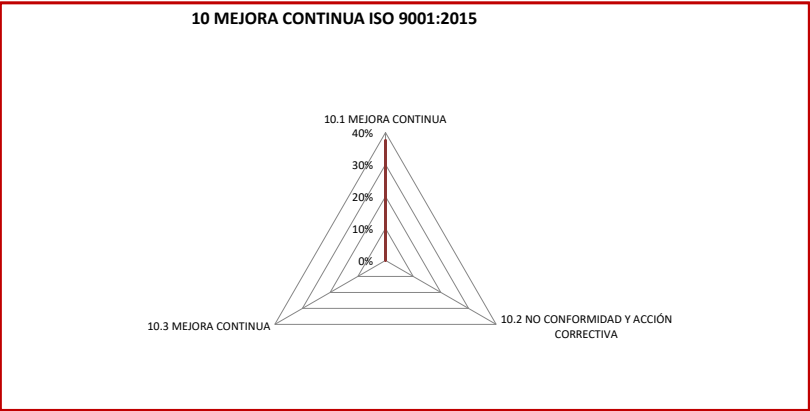
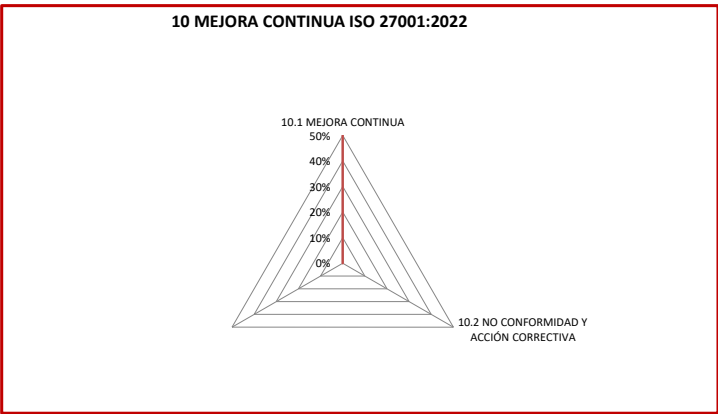
DIAGNÓSTICO NTC ISO 9001:2015 E ISO/IEC 27001: 2022

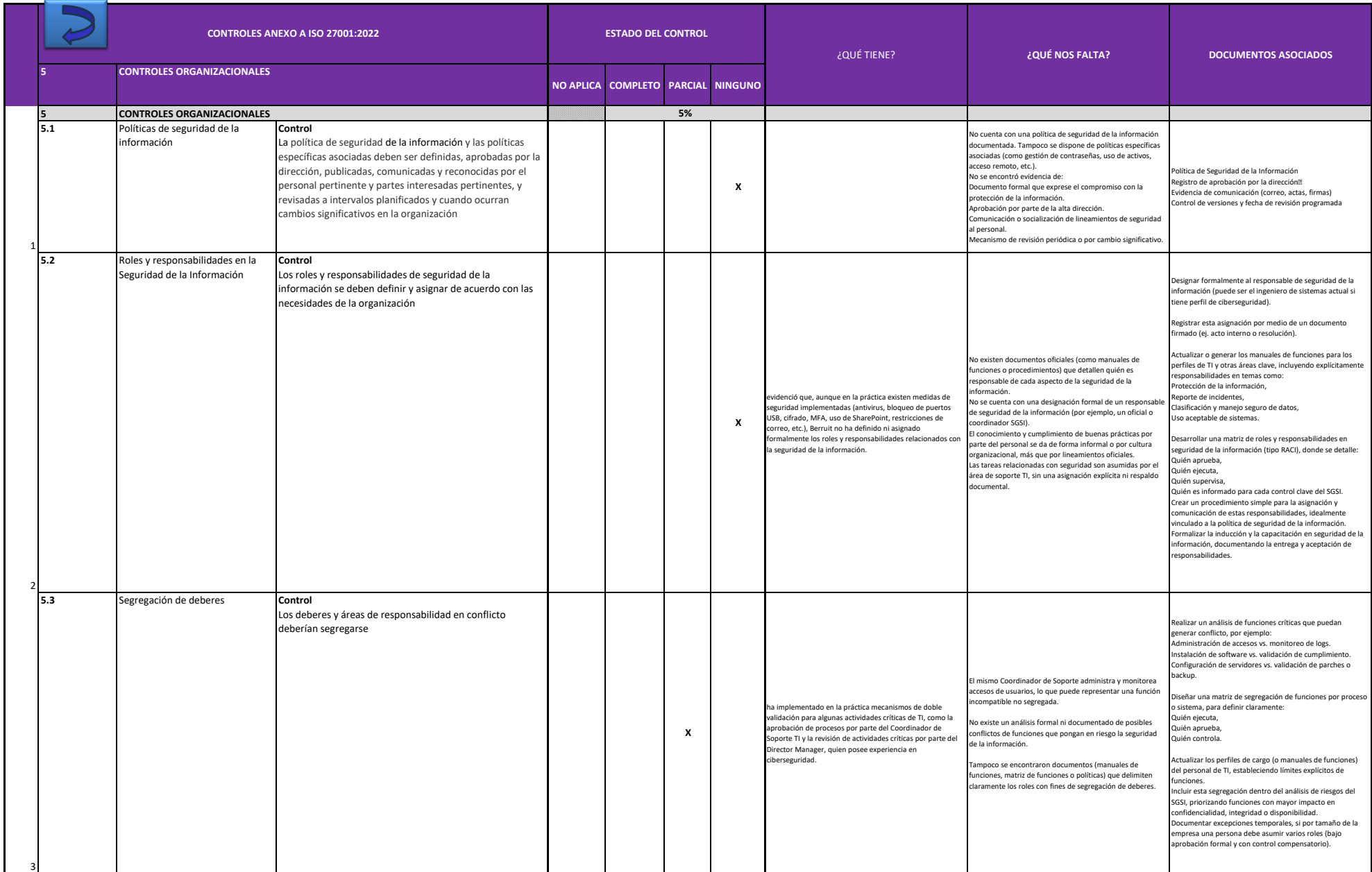
10 MEJORA ISO 9001:2015	10 MEJORA ISO 27001:2022	ISO 9001:2015				ISO 27001:2022				QUÉ TIENE?	QUE NOS FALTA	Documentos Asociados
		NO APLICA	COMPLETO	PARCIAL	NINGUNO	NO APLICA	COMPLETO	PARCIAL	NINGUNO			
10.1 MEJORA CONTINUA - GENERALIDADES	10.1 MEJORA CONTINUA				38%				50%			
¿Se han determinado, seleccionado las oportunidades de mejora e implementado cualquier acción necesaria para cumplir los requisitos del cliente, aumentar la satisfacción del cliente y para lograr los resultados previstos	La organización debe mejorar continuamente la sostenibilidad, adecuación y efectividad del sistema de gestión de la seguridad de la información.			X				X		* Actas de aceptación de productos cuando se entregan al cliente	Aunque se describe de manera general algo sobre la mejora, no se evidencia que esto se haya evaluado y documentado. Crear documento de mejora del sistema de gestión	
Mejorar los productos y servicios para cumplir los requisitos, así como considerar las necesidades y expectativas futuras;				X						Reuniones con cliente donde se indican las cosas a corregir o mejorar. No se dejan actas de reunión de estos compromisos	Crear documento de mejora del sistema de gestión	
Corregir, prevenir o reducir los efectos no deseados;				X						Se atienden los requerimientos pero no queda documentado	Crear documento de mejora del sistema de gestión	
Mejorar el desempeño y la eficacia del sistema de gestión de la calidad.					X						Crear documento de mejora del sistema de gestión	
			0	3	1		0	1	0			
10.2 NO CONFORMIDAD Y ACCIÓN CORRECTIVA	10.2 NO CONFORMIDAD Y ACCIÓN CORRECTIVA				0%				0%			
Cuando ocurra una no conformidad, la organización debe:	Cuando ocurra una no conformidad, la organización debe:											
Cuando ocurre una no conformidad o un incidente, incluida cualquiera originada por quejas, la organización:	a) reaccionar ante la no conformidad, y según sea aplicable 1. tomar acciones para controlarla y corregirla, y 2. hacer frente a las consecuencias;				X				X			
Reacciona ante la no conformidad y/o incidente y, cuando sea aplicable:	b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante: 1. la revisión de la no conformidad 2. la determinación de las causas de la no conformidad, y 3. la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;				X				X			
¿Toma acciones para controlar y corregir la no conformidad o el incidente? ¿Hace frente a las consecuencias, incluida la mitigación de los impactos ambientales adversos?	c) implementar cualquier acción necesaria;				X				X			
Evalúa con la participación de los trabajadores e involucra otras partes interesadas pertinentes, la necesidad de acciones para eliminar las causas de la no conformidad o el incidente, con el fin de que no vuelva a ocurrir ni ocurra en otra parte mediante:	d) revisar la eficacia de las acciones correctivas tomadas, y				X				X			
¿La revisión y el análisis de la no conformidad y/o la investigación del incidente?	e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario.				X				X		Crear el procedimiento de acciones correctivas. Diseñar un formato de reporte de no conformidades y acciones correctivas. Registra todos los incidentes, nulias, errores detectados, nua	

