Validación de Cumplimiento TI bajo la Norma NTC-ISO/IEC 27001:2013

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
A.5..	**A.5..**	**Política de Seguridad de la Información**		2	0	1	0	1	25%	25%	
A.5.1.	A.5.1.	Gestión de la Dirección para la Seguridad de la Información		2	0	1	0	1	25%		
A.5.1.1	A.5.1.1	Políticas de Seguridad de la Información	¿Están documentadas las políticas de seguridad de la información de la organización?	pa				✔			Se observa que el Macroproceso de GIT, tiene un documento que define como Politicas de Seguridad, pero no se observa si este ha sido aprobadas al interior de la Universidad, se observa en el SGC el listado de POLÍTICAS DE LA UNIVERSIDAD DEL QUINDÍO, para verificar la existencia.
A.5.1.2	A.5.1.2	Revisión de las políticas de seguridad de la Información	¿Se realiza revisión periódica de las políticas de seguridad de la información de la organización?	no		✔					No se observa el cumplimiento de este Control.
A.6..	**A.6..**	**Organización de la Seguridad de la Información**		7	2	1	0	4	57%	48%	
A.6.1.	**A.6.1.**	**Organización Interna**		5	2	0	0	3	70%		
A.6.1.1	A.6.1.1	Roles y responsabilidades en Seguridad de la Información	¿Se tiene definido los roles, responsabilidad y autoridad a cumplir en el SGSI? Por ejemplo en Perfiles de cargos o manuales de funciones?	pa				✔			Se observa en el manual de funciones la responsabilidad asignada desde seguridad, no se observa si esta orientada a dar cumplimiento al SGSI o MSPI.
A.6.1.2	A.6.1.2	Separación de deberes	¿Existen controles de Segregación de Funciones?	PA				✔			Se observa que en el manual de funciones esta definido el tema. Seguridad, no se observa si se hace seguimiento, verificacion ,o se comunica las responsabilidades en materia de seguirdad de la informacion.
A.6.1.3	A.6.1.3	Contacto con las autoridades	¿Se cuenta con directorio de contacto con todas las autoridades o organismos de reglamentación (empresas de servicios públicos, emergencia, bomberos, prov. Telecomunicación, autoridades judiciales..etc....) del SI?	PA				✔			Se observa que se tiene para seguridad de vigilancia privada. No se observa para temas del Sistema de Seguridad de la información este directorio.
A.6.1.4	A.6.1.4	Contacto con grupos de interés especial	¿Se cuenta con afiliación, membresía o suscripción con asociaciones y o profesionales especializados en seguridad?	SI	✔						Area de TELEMATICa tiene diplomado en 27001:2005. Sonic WALL, poseen suscipcion activa.
A.6.1.5	A.6.1.5	Seguridad de la información en proyectos	¿Se ha incluido en la metodología de gestión de proyectos de la institución la SI?	SI	✔						No se observo en el momento del diagnostico. En el diagnostico, se informa que el proyecto de implementación de ECOTIC tiene reuniones en la fase de implementacion y se tiene evidencia por numeros de caso.
A.6.2.	**A.6.2.**	**Dispositivos móviles y teletrabajo**		2	0	1	0	1	25%		
A.6.2.1	A.6.2.1	Política de Dispositivo Móvil	¿Se cuenta con las políticas documentada y aprobada?	no		✔					En el diagnostico se observa una politica de seguridad, no se observa si esta definido en marco de esta, una politica para el uso de dispositivos moviles. Se observa que se usan los moviles de los funcionarios para revisiones de documentos y sistemas de monitoreo.
A.6.2.2	A.6.2.2	Teletrabajo	¿Se cuenta con políticas documentadas y medidas de seguridad para proteger l información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza l trabajo?	PA				✔			No se observa si se tienen listados. No se observa si se documenta. Va un funcionario de conectivad. Se puede ver quienes acceden. Se establecen enlaces VPN. Se registra en sonic WALL. En la Resolución de Rectoría número 1693 del 19 de abril del año 2016. Cartilla de Teletrabajo, se define las caracteristicas, pero no se direcciona a GIT para temas de seguridad de la informacion.
A.7..	**A.7..**	**Seguridad en los Recursos Humanos**		6	1	1	0	4	50%	53%	
A.7.1.	**A.7.1.**	**Antes de asumir el empleo**		2	1	0	0	1	75%		
A.7.1.1	A.7.1.1	Selección	¿Se cuenta con la verificación de antecedentes de los candidatos?	si	✔						Se observa que en el macroproceso de gestion humana, se tiene establecido, documentado en el SGC.
