Estado actual controles

Area	Definiciones	% Cumplimiento
	Controles	
A.5	A.5 políticas de seguridad de la información	55
A.6	A.6 organización de la seguridad de la información	20
A.7	A.7 seguridad en los recursos humanos	0
A.8	A.8 gestión de activos	40
A.9	A.9 Control de accesos	85
A.10	A.10 Criptografía	0
A.11	A.11 Seguridad física y ambiental	60
A.12	A.12 Seguridad en las operaciones	40
A.13	A.13 Seguridad en las comunicaciones	60
A.14	A.14 Adquisición, desarrollo y mantenimiento de sistemas	80
A.15	A.15 Relaciones con proveedores	90
A.16	A.16 Gestión de incidentes de seguridad de la información	60
A.17	A.17 Aspectos de seguridad de la información dentro de la continuidad del negocio	20
A.18	A.18 Conformidad	40

Estado actual requisitos

Requisitos	% Cumplimiento
4. contexto	40%
5. liderazgo	30%
6. planificacion	40%
7. soporte	70%
8.operacion	65%
9.evaluacion desempeño	0%
10. mejora	10%

Anexo A de referencia	Título de control	Descripción del control	Función	Status	Hallazgos
A.5	Políticas de seguridad de la información				
5.1	Directrices de la Dirección en seguridad de la información.				
5.1.1	Conjunto de políticas para la seguridad de la información	Existe un documento. Más se requiere su actualización a la nueva plataforma		MD	Está documentado, se pone en práctica pero falta la formalización
5.1.2	Revisión de las políticas para la seguridad de la información	No se ha realizado la revisión por parte de la alta gerencia		MD	Está documentado, se pone en práctica pero falta la formalización
A.6	Aspectos Organizativos De La Seguridad De La Información				
6.1	Organización interna.				
6.1.1	Asignación de responsabilidades para la segur. de la información	No existe una designación formal de estas responsabilidades		RD	El control está diseñado pero no se ajusta a la norma
6.1.2	Segregación de tareas			RD	No se realiza mediante medios convencionales
6.1.3	Contacto con las autoridades			RD	No está establecido
6.1.4	Contacto con grupos de interés especial			MD	
6.1.5	Seguridad de la información en la gestión de proyectos.	No existe		MD	
6.2	Dispositivos para movilidad y teletrabajo.				
6.2.1	Política de uso de dispositivos para movilidad			RD	
6.2.2	Teletrabajo	En formulación		RD	Aunque existe una política del estado Colombiano, en la entidad no se ha establecido el proceso, ni mucho menos los controles
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS				
7.1	Antes de la contratación.				
7.1.1	Investigación de antecedentes			MD	Depende de recursos humanos y no se tiene claridad si se hace o no
7.1.2	Términos y condiciones de contratación.			MD	Depende de recursos humanos y no se tiene claridad si se hace o no
7.2	Durante la contratación				
7.2.1	Responsables de gestión			D	
7.2.2	Concienciación, educación y capacitación en seguridad de la información.			RD	No está establecido
7.2.3	Proceso disciplinario			RD	Depende dejuridica y no se tiene claridad si se hace o no
7.3	Cese o cambio de puesto de trabajo.				
7.3.1	Cese o cambio de puesto de trabajo.			RD	No se hace