¿La determinación de las causas de la no conformidad o el incidente que permita eliminar la causa raíz?	Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.				X					X
¿La determinación de si existen no conformidades o incidentes similares, si existen no conformidades, o que potencialmente puedan ocurrir?	La organización debe conservar información documentada adecuada, como evidencia de: f) la naturaleza de las no conformidades y cualquier acción posterior tomada; y				X					X
¿Se implementa cualquier acción necesaria? ¿Y se realiza seguimiento al cumplimiento?	g) los resultados de cualquier acción correctiva.				X					X
¿Se revisa la eficacia de cualquier acción correctiva tomada?					X					
Si fuera necesario, ¿se revisan y actualizan los riesgos y oportunidades determinados durante la planificación y las evaluaciones existentes de los riesgos para la SSG?					X					
Si fuera necesario, ¿se hacen cambios al SGC?					X					
¿Las acciones correctivas son apropiadas a los efectos de las no conformidades encontradas, incluidos los impactos ambientales y los efectos o efectos potenciales de los incidentes?					X					
¿Se conserva información documentada como evidencia de:					X					
¿La naturaleza de las no conformidades y de los incidentes y cualquier acción tomada posteriormente?					X					
¿Los resultados de cualquier acción y acción correctiva, incluyendo su eficacia?					X					
			0	0	15		0	0		8
10.3 MEJORA CONTINUA					0%					
¿Se evidencia la mejora continua de la conveniencia, adecuación y eficacia del SGC para:					X					
¿Se consideran los resultados del análisis y la evaluación, y las salidas de la revisión por la dirección, para determinar si hay necesidades u oportunidades que deben considerarse como parte de la mejora continua?					X					
			0	0	2					

RESUMEN NUMERAL ISO 9001:2015		ISO 9001
10.1 MEJORA CONTINUA	10.1 MEJORA CONTINUA	38%
10.2 NO CONFORMIDAD Y ACCIÓN CORRECTIVA	10.2 NO CONFORMIDAD Y ACCIÓN CORRECTIVA	0%
10.3 MEJORA CONTINUA		0%
PROMEDIO AVANCE		13%