A.7.1.2	**A.7.1.2**	Términos y condiciones de empleo	¿Acuerdos contractuales incluyen políticas de seguridad de la información, acuerdos de confidencialidad, derechos de autor, entre otros y las sanciones a tomar en caso de incumplimiento?	pa				✔			Se observa que existe una resolucion de la Rectoria en cuanto a temas de Etica y Buen Gobierno, se pide firmar un acuerdo de confidencialidad. No observa que se hable sobre Politicas de Seguridad y que acciones se deben tomar en caso de una vulnerabilidad.
A.7.2.	**A.7.2.**	**Durante la ejecución del empleo**			0	1	0	2	33%		

Validación de Cumplimiento TI bajo la Norma NTC-ISO/IEC 27001:2013

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
A.7.2.1	A.7.2.1	Responsabilidades de la dirección	¿Se evidencia la difusión de los roles y responsabilidades en cuanto a la SI hacia el personal y registros que demuestre la difusión realizada por la dirección? ¿Difundir las políticas de SI en la inducción o entrega del cargo?	no		✔					Se observa que en la resolucion 1350 de 2015. POR MEDIO DE LA CUAL SE AJUSTA EL MANUAL DE FUNCIONES Y DE COMPETENCIAS LABORALES PARA LOS CARGOS DE LOS NIVELES DIRECT! VO, ASESOR YPROFESIONAL ESTABLECIDOS EN LA PLANTA DE PERSONAL ADMINISTRA TI VA DE LA UNIVERSIDAD DEL QUINDIO. Profesional Especializado COdigo 2028 Grado 18. GestiOn TICS. se tiene establecido las responsabilidades de seguridad de la informacion. Se tiene claro en el proceso de gestion documental. pero desde la ley general de archivo.
A.7.2.2	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	¿Se evidencia la realización actividades de capacitación y sensibilización sobre SI? Proveedores, contratista, y funcionarios	pa				✔			Según lo diagnosticado en los macroprocesos, esta no se exige a proveedores. Y la concientizacion esta dada para el proceso de gestion documental.
A.7.2.3	A.7.2.3	Proceso disciplinario	¿Se cuenta con un proceso disciplinario formal y comunicado SI?	pa				✔			se observa que se tiene proceso control disciplinario interno.
A.7.3.	**A.7.3.**	**Terminación y cambio de empleo**		1	0	0	0	1	50%		
A.7.3.1	A.7.3.1	Terminación o cambio de responsabilidades de empleo	¿Se cuenta con un proceso que comunique las responsabilidades en cuanto SI del empleado o contratista que se retira o cambia de puesto? ¿Se cuenta con un proceso que comunique sobre el retiro o cambio de personal o contratista, a los procesos correspondientes para el retiro de derechos de acceso? ¿Existen políticas para la devolución de los activos al terminar el empleo o contrato?	pa				✔			se observa que se tiene devolucion de activos fijos. No seobserva si se cuenta con un proceso para comunicar responsabilidades desde el SGSI en retiro o cambio de puesto.
A.8..	**A.8..**	**Gestión de los activos**		10	3	6	0	1	35%	29%	
A.8.1.	**A.8.1.**	**Responsabilidad por los activos**		4	3	0	0	1	88%		
A.8.1.1	A.8.1.1	Inventario de Activos	¿Se cuenta con un listado documentado de activos de información donde se identifiquen los responsables?	si	✔						Se informa en el diagnostico que existe un inventario de activos fisicos y de Software. Se observa listado de documentos e información.
A.8.1.2	A.8.1.2	Propiedad de los activos		si	✔						
A.8.1.3	A.8.1.3	Uso aceptable de los activos	¿Existen políticas asociados con el uso aceptable de los recursos de procesamiento de información? incluye contratista?	si	✔						se observa que en el manual de funciones, el código de etica y buen gobierno, el Programa de Gestión Documental se deja claro el aspecto relacionado con recursos de procesamiento de la informacion.
A.8.1.4	A.8.1.4	Devolución de activos	¿Existen políticas asociadas a la devolución de los activos al terminar el empleo o contrato?	pa				✔			Se observa que este esta contemplado desde el PGD y de la devolucion de activos fisicos.