A.8	Gestión de activos				
8.1	Responsabilidad sobre los activos				
8.1.1	Inventario de activos.			MD	
8.1.2	Propiedad de los activos			MD	
8.1.3	Uso aceptable de los activos.			MD	El control se diseñó, se aplica pero no se alinea con la norma
8.1.4	Devolución de activos.			MD	no se utiliza
8.2	Clasificación de la información				
8.2.1	Directrices de clasificación.			RD	El control se diseñó y aplica, pero no está ajustado del todo con la norma
8.2.2	Etiquetado y manipulado de la información			RD	El control se diseñó y aplica, pero no está ajustado del todo con la norma
8.2.3	Manipulación de activos			RD	El control se diseñó y aplica, pero no está ajustado del todo con la norma
8.3	Manejo de los soportes de almacenamiento				
8.3.1	Gestión de soportes extraibles			RD	
8.3.2	Eliminación de soporte			PNP	no se hace
8.3.3	Soportes físicos en transito			RD	no se hace seguimiento
A.9	Control de accesos				
9.1	Requisitos de negocio para el control de accesos.				
9.1.1	Política de control de accesos			MD	
9.1.2	Control de acceso a las redes y servicios asociados.			MD	
9.2	Gestión de acceso de usuario.				
9.2.1	Gestión de altas/bajas en el registro de usuarios.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
9.2.2	Gestión de los derechos de acceso asignados a usuarios.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
9.2.3	Gestión de los derechos de acceso con privilegios especiales.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
9.2.4	Gestión de información confidencial de autenticación de usuarios.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
9.2.5	Revisión de los derechos de acceso de los usuarios.			RD	
9.2.6	Retirada o adaptación de los derechos de acceso			MD	Falta formalizar la política
9.3	Responsabilidades del usuario				
9.3.1	Uso de información confidencial para la autenticación			MD	
9.4	Control de acceso a sistemas y aplicaciones.				
9.4.1	Restricción del acceso a la información.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
9.4.2	Procedimientos seguros de inicio de sesión.			MD	
9.4.3	Gestión de contraseñas de usuario.			MD	
9.4.4	Uso de herramientas de administración de sistemas.			MD	
9.4.5	Control de acceso al código fuente de los programas.			NA (Not Applicable)	
A.10	Cifrados				
10.1	Controles criptográficos				
10.1.1	Política de uso de los controles criptográficos			RD	No se trabaja controles criptográficos
10.1.2	Gestión de claves			RD	No se trabaja controles criptográficos
A.11	Seguridad física y ambiental				
11.1	Areas seguras				
11.1.1	Perímetro de seguridad física.			MD	
11.1.2	Controles físicos de entrada.			MD	
11.1.3	Seguridad de oficinas, despachos y recursos.			MD	Hasta ahora estan conformando el equipo que maneja la seguridad de oficinas
11.1.4	Protección contra las amenazas externas y ambientales.			MD	
11.1.5	El trabajo en áreas seguras.			MD	
11.1.6	Áreas de acceso público, carga y descarga			MD	
11.2	Seguridad de los equipos				
11.2.1	Emplazamiento y protección de equipos.			RD	
11.2.2	Instalaciones de suministro.			RD	