ISO 27001
% AVANCE
50%
0%
25%





4

5

6

7

5.4	Responsabilidades de la dirección	Control La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la Información de acuerdo con la política de seguridad de la Información establecida, las políticas y los procedimientos específicos de la organización en los aspectos correspondientes.				X		<p>La Alta Dirección de Berruit manifiesta de manera verbal su compromiso con la seguridad de la información y exige informalmente su cumplimiento al personal. Sin embargo: No existen políticas o procedimientos documentados que establezcan claramente lineamientos de seguridad de la información.</p> <p>No se ha comunicado formalmente ningún mensaje de la alta dirección que refuerce el cumplimiento de estas prácticas.</p> <p>No se observan acciones visibles de liderazgo en temas de seguridad, como la participación en reuniones de seguimiento, auditorías o firma de comunicados internos.</p> <p>No hay un mecanismo disciplinario formalizado ante posibles incumplimientos de buenas prácticas de seguridad.</p> <p>Aunque los colaboradores reciben certificaciones técnicas impartidas por los fabricantes (lo cual fortalece la competencia técnica del personal), esto no está vinculado directamente al cumplimiento interno de políticas de seguridad de la información, ni representa un mecanismo de control institucional.</p>	<p>Declaración de compromiso con la seguridad (firmada)¶</p> <p>Política de Seguridad de la Información (aprobada)¶</p> <p>Comunicación oficial al personal¶</p> <p>Procedimiento disciplinario por incumplimiento de seguridad¶</p> <p>Registros de participación en actividades del SGSI</p>
5.5	Contacto con las autoridades	Control La organización debe establecer y mantener contacto con las autoridades pertinentes.				X		<p>No ha establecido contacto ni mantiene relaciones con autoridades pertinentes en materia de seguridad de la información, tales como la Superintendencia de Industria y Comercio (SIC), Policía Cibernética, MinTIC u otras entidades regulatorias nacionales.</p> <p>Actualmente:</p> <p>No existe un listado de autoridades relevantes, ni responsables internos designados para tales comunicaciones.</p> <p>No se ha definido cuándo, cómo o quién debe contactar a las autoridades en caso de incidentes de seguridad, filtraciones de datos personales, o cumplimiento normativo.</p> <p>No se cuenta con procedimientos ni registros históricos de interacción con entidades externas en contextos regulatorios, de seguridad o cumplimiento.</p>	<p>Listado de autoridades y contactos clave¶</p> <p>Procedimiento de contacto con autoridades¶</p> <p>Designación del responsable de contacto externo¶</p> <p>Registro de contacto con autoridades (si aplica)</p> <p>Inclusión en plan de respuesta a incidentes (SGSI)</p>
5.6	Contacto con grupos de interés especial	Control La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad			X		<p>Se realiza seguimiento pasivo a contenidos técnicos por LinkedIn, lo que mantiene al personal actualizado en tendencias.</p> <p>Se participa en eventos y capacitaciones ofrecidos por los mayoristas y fabricantes de soluciones de seguridad, quienes también comparten alertas o novedades relevantes.</p>	<p>no mantiene contacto formal ni ha establecido relaciones institucionales con grupos de interés, foros o asociaciones profesionales especializadas en seguridad de la información. Sin embargo, se observan algunas prácticas informales que aportan parcialmente al cumplimiento de este control:</p> <p>No obstante, estas acciones no están documentadas, ni están organizadas bajo una estrategia formal de vigilancia tecnológica ni de participación sectorial.</p>	<p>Lista de fuentes confiables de seguridad¶</p> <p>Registro de asistencia a eventos o capacitaciones¶</p> <p>Designación de responsable de monitoreo técnico¶</p> <p>Procedimiento de vigilancia de amenazas externas¶</p> <p>Registro de alertas relevantes compartidas internamente</p>
5.7	Inteligencia de amenazas	Control La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas.						<p>no cuenta con un mecanismo formal para recopilar, analizar y documentar información sobre amenazas a la seguridad de la información. No obstante:</p> <p>Se reciben verbalmente algunas alertas o recomendaciones de fabricantes a través de mayoristas.</p> <p>Estas alertas se aplican de forma reactiva en acciones como actualizaciones, bloqueos o capacitaciones puntuales, lo cual indica cierta conciencia operacional ante amenazas emergentes.</p> <p>Sin embargo:</p> <p>No existe una fuente técnica sistematizada o lista de referencia (OWASP, CSIRT, MITRE, etc.).</p> <p>No se lleva registro de las amenazas analizadas ni de las decisiones adoptadas como consecuencia de su evaluación.</p> <p>No se genera ni conserva evidencia documental que demuestre una inteligencia de amenazas activa y estructurada.</p>	<p>Establecer una fuente oficial de vigilancia de amenazas, por ejemplo:</p> <p>OWASP</p> <p>CSIRT Colombia (www.csirt.gov.co)</p> <p>Boletines de los fabricantes de antivirus y firewalls usados en la empresa.</p> <p>Diseñar un formato simple de registro de alertas o amenazas que incluya:</p> <p>Fecha, origen de la amenaza, descripción.</p> <p>Evaluación del impacto.</p> <p>Acción tomada (si aplica).</p> <p>Responsable de la decisión.</p> <p>Asignar un responsable de vigilancia de amenazas (puede ser el coordinador o analista TI), quien se encargue de:</p> <p>Recoger amenazas.</p> <p>Socializarlas internamente.</p> <p>Tomar o proponer acciones.</p> <p>Incluir este procedimiento dentro del plan de mantenimiento y operación del SGSI, como parte del enfoque proactivo a la gestión de riesgos.</p> <p>Capacitar al personal técnico en fuentes de inteligencia de amenazas y cómo utilizarlas de manera sistemática.</p>