A.8.2.	**A.8.2.**	**Clasificación de la Información**		3	0	3	0	0	0%		
A.8.2.1	A.8.2.1	Clasificación de la información	¿se tiene un procedimiento para la clasificación de los Activos Información?	no		✔					Se observa que esta desde la perspectiva de la tabla de retencion documental. No se observa desde los criterios de confidencialidad, integridad y disponibiliad.
A.8.2.2	A.8.2.2	Etiquetado y manejo de la información	¿Existe un procedimiento para el etiquetado de la información según la clasificación definida?	no		✔					
A.8.2.3	A.8.2.3	Manejo de activos	¿Existe un procedimiento para el manejo para el procesamiento, almacenamiento, comunicación de información de acuerdo a su clasificación?	no		✔					
A.8.3.	**A.8.3.**	**Manejo de los Medios**		3	0	3	0	0	0%		
A.8.3.1	A.8.3.1	Gestión de los medios removibles	¿Existe políticas o procedimientos para medios removibles? ¿Existen políticas o procedimientos para la gestión de medios removibles (discos duros externos, memorias USB, cds, dvds, cintas de respaldo, entre otros)?	no		✔					no se observa si se cuenta con esta politica. En el borrador de politica no se especifica.
A.8.3.2	A.8.3.2	Disposición de los medios	¿Existe políticas o procedimientos para disponer de forma segura los medios físicos cuando no son requeridos?	no		✔					no se observa si se cuenta con esta politica. En el borrador de politica no se especifica.

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	M	Controles		RE	SI	NO	NA	PA	Cumplimiento Control	Objetivos	Justificación
A.8.3.3	A.8.3.3	Transferencia de los medios físicos	¿Existe políticas o procedimientos de seguridad para la protección de medios físicos durante el transporte (servicio de mensajería, embalaje ?	no		✔					no se observa si se cuenta con esta politica. En el borrador de politica no se especifica.
A.9..	**A.9..**	**Control de Acceso**		14	0	1	0	13	**46%**	38%	
A.9.1.	**A.9.1.**	**Requisitos del Negocio para el Control de Acceso**		2	0	0	0	2	**50%**		
A.9.1.1	A.9.1.1	Política de control del acceso	¿Se han definido políticas para control de acceso físico y lógico?	pa				✔			Se observa que esta definido, pero en el diagnostico se no se observa si se aplican los controles. Se esta trabajando un proyecto para mejorar este aspecto. Falta Documentar.
A.9.1.2	A.9.1.2	Acceso a redes y a servicios en red		pa				✔			
A.9.2.	**A.9.2.**	**Gestión de Acceso de Usuarios**		6	0	0	0	6	**50%**		
A.9.2.1	A.9.2.1	Registro de usuarios y cancelación del registro de usuarios	¿Existen políticas o procedimientos de gestión de acceso de usuarios a los sistemas, servicios, redes y código fuente de la organización?	pa				✔			se informa que se realiza procedimiento y se genera paz y salvo.
A.9.2.2	A.9.2.2	Suministro de acceso de usuarios		pa				✔			
A.9.2.3	A.9.2.3	Gestión de derechos de acceso privilegiado		pa				✔			
A.9.2.4	A.9.2.4	Gestión de información de autenticación secreta de usuarios		pa				✔			No se observa si se tiene definido una matriz de roles y privilegios que pueda sustentar de forma adecuada la gestion de derechos de acceso.
A.9.2.5	A.9.2.5	Revisión de los derechos de acceso de usuarios		pa				✔			
A.9.2.6	A.9.2.6	Retiro o ajuste de los derechos de acceso		pa				✔			Se informa que se realiza. no se observa si estaprocedientado.
A.9.3.	**A.9.3.**	**Responsabilidades de los usuarios**		1	0	1	0	0	0%		
A.9.3.1	A.9.3.1	Uso de información de autenticación secreta	¿Existen políticas o procedimientos de gestión de acceso de usuarios a los sistemas, servicios, redes y código fuente de la organización?	no		✔					Se informa que dependen de la buena fe de los funcionarios. Por eso la clasificacion.