11.2.3	Seguridad del cableado.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
11.2.4	Mantenimiento de los equipos.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
11.2.5	Salida de activos fuera de las dependencias de la empresa.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.			RD	
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.			RD	no hay un proceso establecido para esto
11.2.8	Equipo informático de usuario desatendido.			RD	
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla			MD	
A.12	SEGURIDAD EN LA OPERATIVA				
12.1	Responsabilidades y procedimientos de operación				
12.1.1	Documentación de procedimientos de operación.			PNP	No existe
12.1.2	Gestión de cambios.			RD	
12.1.3	Gestión de capacidades.			RD	
12.1.4	Separación de entornos de desarrollo, prueba y producció			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
12.2	Protección contra código malicioso				
12.2.1	Controles contra el código malicioso			RD	
12.3	Copias de seguridad				
12.3.1	Copias de seguridad de la información			MD	
12.4	Registro de actividad y supervisión				
12.4.1	Registro y gestión de eventos de actividad.			MD	
12.4.2	Protección de los registros de información.			RD	no se ha establecido
12.4.3	Registros de actividad del administrador y operador del sistema.			RD	no hay seguimiento ni control ni procedimiento
12.4.4	Sincronización de relojes			MD	No se realiza formalmente
12.5	Control de software en explotación				
12.5.1	Instalación del software en sistemas en producción			MD	
12.6	Gestión de la vulnerabilidad técnica				
12.6.1	Gestión de las vulnerabilidades técnicas.			MD	
12.6.2	Restricciones en la instalación de software			MD	
12.7	Consideraciones de las auditorías de los sistemas de información				
12.7.1	controles de auditoría de los sistemas de información			MD	
A.13	Seguridad en las telecomunicaciones				
13.1	Gestión de la seguridad en las redes				
13.1.1	Controles de red.			MD	Hasta ahora van a comenzar su formulación
13.1.2	Mecanismos de seguridad asociados a servicios en red.			MD	
13.1.3	Segregación de redes			MD	
13.2	Intercambio de información con partes externas				
13.2.1	Políticas y procedimientos de intercambio de información.			RD	
13.2.2	Acuerdos de intercambio.			RD	
13.2.3	Mensajería electrónica.			RD	
13.2.4	Acuerdos de confidencialidad y secreto.			RD	No están formalizados a pesar de que existe un documento. Solo en contadas ocasiones los trabajan
A.14	Adquisición, desarrollo y mantenimiento de sistemas				
14.1	Requisitos de seguridad de los sistemas de información				
14.1.1	Análisis y especificación de los requisitos de seguridad.			MD	
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas			MD	
14.2	Seguridad en los procesos de desarrollo y soporte				
14.2.1	Política de desarrollo seguro de software.			RD	No existe
14.2.2	Procedimientos de control de cambios en los sistemas.			RD	No existe
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo			RD	No existe
14.2.4	Restricciones a los cambios en los paquetes de software.			MD	
14.2.5	Uso de principios de ingeniería en protección de sistemas.			MD	
14.2.6	Seguridad en entornos de desarrollo.			RD	No existe
14.2.7	Externalización del desarrollo de software.			MD	No existe
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.			RD	
14.2.9	Pruebas de aceptación.			RD	
14.3	Daños de prueba				
14.3.1	Protección de los datos utilizados en pruebas			MD	
A.15	RELACIONES CON SUMINISTRADORES				
15.1	Seguridad de la información en las relaciones con suministradores				
15.1.1.	Política de seguridad de la información para suministradores.			RD	
15.1.2	Tratamiento del riesgo dentro de acuerdos con suministradores			RD	
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones			RD	
15.2	Gestión de la prestación del servicio por suministradores				
15.2.1	Supervisión y revisión de los servicios prestados por terceros.			RD	
15.2.2	Gestión de cambios en los servicios prestados por terceros			RD	
A.16	Gestión de incidentes de seguridad de la información				
16.1	Gestión de incidentes de seguridad de la información y mejoras				
16.1.1	Responsabilidades y procedimientos.			MD	
16.1.2	Notificación de los eventos de seguridad de la información.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
16.1.3	Notificación de puntos débiles de la seguridad.			MD	
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
16.1.5	Respuesta a los incidentes de seguridad.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
16.1.6	Aprendizaje de los incidentes de seguridad de la información.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
16.1.7	Recopilación de evidencias			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
A.17	Aspectos de seguridad de la información dentro de la continuidad del negocio				
17.1	Continuidad de la seguridad de la información				
17.1.1	Planificación de la continuidad de la seguridad de la información			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma
17.1.2	implantación de la continuidad de la seguridad de la información.			RD	
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información			RD	
17.2	Redundancias				
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información			RD	
A.18	Cumplimiento				