8	5.8	Seguridad de la Información en la gestión de proyectos	Control La seguridad de la información se debe integrar en la gestión de proyectos			X		no se cuenta con un documento que da los parámetros para la gestión de proyectos, lo que permite realizar una organización sencilla y llevar a cabo los proyectos. Se debe incluir o hacer referencia a los documentos que hablen de la importancia del cuidado y manejo de la información	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con P-ST-15 Desarrollo y Gestión de Proyectos de TI V1.pdf
9	5.9	Inventario de información y otros activos asociados	Control Se debe elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios			X		no se cuenta con un documento de procedimiento de inventario de los activos utilizados y el proceso de control y gestión de activos Realizar registro de la información de inventario, auditoría y verificación de lo plasmado en los registros, y recopilar las evidencias para generar planes de mejora. No se cuenta con un inventario de información	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con P-ST-17 Actualización y Gestión de Licencias de Software V1.pdf P-ST-13 Política de Uso Aceptable de Recursos de TI V1.pdf P-ST-11 Control de Inventario de Activos de TI V1.pdf
10	5.10	Uso aceptable de la información y otros activos asociados	Control Se deben identificar, documentar y implementar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.			X		No se cuenta con un documento que referencie el uso aceptable de los diferentes activos de la compañía, delimitando usos permitidos y no permitidos, indica también las acciones ante incumplimientos en los diferentes usos Documento de evidencia de entendimiento y aceptación de la política de seguridad de la información	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con P-ST-13 Política de Uso Aceptable de Recursos de TI V1.pdf
11	5.11	Devolución de activos	Control El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo			X		No se tiene un documento que referencie el proceso de retorno de activos, en los documentos de control de activos se indique el cuidado y manejo ante pérdidas, detalle como retornar los activos Procedimiento de altas y bajas en el cual se detalla el proceso en conjunto con RRHH para la recolección de activos del usuario, así como la correlación con otros documentos y procesos que apoyan la gestión de activos	Política de Uso Aceptable de Recursos de TI Control de Inventario de Activos de TI
12	5.12	Clasificación de la información	Control La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas			X		Documento que referencie la información (crítica, sensible, importante, etc) y así poder hacer una correcta clasificación de la información que permita complementar la documentación de manejo y cuidado como lo referente backups	Respaldo y Restauración de Datos Respuesta ante Incidentes de Seguridad en TI Pruebas de Recuperación ante Desastres en TI Gestión de Respaldo y Recuperación de Datos
13	5.13	Etiquetado de la información	Control Se debe elaborar y implementar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización.			X		No se cuenta con un documento que referencie la información (crítica, sensible, importante, etc) y así poder hacer una correcta etiquetado de la información que permita complementar la documentación de manejo y cuidado como lo referente backups	Respaldo y Restauración de Datos Respuesta ante Incidentes de Seguridad en TI Pruebas de Recuperación ante Desastres en TI Gestión de Respaldo y Recuperación de Datos
14	5.14	Transferencia de información	Control Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.			X		No se cuenta con un documento que indique el proceso de paso de información cuando se da rotación de la información que se debe retomar de la información del usuario saliente para poder entregarla al nuevo usuario y/o quedar a disposición de los interesados. Este documento puede hacer parte del proceso de altas y bajas que se desarrolle en conjunto con RRHH	
15	5.15	Control de acceso	Control Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la información			X		No se cuenta con un documento que detalle el correcto uso del MFA y los correctivos ante evidencias de no uso, así como los procesos para restablecimiento y/o modificación	
16	5.16	Gestión de identidades	Control Se debe gestionar el ciclo de vida completo de las identidades.			X		No se cuenta con un documento que indique el ciclo de vida de las credenciales utilizadas detallando parámetros de robustecimiento de contraseñas, periodicidad de cambio e importancia del no uso de contraseñas recicladas	
17	5.17	Información de autenticación	Control La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.			X		No se cuenta con un documento que detalle el control de accesos y como se debe gestionar, este documento se debe correlacionar con el de gestión de identidades para reforzar su alcance Asociación con el documento de gestión de identidades y política de seguridad de la información	P-ST-02 Control de Acceso a Sistemas
18	5.18	Derechos de acceso	Control Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.			X		Definición del control y documento que contenga los detalles del proceso, que permita controlar el acceso a la información y/o activos de la organización	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con P-ST-02 Control de Acceso a Sistemas V1.pdf

19	5.19	Seguridad de la información en las relaciones con proveedores	Control Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.				X		Dentro de la política de seguridad de la información se debe detallar e incluir el manejo que se le dará a la información en cada ciente, haciendo referencia que cada uno contará con su política de seguridad de la información	
20	5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	Control Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor				X		Se lleva documento de confidencialidad con cada proveedor junto con los contratos socialización con las partes involucradas al interior y dejar evidencias del entendimiento y conocimiento del documento	
21	5.21	Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)	Control Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.				X		No se cuenta con la documentación de respuesta ante incidencias de seguridad, pruebas de recuperación ante desastres y la gestión de respaldo y recuperación, estos detallan los procesos a realizar para recopilar la información y sus backups así como la restauración al ser requerida o ante desastres Asociar con la clasificación y etiquetado e la información para así gestionar de forma más óptima los procesos de respaldo y restauración	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con P-ST-09 Respuesta ante Incidentes de Seguridad en TI V1.pdf P-ST-14 Pruebas de Recuperación ante Desastres en TI V1.pdf P-ST-19 Gestión de Respaldo y Recuperación de Datos V1.pdf
22	5.22	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	Control La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios.				X		Se lleva proceso de control de cambios para las diferentes actividades programadas de mantenimiento y para aquellas que se presenten extraordinariamente, documentos que soportan las actividades a realizar y los resultados Documento que detalle el correcto diligenciamiento de los planes de trabajo y la socialización de los documentos para el correcto entendimiento	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con P-ST-06 Gestión de Cambios en el Entorno de TI V1.pdf F-ST-09 Formato RFC - Request for Change V1.xlsx
23	5.23	Seguridad de la información para el uso de servicios en la nube	Control Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer, de acuerdo con los requisitos de seguridad de la información de la organización				X		Documento que detalla la gestión que se debe tener al implementar recursos en la nube, y detallando la supervisión y monitoreo continuo, optimización de recursos, manejo de la seguridad y cumplimiento mantenimiento y mejora continua y la gestión de incidentes en la nube Evidencias y documentos que soporte la existencia de los procesos realizados	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con P-ST-12 Gestión de Servicios en la Nube V1.pdf
24	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Control La organización debe planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de				X		Documentos que detallan el manejo, gestión, comunicación, responsabilidades para realizar una correcta gestión a las incidencias reportadas soportes de la socialización y conocimiento por parte de toda la organización.	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con P-ST-01 PROCEDIMIENTO DE SOPORTE TI V1.pdf P-ST-09 Respuesta ante Incidentes de Seguridad en TI V1.pdf P-ST-20 Monitoreo y Gestión de Incidentes en Sistemas de TI V1.pdf P-ST-21 Gestión de Incidentes V1.pdf
25	5.25	Evaluación y decisión sobre eventos de seguridad de la información	Control La organización debe evaluar los eventos de seguridad de la información y debe decidir si clasificarse como incidentes de seguridad de la información				X		No se cuenta con un formato para el registro de los eventos de seguridad que permita tomar decisiones sobre los eventos, así como el seguimiento a los sucesos y los análisis realizados para generar planes de mejora	
26	5.26	Respuesta a incidentes de seguridad de la información	Control Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados.				X		Documentos que detallan el manejo, gestión, comunicación, responsabilidades al momento de presentarse incidentes de seguridad de la información. Soportes de la socialización y conocimiento por parte de toda la organización.	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con P-ST-01 PROCEDIMIENTO DE SOPORTE TI V1.pdf P-ST-09 Respuesta ante Incidentes de Seguridad en TI V1.pdf P-ST-20 Monitoreo y Gestión de Incidentes en Sistemas de TI V1.pdf P-ST-21 Gestión de Incidentes V1.pdf
27	5.27	Aprender de los incidentes de seguridad de la información	Control Los conocimientos adquiridos a partir de incidentes de seguridad de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la información.				X		Por medio del formato para el registro de los eventos de seguridad poder realizar planes de mejora en base a las lecciones aprendidas	
28	5.28	Recopilación de evidencias	Control La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.				X		Por medio del formato para el registro de los eventos de seguridad y definiendo un repositorio que contenga todas las evidencias, acciones tomadas, lecciones aprendidas y planes de mejora. Esto permitiría llevar un correcto seguimiento a las incidencias y lecciones aprendidas	
29	5.29	Seguridad de la información durante una interrupción	Control La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.				X		No se cuenta con un documento de continuidad del negocio que estructure las contingencias y permita dar continuidad ante interrupciones	