A.9.4.	**A.9.4.**	**Control de acceso a sistemas y aplicaciones**		5	0	0	0	5	**50%**		
A.9.4.1	A.9.4.1	Restricción de acceso a la información	¿Existen políticas o procedimientos de gestión de acceso de usuarios a los sistemas, servicios, redes y código fuente de la organización?	pa				✔			
A.9.4.2	A.9.4.2	Procedimiento de ingreso seguro		pa				✔			
A.9.4.3	A.9.4.3	Sistema de gestión de contraseñas		pa				✔			se inorma que se empezo implementacion con proyecto ECOTIC
A.9.4.4	A.9.4.4	Uso de programas utilitarios privilegiados		pa				✔			se informa que esta en cabeza de un funcionario y que Falta documentar.
A.9.4.5	A.9.4.5	Control de acceso a códigos fuente de programas		pa				✔			
A.10..	**A.10..**	**Criptografía**		2	0	0	0	2	**50%**	**50%**	
A.10.1.	**A.10.1.**	**Controles Criptográficos**		2	0	0	0	2	**50%**		
A.10.1.1	A.10.1.1	Política sobre uso de controles criptográficos		pa				✔			se informa que se realizapero no se documenta el proceso. Se le hace seguimiento.
A.10.1.2	A.10.1.2	Gestión de llaves		pa				✔			
A.11..	**A.11..**	**Seguridad Física y del Entorno**		15	0	7	1	7	30%	32%	
A.11.1.	**A.11.1.**	**Áreas Seguras**		6	0	2	1	3	**42%**		
A.11.1.1	A.11.1.1	Perímetro de seguridad física		pa				✔			se informa que se presento robo de equipos . Proyecto de seguridad fisica.
A.11.1.2	A.11.1.2	Controles de acceso físicos		no		✔					
A.11.1.3	A.11.1.3	Seguridad de oficinas, recintos e instalaciones		pa				✔			
A.11.1.4	A.11.1.4	Protección contra amenazas externas y ambientales		pa				✔			Se informa que existen sistemas de proteccion para el DATACENTER, como pararrayos. Sobretensiones, inundacion, no incendio.
A.11.1.5	A.11.1.5	Trabajo en áreas seguras		no		✔					No se observa si se tiene establecido trabajo en areas seguras.
A.11.1.6	A.11.1.6	Áreas de despacho y carga		na			✔				
A.11.2.	**A.11.2.**	**Equipos**		9	0	5	0	4	22%		

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
A.11.2.1	A.11.2.1	Ubicación y protección de los equipos	¿Políticas de ubicación y protección de equipos?	no		✔					No se observa si se tiene politicas de ubicación y proteccion de equipos. No se informa a contratistas.
A.11.2.2	A.11.2.2	Servicios de suministro	¿Políticas o procedimiento de Protección para evitar interrupción causado por fallas eléctricas?	pa				✔			se informa que esta definido solo datacenter y area de sistemas. Todos UPS autonomia 15 min.
A.11.2.3	A.11.2.3	Seguridad del cableado	¿Políticas o procedimiento para evitar interrupción causado por fallas eléctricas?	pa				✔			
A.11.2.4	A.11.2.4	Mantenimiento de equipos	Plan de mantenimiento preventivo de equipos?	pa				✔			Se informa que el mantenimiento es de tipo correctivo y se tiene para salas de internet. No se informa si esta documentado.
A.11.2.5	A.11.2.5	Retiro de activos	Política de retiros de activos de forma segura de los activos?	no		✔					No se observa si se tiene el procedimiento.
A.11.2.6	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Políticas de seguridad de los equipos fuera de la instalaciones	no		✔					No se observa si se tiene el procedimiento.
A.11.2.7	A.11.2.7	Disposición segura o reutilización de equipos	Política de disposición segura o reutilización de equipos	pa				✔			se informa que se realiza, pero que aun no esta procedimentado.
A.11.2.8	A.11.2.8	Equipos de usuarios desatendido	Políticas de equipos desatendido	no		✔					Se informa que se tiene Directorio Activo, No se observa si se tiene una politica.
A.11.2.9	A.11.2.9	Política de escritorio limpio y pantalla limpia	Política de escritorio limpio y pantalla limpia	no		✔					No se observa si se tiene politica como tal de escritorio limpio. Solo se tiene protocolo de atencion al usuario, pero no se le realiza seguimiento.
A.12..	**A.12..**	**Seguridad de las Operaciones**		14	3	3	0	8	**50%**	**63%**	
A.12.1.	**A.12.1.**	**Procedimientos Operacionales y Responsabilidades**		4	0	3	0	1	13%		
A.12.1.1	A.12.1.1	Procedimientos de operación documentados	Procedimientos documentados	no		✔					No se observa si se tienen documentados los procedimientos según el diagnostico realizado.