18.1	Cumplimento de los requisitos legales y contractuales				
18.1.1	Identificación de la legislación aplicable.			MD	
18.1.2	Derechos de propiedad intelectual (DPI).			MD	Hay un control que no cumple con las normas. Debe ser rediseñado
18.1.3	Protección de los registros de la organización.			MD	
18.1.4	Protección de datos y privacidad de la información personal.			MD	El control se realiza pero falta su documentación formal. Está alineado con la norma y las leyes y políticas existentes en el país
18.1.5	Regulación de los controles criptográficos			RD	no existe
18.2	Revisiones de la seguridad de la información				
18.2.1	Revisión independiente de la seguridad de la información.			RD	no existe
18.2.2	Cumplimiento de las políticas y normas de seguridad.			RD	no existe
18.2.3	Comprobación del cumplimiento			RD	no existe

Cantidad	Códigos Status	Significado	%	Contribución %
1	D	El control se documentó e implementó	100	1%
61	MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	90	54%
48	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	50	43%
2	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	0	2%
0	NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio		0%
112				

El análisis de brechas: estado de aplicación de ISO 27001

ISO 27001 clausulas	Requisito obligatorio para el SGSI	Status	Buscar	Hallazgos	Recomendaciones
4	**Contexto de la organización**				
4,1	**Conocimiento de la organización y de su contexto**				
4,1	La empresa debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito…….	**DEF**			
4,2	**Comprensión de las necesidades y expectativas de las partes interesadas**				
4.2.1 (a)	determinar las partes interesadas que son pertinentes al SGSI	**PNP**			
4.2.1 (b)	Los requisitos de las partes interesadas	**PNP**			
4.3	**Determinación del alcance del SGSI**				
4.3(a)	Para determinar los límites y la aplicabilidad del SGSI se debe considerar los aspectos internos y externos referidos en 4.1	**RD**			
4.3(b)	Considerar los requisitos referidos en 4.2	**RD**			
4.3 c	Considerar las interfaces y dependencias entre las actividades realizadas y las que realizan otras empresas	**RD**			
5	**Liderazgo**				
5.2	**Política**				
5.2(a)	La alta direccion establece una política que sea adecuada al propósito de la empresa	**RD**			
5.2b)	La política incluye objetivos de seguridad de la información o proporciona el marco para el establecimiento de los mismos	**RD**			
5.2(c)	La alta direccion establece una política que incluye un compromiso de cumplir los requisitos aplicables relacionados con la seguridad	**RD**			
5.2(d)	La alta direccion establece una política que incluye un compromiso de mejora continua	**RD**			
5.2(e)	La alta direccion establece una política que está como información documentada	**RD**			
5.2(f)	La alta direccion establece una política que permite comunicarse dentro de la empresa	**RD**			
5.2(g)	La alta direccion establece una política que permite estar disponible por las partes interesadas, según sea apropiado	**RD**			
6	**Planificación**				
6.1	**acciones para tratar riesgos y oportunidades**				
6.1.2	**Evaluación de riesgos de la seguridad de la informacion**				
6.1.2 (a)	Establecer y mantener criterios de riesgo de seguridad que incluyen criterios de aceptación de riesgos y criterios para realizar evaluaciones de riesgos	**RD**			
6.1.2 (b)	Asegurar que las evaluaciones repetidas de riesgos producen resultados consistentes, válidos y comparables	**RD**			
6.1.2 (c)	Identificar los riesgos	**MD**			
6.1.2 (d)	Analizar los riesgos	**MD**			
6.1.2 (e)	Evaluar los riesgos	**MD**			
6.1.3	**Tratamiento de riesgos de la seguridad de la información**				
6.1.3 (a)	Seleccionar las opciones apropiadas de tratamiento de riesgos, teniendo en cuenta los resultados de la evaluación de riesgos	**PNP**			
6.1.3 (b)	Determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos	**RD**			
6.1.3 (c)	comparar los controles determinados en 6.1.3 (b) con los del anexo A y verificar que no se han omitido controles	**RD**			
6.1.3 (d)	Elaborar una declaración de aplicabilidad que tenga los controles necesarios y la justificación de las exclusiones, que sea que se implementen o no y la justificación para las exclusiones	**RD**			
6.1.3 (e)	formular un plan de tratamiento de riesgos	**RD**			
6.1.3 (f)	Obtener la aprobación del plan de tratamiento de riesgos y la aceptación de riesgos residuales por parte de los dueños de los riesgos	**RD**			
6.2	**Objetivos de seguridad de la información y planes para lograrlos**				
6.2 (a)	Los objetivos deben Ser coherentes con la política	**RD**			
6.2 (b)	Ser medibles (Si es posible)	**RD**			
6.2 (c)	Tener en cuenta los requisitos de seguridad aplicables, y los resultados de la evaluación y del tratamiento de riesgos	**RD**			
6.2 (d)	ser comunicados	**RD**			
6.2 (e)	Ser actualizados	**RD**			
6.2 (f)	Cuando se planifica para lograr los objetivos se debe determinar lo que se va a hacer	**RD**			