30	5.30	Preparación de las TIC para la continuidad de negocio	Control La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC				X		El documento de continuidad del negocio por medio de la identificación de la información crítica, los usuarios relevantes, permite detallar la preparación que se deben tener en cada una de las áreas	
31	5.31	Requisitos legales, legales, reglamentarios y contractuales	Control Los requisitos legales, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.				X	ha identificado de forma parcial los requisitos legales y contractuales relacionados con la seguridad de la información: Se reconoce la Ley 1581 de 2012 como requisito legal aplicable a la protección de datos personales. Se incluye una cláusula de confidencialidad y tratamiento de datos personales en los contratos con los clientes. Se ha publicado en la página web una política de tratamiento de datos personales, en línea con los requisitos normativos colombianos.	No se cuenta con una matriz o listado estructurado de todos los requisitos legales, reglamentarios y contractuales aplicables. No se ha definido un enfoque formal de cumplimiento (cómo se asegura el cumplimiento legal y contractual, cómo se verifica, cómo se actualiza). No hay evidencia de revisión periódica o actualización frente a cambios normativos o contractuales. No se ha asignado un responsable documentado para esta función crítica del SGS.	Matriz de requisitos legales y contractuales❏ Procedimiento de revisión de requisitos❏ Registro de revisiones (firmado o controlado)❏ Evidencia del responsable designado
32	5.32	Derechos de propiedad intelectual	Control La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual.				X	ha tomado acciones parciales y no estructuradas para la protección de los derechos de propiedad intelectual: Se utiliza software con licencias válidas o de uso comercial mediante membresías (como Zoho Mail). Los contratos incluyen cláusulas de propiedad intelectual, lo cual protege en parte los activos de la empresa frente a terceros.	Sin embargo, se identifican importantes brechas frente a los requisitos de este control: No se cuenta con una política o procedimiento que defina cómo proteger los DPI. No hay un inventario de software con licencias activas, lo cual impide una trazabilidad clara de cumplimiento. No se han definido controles para evitar el uso de software no autorizado, ni hay restricciones formales sobre contenidos protegidos por derechos de autor. La propiedad intelectual generada por Berruit (ej. plantillas, scripts, diseños) no está identificada ni protegida explícitamente.	Política de uso de software y protección de DPI❏ Inventario de software y licencias❏ Contratos con cláusulas sobre propiedad intelectual❏ Procedimiento de revisión de licencias❏ Registro de activos intangibles desarrollados
33	5.33	Protección de registros	Control Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados					X	genera registros relacionados con sus procesos, tales como informes, actas de entrega, contratos y reportes de plataformas como GLP y Centreon. Sin embargo: Todos los registros se encuentran almacenados en el computador o el OneDrive del Director Manager, o en su cuenta de correo electrónico. El acceso está restringido solo al Director Manager, o eventualmente al colaborador que los elabora, lo que impide trazabilidad organizacional y gestión compartida. No se han establecido controles de respaldo, autenticidad, control de acceso por roles, integridad ni trazabilidad. No existe un procedimiento de gestión de registros, ni lineamientos sobre tiempos de conservación, estructuras de almacenamiento ni protección contra pérdida, modificación o acceso no autorizado. Esto constituye una debilidad crítica en la protección, disponibilidad y trazabilidad de la información documentada que respalda la operación y cumplimiento de requisitos del SGS.	Procedimiento para la gestión de registros❏ Estructura de carpetas compartidas en OneDrive o SharePoint❏ Registro de copias de seguridad de registros críticos❏ Control de acceso por usuario y rol Registro de cambios / control de versiones
34	5.34	Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés)	Control La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales					X	Un documento que referencie el control y cuidado sobre la privacidad y protección de la información, que se de a conocer a la organización y se registre su entendimiento	
35	5.35	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se debe revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos					X	La documentación para la gestión de seguridad de la información cuenta con controles de revisión y versionamiento, que permite registrar los cambios y/o actualizaciones realizados a la documentación	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con los siguientes documentos P-ST-02 Control de Acceso a Sistemas V1.pdf P-ST-06 Gestión de Cambios en el Entorno de TI v1.pdf P-ST-09 Respuesta ante Incidentes de Seguridad en TI V1.pdf P-ST-13 Política de Uso Aceptable de Recursos de TI V1.pdf P-ST-21 Gestión de Incidentes V1.pdf P-ST-22 Gestión de requerimientos V1.pdf
36	5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información	Control El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.					X	La documentación para la gestión de seguridad de la información cuenta con controles de revisión y versionamiento, que permite registrar los cambios y/o actualizaciones realizados a la documentación	En la ruta Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con los siguientes documentos P-ST-02 Control de Acceso a Sistemas V1.pdf P-ST-06 Gestión de Cambios en el Entorno de TI v1.pdf P-ST-09 Respuesta ante Incidentes de Seguridad en TI V1.pdf P-ST-13 Política de Uso Aceptable de Recursos de TI V1.pdf P-ST-21 Gestión de Incidentes V1.pdf P-ST-22 Gestión de requerimientos V1.pdf
37	5.37	Procedimientos operativos documentados	Control Los procedimientos operativos de las instalaciones de procesamiento e la información se debe documentar y poner a disposición del personal que los necesite					X	La información esta contenida en un Sharepoint organizacional al que tienen acceso los usuarios por medio de sus credenciales asignadas, allí pueden consultar la documentación en el momento en que se desee	En la ruta de SharePoint Berruit\SGC - 2. SOPORTE TÉCNICO se cuenta con la diferente documentación
				0	0	4	32			
6	CONTROLES DE PERSONAS						13%			