A.12.1.2	A.12.1.2	Gestión de cambios	Procedimiento de gestión de cambios	no		✔					no se informa que se realizaseguimiento a la gestion de cambios.
A.12.1.3	A.12.1.3	Gestión de capacidad	procedimiento de gestión de la capacidad	pa				✔			se informa y observa que monitorea. Pero no se informa si esta procedimentado o escrito
A.12.1.4	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Procedimiento o metodología de desarrollo de software y pruebas de software	no		✔					no se observa si se cuenta con un procedimiento para separar los ambientes de produccion y pruebas.
A.12.2.	**A.12.2.**	**Protección contra códigos maliciosos**		1	0	0	0	1	**50%**		
A.12.2.1	A.12.2.1	Controles contra códigos maliciosos	Procedimiento y políticas contra códigos maliciosos	pa				✔			Se informa que se realiza con herramienta sonic wall/ WAF fisico y virtual. No se informa si esta documentado.
A.12.3.	**A.12.3.**	**Copias de respaldo**		1	0	0	0	1	**50%**		
A.12.3.1	A.12.3.1	Respaldo de la información	Procedimientos de copias de respaldo	pa				✔			se informa que se tiene un procedimiento de copias de respaldo. Se ejecutan a nivel de datacenter. Y algunos procesos lo realizan de forma manual.
A.12.4.	**A.12.4.**	**Requisitos y seguimiento**		4	0	0	0	4	**50%**		
A.12.4.1	A.12.4.1	Registro de eventos	Procedimiento de fallas y eventos de SI (monitoreo de log)	pa				✔			se informa que existe el procedimiento de fallas y eventos, no se observa si estadocumentador
A.12.4.2	A.12.4.2	Protección de la información del registro	Procedimiento que indique como se protege la información	pa				✔			
A.12.4.3	A.12.4.3	Registros de administrador y de operador	Políticas o procedimientos para registrar administración y el registro del sistema	pa				✔			no se infora si esta documentado.
A.12.4.4	A.12.4.4	Sincronización de relojes	Definir el procedimiento para la sincronización de relojes	pa				✔			se informa que esta el procedimiento aplicado, no documentado.
A.12.5.	**A.12.5.**	**Control de software operacional**		1	1	0	0	0	100%		
A.12.5.1	A.12.5.1	Instalación de software en sistemas operativos	Procedimiento para controlar la instalación de software en el sistema operativo	si	✔						se informa que esta documentado, pero no se informa controles.
A.12.6.	**A.12.6.**	**Gestión de la Vulnerabilidad Técnica**		2	1	0	0	1	75%		
A.12.6.1	A.12.6.1	Control de las vulnerabilidades técnicas	Procedimiento o políticas para análisis de vulnerabilidades técnicas, evidencia que se este haciendo	pa				✔			SoniC Wall. se informa que se realizaprocedimiento. No esta documentado.
A.12.6.2	A.12.6.2	Restricciones sobre la instalación de software	Política de instalación de software por parte de usuarios	si	✔						Se informa que si existe la politica. Se observaron equipos con usuario ADMIN.
A.12.7.	**A.12.7.**	**Consideraciones de la Auditoría de los sistemas de Información**		1	1	0	0	0	100%		
A.12.7.1	A.12.7.1	Controles de auditorias de sistemas de información	Procedimiento para planes de auditoria del SI	si	✔						Se informa que se les realiza el procedimiento desde el area de CI, el area de GIT ha realizado auditorias.
A.13..	**A.13..**	**Seguridad de las Comunicaciones**		**7**	**3**	**2**	**0**	**2**	**57%**	**63%**	
A.13.1.	**A.13.1.**	**Gestión de la Seguridad de las Redes**		3	**3**	**0**	**0**	**0**	100%		
A.13.1.1	A.13.1.1	Controles de las redes	¿Se cuentan con controles de red que garanticen la seguridad de los servicios y de la información (Firewall, proxys)? ¿se informa que se realizasegmentación de redes mediante	si	✔						se informa que se tienen y se documentan
A.13.1.2	A.13.1.2	Seguridad de los servicios de red		si	✔						

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
A.13.1.3	A.13.1.3	Separación en las redes	Vlans? Se manejan Registros?	si	✔						
A.13.2.	**A.13.2.**	**Transferencia de Información**		**4**	**0**	**2**	**0**	**2**	25%		
A.13.2.1	A.13.2.1	Política y procedimientos de transferencia de información	Políticas para la gestionar y controlar las redes y transferencia de información	pa				✔			No se observa si se tiene documentado. No existe la politica, se hace por iniciativa del funcionario de GIT
A.13.2.2	A.13.2.2	Acuerdos sobre transferencia de información	Políticas/procedimientos para la transferencia de información según la clasificación establecida (confidencial, privada, publica) y los acuerdos sobre el tratamiento de la información en la transferencia.	no		✔					No se observa si se tiene.