6.2 (g)	Cuando se planifica para lograr los objetivos se debe determinar los recursos requeridos	**RD**			
6.2 (h)	Cuando se planifica para lograr los objetivos se debe determinar el responsable	**RD**			
6.2 (i)	Cuando se planifica para lograr los objetivos se debe determinar cuando se finalizará	**RD**			
6.2 (j)	Cuando se planifica para lograr los objetivos se debe determinar como se evaluarán los resultados	**RD**			
7	**SOPORTE**				
7.1	**Recursos: se debe determinar y proporcionar los recursos**	**RD**			
7.2	**Competencia**	**DEF**			
7.2 (a)	Determinar la competencia de las personas que realizan un trabajo que afecte el desempeño de la seguridad de la información	**DEF**			
7.2 (b)	Asegurar que las personas sean competentes, basándose en: educación, formación o experiencias adecuadas	**DEF**			
7.2 (c)	Tomar acciones para adquirir las competencias necesarias y evaluar su eficacia (cuando sea aplicable)	**DEF**			
7.2 (d)	Conservar la información documentada apropiada como evidencia	**DEF**			
7.3	**Toma de conciencia**				
7.3 (a)	Las personas deben tomar conciencia de la política	**PNP**			
7.3 (b)	Las personas deben tomar conciencia de su contribución a la eficacia, incluyendo los beneficios de una mejora del desempeño	**PNP**			
7.3 (c)	Las personas deben tomar conciencia de las implicaciones de la NO conformidad con los requisitos del SGSI	**PNP**			
7.4	**Comunicación**				
7.4 (a)	Se debe determinar la necesidad de comunicaciones internas y externas que incluyan l contenido de la comunicación	**RD**			
7.4 (b)	Se debe determinar la necesidad de comunicaciones internas y externas que incluyan cuando comunicar	**RD**			
7.4 (c)	Se debe determinar la necesidad de comunicaciones internas y externas que incluyan a quien comunicar	**RD**			
7.4 (d)	Quien debe comunicar	**RD**			
7.4 (e)	Los procesos para llevar a cabo la comunicación (divulgación)	**RD**			
7.5	**información documentada**				
7.5.1	**Generalidades**				
7.5.1 (a)	Incluir información documentada requerida por la norma	**RD**			
7.5.1 (b)	Incluir información documentada que la empresa determine que es necesaria para la eficacia del SGSI	**REP**			
7.5.2	**Creación y actualización**				
7.5.2 (a)	Asegurar la identificación y descripción cuando se crea o actualiza información documentada	**REP**			
7.5.2 (b)	cuando se crea o actualiza información documentada se asegura el formato y sus medios de soporte	**REP**			
7.5.2 (c)	cuando se crea o actualiza información documentada se debe asegurar la revisión y aprobación con respecto a la idonieidad y adecuación	**REP**			
7.5.3	**Control de la información documentada**				
7.5.3 (a)	La información documentada se debe controlar para asegurar que esté disponible y adecuada para su uso, cuando y donde se requiere	**RD**			
7.5.3 (b)	La información documentada se debe controlar para asegurar que esté protegida adecuadamente	**RD**			
7.5.3 (c)	para controlar la información se debe tratar la distribución, acceso, recuperación y uso	**RD**			
7.5.3 (d)	Se realiza almacenamiento y preservación, incluido legibilidad	**REP**			
7.5.3 (e)	Hacer controles de cambios	**REP**			
7.5.3 (f)	Realizar retención y disposición	**RD**			
8	**OPERACIÓN**				
8.1	**Planificación y control operacional**	**RD**			
8.2	Evaluacion de riesgos según los criterios establecidos en 6.1.2 (a)	**RD**			
8.3	Tratamiento de riesgos de la seguridad de la información	**RD**			