38	6.1	RESPONSABILIDAD DE LA DIRECCIÓN	Control Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos				X		no ha implementado controles específicos ni documentados para realizar verificaciones de antecedentes previas o posteriores a la vinculación del personal. No se ha evidenciado una política formal, ni un formato de validación, ni consideraciones diferenciadas por nivel de riesgo o tipo de información que la persona pueda manejar. Esto implica un riesgo directo a la confidencialidad, integridad y disponibilidad de la información en caso de incidentes internos (errores o amenazas intencionales).	Procedimiento de verificación de antecedentes Formato de validación de antecedentes Clasificación de cargos según nivel de riesgo Cláusula contractual de integridad y antecedentes
39	6.2	Términos y condiciones de empleo	Control Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información				X			
40	6.3	Conciencia de seguridad de la información, educación y formación	Control El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral			X		Se realizan las socializaciones sobre la documentación y su aplicación en las actividades laborales	Registros de las socializaciones y documentos de aceptación y entendimiento de los documentos	
41	6.4	Proceso disciplinario	Control Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información				X			
42	6.5	Responsabilidades después de la terminación o cambio de empleo	Control Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se debe definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas				X			
43	6.6	Acuerdos de confidencialidad o no divulgación	Control Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.				X			
44	6.7	Trabajo remoto	Control Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización			X				

45	6.8	Informes de eventos de seguridad de la información	Control La organización debe proporcionar un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados				X			
				0	0	2	6			
	7	CONTROLES FÍSICOS		23%						
46	7.1	Perímetros de seguridad física	Control Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.				X			
47	7.2	Entrada física	Control Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados	X						
48	7.3	Asegurar oficinas, habitaciones e instalaciones	Control Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.	X						
49	7.4	Monitoreo de la seguridad física	Control Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados	X						
50	7.5	Protección contra amenazas físicas y ambientales	Control Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.				X	Se realizan capacitaciones y charlas sobre seguridad en el trabajo de forma periódica con los empleados		Evaluaciones de las capacitaciones realizadas
51	7.6	Trabajar en áreas seguras	Control Se deben diseñar e implementar medidas de seguridad para trabajar en zonas seguras				X	Se realizan capacitaciones y charlas sobre seguridad en el trabajo de forma periódica con los empleados		Evaluaciones de las capacitaciones realizadas
52	7.7	Escritorio y pantalla limpios	Control Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información.				X	Se realizan capacitaciones y charlas sobre seguridad en el trabajo de forma periódica con los empleados		Evaluaciones de las capacitaciones realizadas
53	7.8	Emplazamiento y protección de equipos	Control El equipo debe estar situado de forma segura y protegida				X			
54	7.9	Seguridad de los activos fuera de las instalaciones	Control Los activos externos deben estar protegidos.			X			Se debe contemplar en la política de seguridad de la información en uso adecuado de los equipos fuera de las instalaciones laborales.	
55	7.10	Medios de almacenamiento	Control Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización				X			
57	7.11	Servicios públicos de apoyo	Control Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos			X				
	7.12	Seguridad del cableado	Control Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños.			X				
58	7.13	Mantenimiento de equipos	Control El equipo se debe mantener correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.			X				

59	7.14	Disposición o reutilización segura de los equipos	Control Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización.			X				
				3	0	5	6			
	8	CONTROLES TECNOLOGICOS		25%						
60	8.1	Dispositivos de punto final de usuario	Control Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario				X			
61	8.2	Derechos de acceso privilegiado	Control La asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.				X			
62	8.3	Restricción de acceso a la información	Control El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.				X			
63	8.4	Acceso al código fuente	Control El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente	X						
64	8.5	Autenticación segura	Control Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.			X				
65	8.6	Gestión de la capacidad	Control El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidad actuales y previstas.			X				
66	8.7	Protección contra malware	Control La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.			X				
67	8.8	Gestión de vulnerabilidades técnicas	Control Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas.			X				
68	8.9	Gestión de la configuración	Control Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.			X				
69	8.10	Eliminación de información	Control La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesario				X			
70	8.11	Enmascaramiento de datos	Control El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas relacionadas con temas específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable				X			

71	8.12	Prevención de fugas de datos	Control Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.			X				
72	8.13	Copia de seguridad de la información	Control Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos				X			
73	8.14	Redundancia de las instalaciones de procesamiento de información	Control Las instalaciones de procesamiento de la información se deben implantar con redundancia suficiente para cumplir los requisitos de disponibilidad				X			
74	8.15	Registro	Control Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar				X			
75	8.16	Actividades de seguimiento	Control Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.			X				
76	8.17	Sincronización de reloj	Control Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas.			X				
77	8.18	Uso de programas de utilidad privilegiados	Control El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación debe restringirse y controlarse estrictamente.			X				
78	8.19	Instalación de software en sistemas operativos	Control Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos				X			
79	8.20	Seguridad de redes	Control Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.			X				
80	8.21	Seguridad de los servicios de red	Control Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.			X				
81	8.22	Segregación de redes	Control Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización.			X				
82	8.23	Filtrado web	Control El acceso a sitios web externos se debe gestionar para reducir la exposición a contenido malicioso.			X				
83	8.24	Uso de la criptografía	Control Se debe definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.				X			

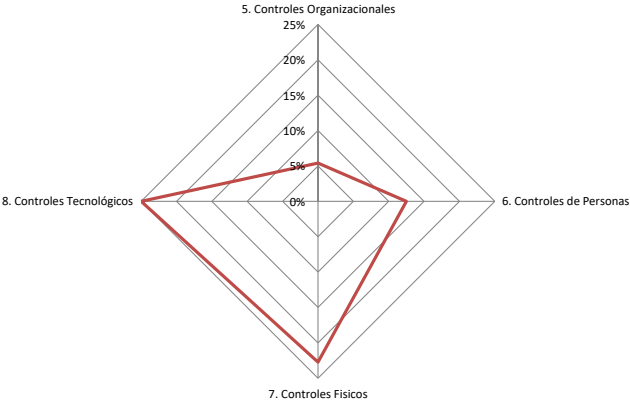
84	8.25	Ciclo de vida de desarrollo seguro	Control Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas	X						
85	8.26	Requisitos de seguridad de las aplicaciones	Control Los requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones			X				
86	8.27	Arquitectura de sistemas seguros y principios de ingeniería	Control Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener y implementar a cualquier actividad de desarrollo de sistemas de información				X			
87	8.28	Codificación segura	Control Los principios de codificación segura se deben implementar al desarrollo de programas informáticos	X						
88	8.29	Pruebas de seguridad en el desarrollo y aceptación	Control Los procesos de ensayo de seguridad se deben definir y implementar en el ciclo de vida del desarrollo	X						
89	8.30	Desarrollo externalizado	Control La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados	X						
90	8.31	Separación de entornos de desarrollo, evidencia y producción	Control Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos	X						
91	8.32	Gestión del cambio	Control Los cambios en las instalaciones de procesamiento de la información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios				X			
92	8.33	Información de las pruebas	Control La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente				X			
93	8.34	Protección de los sistemas de información durante las pruebas de auditoría	Control Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el probador y la dirección adecuada				X			
				6	0	14	14			