A.13.2.3	A.13.2.3	Mensajería electrónica		no		✔					No se observa si se tiene.
A.13.2.4	A.13.2.4	Acuerdos de confidencialidad o de no divulgación	¿Se tiene definidos los acuerdo de confidencialidad?	pa				✔			se informa que se tiene definido un codigo de etica y buen gobierno RES 1366 de 2016. se informa que se tiene n acuerdos para areas de psicologia, centro de salud, CIBM, Gestion Documental. Y se informa que se tiene en cada hoja de vida el acuerdo de confidencialidad. En el diagnostico presencial no se evidencia en el proceso de talento humano.
A.14..	**A.14..**	**Adquisición, Desarrollo y Mantenimiento de Sistemas**		13	9	3	0	1	73%	**52%**	
A.14.1.	**A.14.1.**	**Requisitos de seguridad de los Sistemas de Información**		3	**2**	**0**	**0**	**1**	83%		
A.14.1.1	A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información	Procedimiento de desarrollo de software, desde el análisis y las especificaciones	si	✔						se informa que se realizael procedimiento. Se establecen las especificaciones.
A.14.1.2	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Políticas o instrucciones de protección	pa				✔			existe pero no dcumenta. PSE
A.14.1.3	A.14.1.3	Protección de transacciones de los Servicios de las aplicaciones	Políticas de transacción	si	✔						
A.14.2.	**A.14.2.**	**Seguridad en los Proceso de Desarrollo y Soporte**		9	**7**	**2**	**0**	**0**	78%		
A.14.2.1	A.14.2.1	Política de desarrollo seguro	Establecer políticas de desarrollo seguro	si	✔						
A.14.2.2	A.14.2.2	Procedimiento de control de cambios en sistemas	Procedimientos de control de cambios en desarrollo de software, que tengan políticas de desarrollo seguro	si	✔						se informa que se tiene n establecidos procedimientos de desarrollo seguro. Proyecto ECOTIC.
A.14.2.3	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		si	✔						
A.14.2.4	A.14.2.4	Restricciones en los cambios a los paquetes de software		si	✔						
A.14.2.5	A.14.2.5	Principios de construcción de los sistemas seguros		si	✔						
A.14.2.6	A.14.2.6	Ambiente de desarrollo seguro		si	✔						
A.14.2.7	A.14.2.7	Desarrollo contratado externamente	Definir procedimiento de contratación para desarrollo de software contratado externamente,(definir dueños y propiedad intelectual)	si	✔						
A.14.2.8	A.14.2.8	Pruebas de seguridad de sistemas	Procedimiento de pruebas	no		✔					Aunque se informa que se tiene n definidos procedimientos de desarrollo seguro, No se observa si se informa que se tiene pruebas de seguridad y aceptacion de sistemas. Se da en la marcha.
A.14.2.9	A.14.2.9	Prueba de aceptación de sistemas		no		✔					
A.14.3.	**A.14.3.**	**Datos de Prueba**		1	**0**	**1**	**0**	**0**	0%		
A.14.3.1	A.14.3.1	Protección de Datos de Prueba	Procedimiento de pruebas. Seguridad de datos.	no		✔					No se informa que se realizael procedimiento.
A.15..	**A.15..**	**Relaciones con los Proveedores**		5	0	0	0	5	**50%**	**50%**	
A.15.1.	**A.15.1.**	**Seguridad de la información en las relaciones con los proveedores**		3	**0**	**0**	**0**	**3**	**50%**		
A.15.1.1	A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Definir política de la relación con los proveedores	pa				✔			se informa que se tiene la poltiica pero no se documenta las relaciones para todos los proveedores.
A.15.1.2	A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Acuerdos de nivel de servicio, puntos de seguridad en la contratación	pa				✔			se informa que se tiene n establecidos a nivel contractual. se informa que se realizaseguimiento a traves de Firewall.