Leyenda				
Cantidad	**Codigos Status**	**Significado**		**Contribution %**

0	**D**	El control se documentó e implementó. Está siendo monitoreado y mejorado constantemente		**0%**
3	**MD**	El Control se lleva a cabo y está completo; el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos. Recientemente comenzó a operar		**5%**
6	**DEF**	El control y Los procedimientos están mas o menos completos y/o aún no se han implementado; además el control no ha sido socializado por la alta dirección		
6	**REP**	El control no cumple con las normas/no hay capacitación oo comunicación formal de procedimientos estándar		
41	**RD**	El control no cumple las normas y debe ser rediseñado para cumplir con las normas		**66%**
6	**PNP**	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)		**10%**
0	**NA (No Aplicable)**	El control no es aplicable para la empresa ni para el negocio		**0%**
62				

%	Estado	Descripción Criterios clasificación
0	Inexistente (pnp)	Ausencia total de políticas, procedimientos, no hay documentación
10	Inicial (RD)	Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser re sueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso.
50	Repetible (REP)	Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona
70	Definida (DEF)	Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes
90	Gestionado (MD)	El control se implementó pero no se documentó . Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usa la automatización y herramientas en una forma limitada o fragmentada.
100	Optimizado (D)	El control se implementó y se documentó

Estado implementación 27001 contra clausulas (cláusulas en D)

Clausulas ISO	Cantidad	Conformidad %	Meta
4.1.Conocimiento de la organización y de su conte	0	0	100%
4.2. Comprensión de las necesidades y expectativa	0	0	100%
4.3. Determinación del alcance del SGSI	0	0	100%
5.2. Política	0	0	100%
6.1. Acciones para tratar riesgos y oportunidades	0	0	100%
6.2. Objetivos de seguridad de la información y pla	0	0	100%
7.1. Recursos: se debe determinar y proporcionar	0	0	100%
7.2. Competencia	0	0	100%
7.3. Toma de conciencia	0	0	100%
7.4. Comunicación	0	0	100%
7.5. Información documentada	0	0,00	100%
8.1. Planificación y control operacional	0	0	100%
8.2. Evaluacion de riesgos según los criterios estab	0	0	100%
8.3. Tratamiento de riesgos de la seguridad de la in	0	0	100%

D	MD	DEF	REP	RD	PNP	Porcentaje de cada nivel de madurez en cada cláusula
%	%	%	%	%	%	
0	0	100	0	0	0	**4.1.Conocimiento de la organización y**
0	0	0	0	0	1	**4.2. Comprensión de las necesidades y**
0	0	0	0	100	0	**4.3. Determinación del alcance del SGS**
0	0,00	0,00	0,00	100,00	0	**5.2. Política**
0	27,27	0,00	0,00	63,64	9,09	**6.1. Acciones para tratar riesgos y opor**
0	0	0	0	100	0	**6.2. Objetivos de seguridad de la inforr**
0	0	0	0	1	0	**7.1. Recursos: se debe determinar y pr**
0	0	100	0	0	0	**7.2. Competencia**
0	0	0,00	0	0	100,00	**7.3. Toma de conciencia**
0	0	0	0	1	0	**7.4. Comunicación**
0,00	0,00	0,00	54,55	0,4545	0	**7.5. Información documentada**
0	0	0	0	1	0	**8.1. Planificación y control operacional**
0	0	0	0	1	0	**8.2. Evaluacion de riesgos según los cri**
0	0	0	0	1	0	**8.3. Tratamiento de riesgos de la segur**