Fuente: NTC-ISO-IEC 27001:2022

5
6
7
8

CAPÍTULOS	NIVEL DE IMPLEMENTACIÓN NIVEL ACTUAL
5. Controles Organizacionales	5%
6. Controles de Personas	13%
7. Controles Fisicos	23%
8. Controles Tecnológicos	25%
PROMEDIO	16%

CONTROLES ANEXO A





ISO 9001:2015

RESUMEN ISO 9001:2015

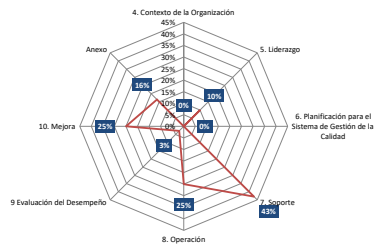


NTC ISO 9001:2015

NUMERALES DE LA NORMA	% IMPLEMENTACIÓN
4. Contexto de la Organización	15%
5. Liderazgo	10%
6. Planificación para el Sistema de Gestión de la Calidad	0%
7. Soporte	48%
8. Operación	23%
9. Evaluación del Desempeño	0%
10. Mejora	13%
TOTAL GENERAL	15%

ISO 27001:2022

RESUMEN ISO 27001:2022

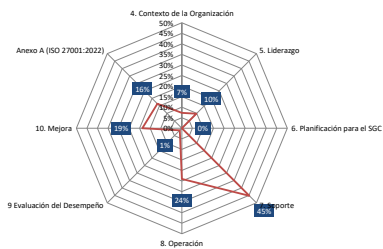


ISO/IEC 27001:2022

NUMERALES DE LA NORMA	% IMPLEMENTACIÓN
4. Contexto de la Organización	0%
5. Liderazgo	10%
6. Planificación para el Sistema de Gestión de la Calidad	0%
7. Soporte	43%
8. Operación	25%
9. Evaluación del Desempeño	3%
10. Mejora	25%
Anexo	16%
TOTAL GENERAL	15%

CONSOLIDADO ISO 9001:2015 E ISO 27001:2022

RESUMEN NTC-ISO 9001:2015 ISO/IEC 27001:2022

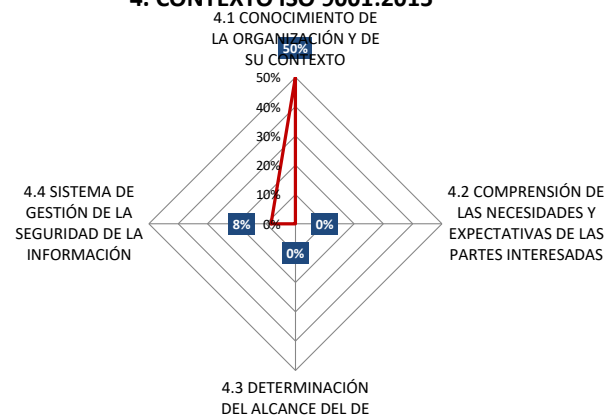


CONSOLIDADO NTC-ISO 9001:2015 ISO/IEC 27001:2022

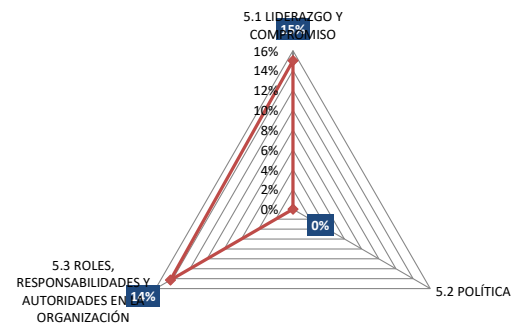
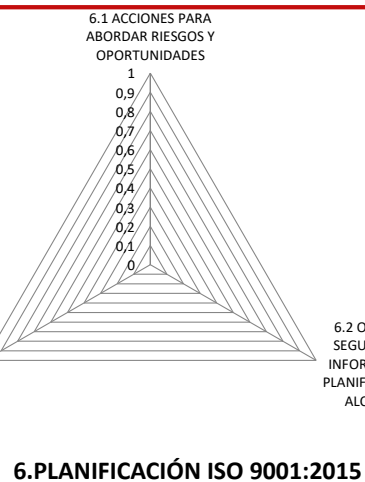
NUMERALES DE LA NORMA	% IMPLEMENTACIÓN
4. Contexto de la Organización	7%
5. Liderazgo	10%
6. Planificación para el SGC	0%
7. Soporte	45%
8. Operación	24%
9. Evaluación del Desempeño	1%
10. Mejora	19%
Anexo A (ISO 27001:2022)	16%
TOTAL GENERAL	15%