A.15.1.3	A.15.1.3	Cadena de suministro de tecnología de información y comunicación		pa				✔			
A.15.2.	**A.15.2.**	**Gestión de la prestación de servicios de Proveedores**		2	**0**	**0**	**0**	**2**	**50%**		
A.15.2.1	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	¿se informa que se realizaseguimiento y revisión de los servicios con los proveedores?	pa				✔			se realizan seguimiento por parte de los interventores del contrato, pero en el diagnostico no se evidencio documentacion.
A.15.2.2	A.15.2.2	Gestión de cambios en los servicios de los proveedores	¿se informa que se tiene establecido gestión de cambios en los servicios de los proveedores?	pa				✔			se informa que se realizaverificacion de cambios a nivel contractual. No se documenta. No existe procedimiento de gestion de cambios.

Validación de Cumplimiento TI bajo la Norma NTC-ISO/IEC 27001:2013

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
A.16..	**A.16..**	**Gestión de incidentes de Seguridad de la Información**		7	0	2	0	5	36%	36%	
A.16.1.	**A.16.1.**	Gestión de Incidentes y Mejoras en la seguridad de la Información		7	**0**	**2**	**0**	**5**	36%		
A.16.1.1	A.16.1.1	Responsabilidades y procedimientos	Procedimiento de gestión de incidentes	pa				✔			se informa que se tiene responsabilidades. Faltan procedimientos
A.16.1.2	A.16.1.2	Reporte de eventos de seguridad de la información		pa				✔			no se establecen los protocolos en caso de la segurida de la información. Solo de activos fijos. Se hace seguimiento a traves del firewall de los eventos externos. Falta eventos internos.
A.16.1.3	A.16.1.3	Reporte de debilidades de seguridad de la información		pa				✔			
A.16.1.4	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		pa				✔			se informa que se tiene procedimiento de gestion de incidentes. No se observa si se hace seguimiento o evaluacion.
A.16.1.5	A.16.1.5	Respuesta a incidentes de seguridad de la información		pa				✔			se informa que se tiene procedimiento de gestion de incidentes. No se observa si se hace seguimiento o evaluacion.
A.16.1.6	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		no		✔					se informa que se tiene procedimiento de gestion de incidentes. No se observa si se hace seguimiento o evaluacion.
A.16.1.7	A.16.1.7	Recolección de evidencia		no		✔					se informa que se tiene procedimiento de gestion de incidentes. No se observa si se hace seguimiento o evaluacion.
A.17..	**A.17..**	**Aspectos de seguridad de la información de la Gestión de Continuidad de Negocio**		4	0	2	0	2	25%	33%	
A.17.1.	**A.17.1.**	**Continuidad de seguridad de la información**		3	**0**	**2**	**0**	**1**	17%		
A.17.1.1	A.17.1.1	Planificación de la continuidad de las seguridad de la información	La continuación de la Seguridad de la Información se ha incluido dentro del PCN o el PRD?	pa				✔			se informa que se tiene una PCN planificado, no se observa si estaimplementado, no se le hace verificacion, revision o evaluacion del mismo en el aspecto de la seguridad de la informacion. Estan los controles por diseñarse en actividad siguiente.
A.17.1.2	A.17.1.2	Implementación de la continuidad de la seguridad de la información		no		✔					
A.17.1.3	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Procedimiento del plan de continuidad del negocio	no		✔					
A.17.2.	**A.17.2.**	**Redundancias**		1	**0**	**0**	**0**	**1**	50%		
A.17.2.1	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Procedimiento del plan de continuidad del negocio	pa				✔			redundancia UPS internet. Core Procesamiento.
A.18..	**A.18..**	**Cumplimiento**		8	2	2	0	4	50%	43%	
A.18.1.	**A.18.1.**	**Cumplimiento de los requisitos legales y contractuales**		5	**2**	**0**	**0**	**3**	70%		
A.18.1.1	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Nomograma	pa				✔			aunque se oberva que se tienen definidos los normogramas, en el diagnostico, no se observo legislacion aplicable en materia de Seguridad y Privacidad.
A.18.1.2	A.18.1.2	Derechos de propiedad intelectual (DPI)	Políticas de propiedad intelectual	si	✔						Se observa que se tiene codigo de etica y buen gobierno. No se observa si se aplican los controles
A.18.1.3	A.18.1.3	Protección de registros	Procedimiento de control de registro, Backus, gestión de activos…	pa				✔			Se observa que se hacen copias de seguridad, no se observa al momento del diagnostico que la información producida en cada equipo fuera de las instalaciones del Perimetro de seguridad guarde informacion centralizada.