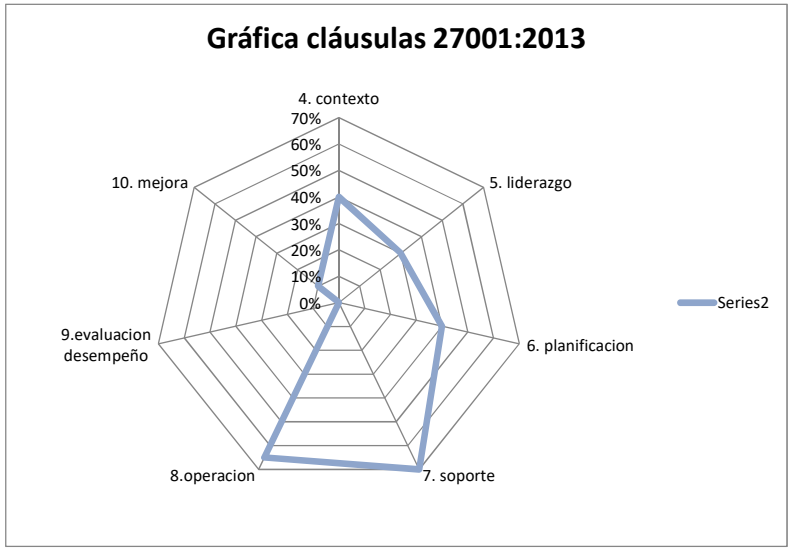
Estado adecuación controles ANEXO A (Valores en D)

Descripción del dominio	Cantidad	%Conformidad	Meta
A.5.políticas de seguridad de la información	0	0	100%
A.6.organización de la seguridad de la información	0	0	100%
A.7. seguridad en los recursos humanos	1	16,66666667	100%
A.8. gestión de activos	0	0	100%
A.9. Control de accesos	0	0	100%
A.10. Criptografía	0	0	100%
A.11. Seguridad física y ambiental	0	0	100%
A.12. Seguridad en las operaciones	0	0	100%
A.13. Seguridad en las comunicaciones	0	0	100%
A.14. Adquisición, desarrollo y mantenimiento de sistemas	0	0	100%
A.15. Relaciones con proveedores	0	0	100%
A.16. Gestión de incidentes de seguridad de la información	0	0	100%
A.17.Aspectos de seguridad de la información dentro de la continuidad del negocio	0	0	100%
A.18. Conformidad	0	0	100%

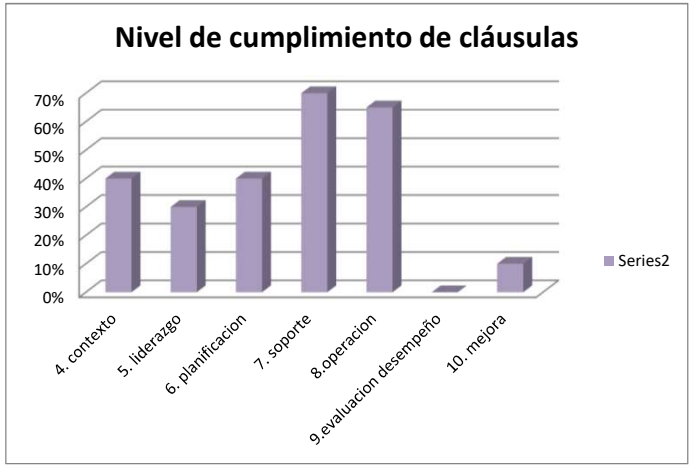
Estado actual requisitos

4. contexto	40%
5. liderazgo	30%
6. planificacion	40%
7. soporte	70%
8.operacion	65%
9.evaluacion des	0%
10. mejora	10%

implementacion procesos cumplen con la norma iso 27001:2013 y están documentados



Apéndice A: Estado actual por dominio



GRÁFICA RADIAL CONTROLES ANEXO A 27002:2013

GRÁFICO DE BARRAS PORCENTAJE CUMPLIMIENTO DOMINIOS ANEXO A