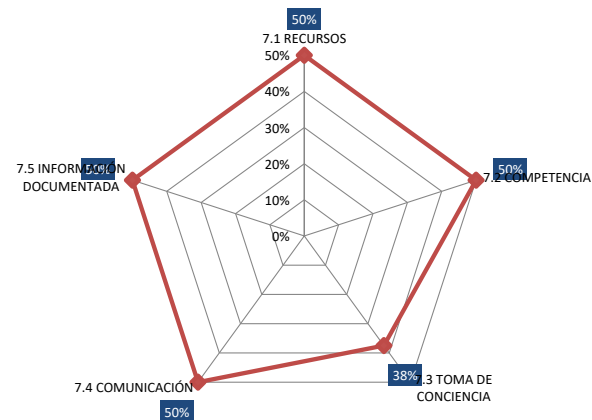
4. CONTEXTO ISO 9001:2015



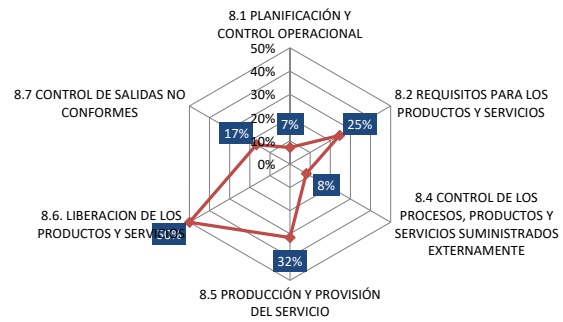
5. LIDERAZGO ISO 9001:2015



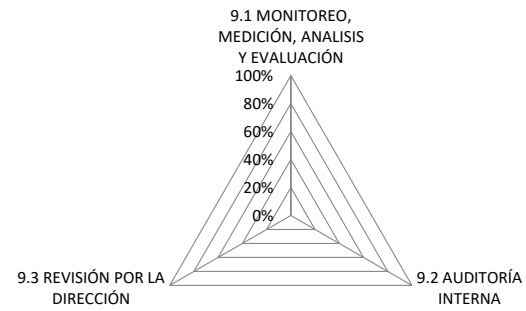
7.SOPORTE ISO 9001:2015



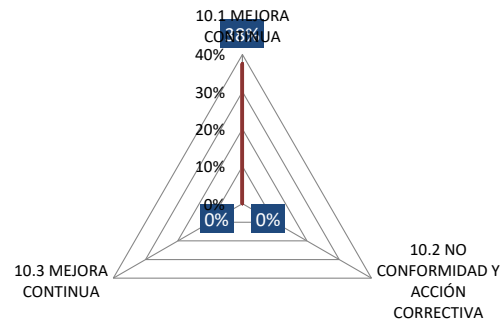
8. OPERACIÓN ISO 9001:2015



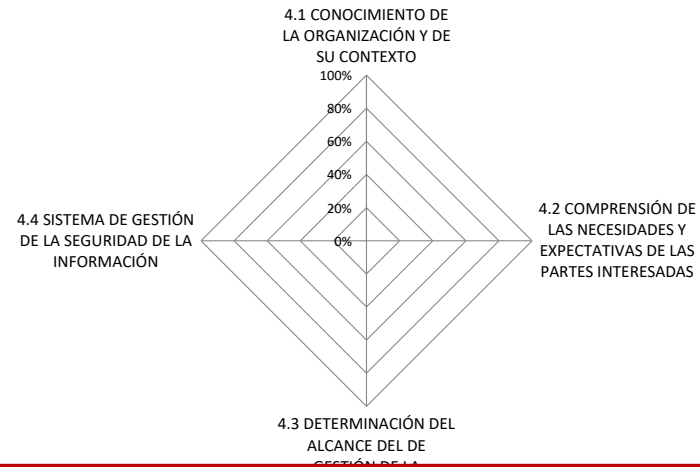
9 EVALUACIÓN DEL DESEMPEÑO ISO 9001:2015



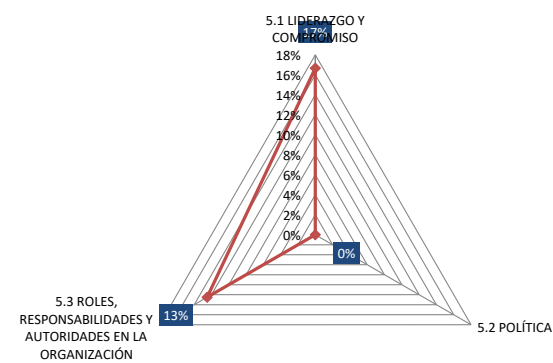
10 MEJORA CONTINUA ISO 9001:2015



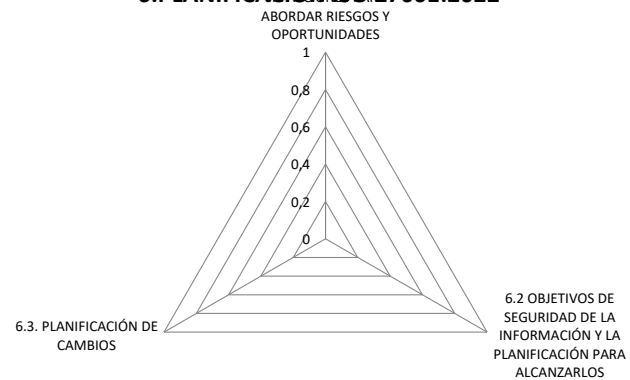
4. CONTEXTO ISO 27001:2022



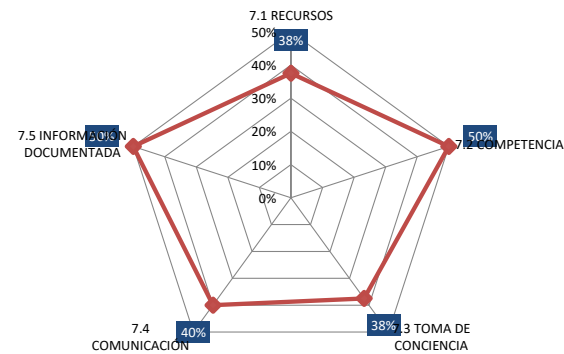
5. LIDERAZGO ISO 27001:2022



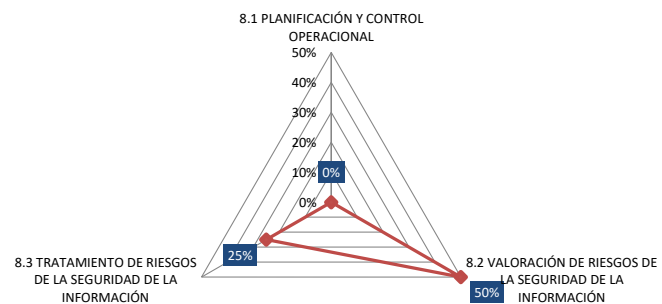
6. PLANIFICACIÓN ISO 27001:2022



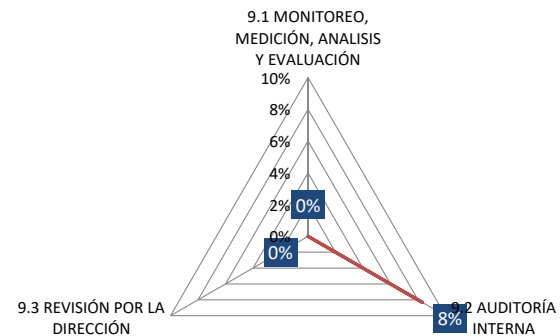
7. SOPORTE ISO 27001:2022



8. OPERACIÓN ISO 27001:2022



9 EVALUACIÓN DEL DESEMPEÑO ISO 27001:2022



10 MEJORA CONTINUA ISO 27001:2022