A.18.1.4	A.18.1.4	Privacidad y protección de información de datos personales	Ley de Habeas Data	pa				✔			Se observa conocimiento del tema en materia legal (ley 1581), no se observa si se realiza el control.
A.18.1.5	A.18.1.5	Reglamentación de los controles criptográficos	Cumplir con los requisitos	si	✔						Se observa aplicación de controles criptograficos.
A.18.2.	**A.18.2.**	**Revisiones de seguridad de la información**		3	**0**	**2**	**0**	**1**	17%		
A.18.2.1	A.18.2.1	Revisión independiente de la seguridad de la información	Auditoria externa o internas	no		✔					no se observa si se han realizado revisiones independientes al SGSI. Se observa que han contratado test de penetracion.
A.18.2.2	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Auditorias (Revisión del cumplimento de las políticas)	no		✔					Se observa un cmplimiento con las auditorias en marco del Sistema de Gestion de Calidad, MECI y NTGCP1000. no se observan auditorias con las recomendaciones de un sistema de sguridad y privacidad de la información.
A.18.2.3	A.18.2.3	Revisión del cumplimiento técnico	Análisis de vulnerabilidades	pa				✔			Se observa que se realizan analisis de vulnerabilidades, el personal esta inscrito en boletines de seguridad, no se observa documenación o registros en marco del SGSI.
			TOTAL	**114**	**23**	**31**	**1**	**59**	**47%**	**44%**	

Validación de Cumplimiento TI bajo la Norma NTC-ISO/IEC 27001:2013

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	M	Controles		RE	SI	NO	NA	PA	Cumplimiento Control	Objetivos	Justificación
Ítem	Ítem	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Cumplimiento Control	Objetivos	Justificación
4..	**4..**	**Contexto de la Organización**		7	1	5	0	1	21%	31%	
4.1.	**4.1.**	**Conocimiento de la Organización y su contexto**		1	1	0	0	0	100%		
4.1.	4.1.	Conocimiento de la Organización y su contexto	¿Se tiene establecido el contexto interno y externo de la organización?	si	✔						Si.la Universidad Esta certificada ISO 9001. tiene un PLAN DE SEGURIDAD DE LA INFORMACIÓN.
4.2.	**4.2.**	**Comprensión de las necesidades y expectativas de las partes interesadas**		2	0	1	0	1	25%		
		La organización debe determinar:			-	-	-	-			
4.2.a	4.2.a	Las partes interesadas que son pertinentes al SGSI	¿Esta definida las partes interesadas?	pa				✔			Se observa que se tienen definidos temas de seguridad, no se observa si estan definidas las partes interesadas desde el SGSI, se observan en SGC.
4.2.b	4.2.b	Los requisitos de estas partes interesadas pertinentes a SI	¿Se tiene los requisitos de estas partes interesadas?	no		✔					
4.3.	**4.3.**	**Determinación del alcance del SGSI**		3	0	3	0	0	0%		
		Cuando se determina este alcance, la organización debe considerar:			-	-	-	-			
4.3.a	4.3.a	Las cuestiones externas e internas referidas en el numera 4.1	¿se ha definido el alcance del SGSI? ¿Se tienen en cuenta factores internos y externos?¿Da cumplimiento a lo requerido por las partes interesadas?	no		✔					no se informa si se ha definido un SGSI, propiamente dicho.
4.3.b	4.3.b	Los requisitos referidos en el numera 4,2		no		✔					
4.3.c	4.3.c	Las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones.		no		✔					
4.4.	**4.4.**	**Sistema de Gestión de la seguridad de la información**		1	0	1	0	0	0%		
4.4.	4.4.	Sistema de Gestión de la seguridad de la información	¿Se cuenta con un cronograma del proyecto y se realiza un seguimiento periódico para su ejecución?	no		✔					no se informa si se ha definido un SGSI, propiamente dicho.
5..	**5..**	**Liderazgo**		17	0	16	0	1	3%	2%	
5.1.	**5.1.**	**Liderazgo y Compromiso**		8	0	7	0	1	6%		
		La dirección debe demostrar liderazgo y compromiso con respecto al SGSI			-	-	-	-			
5.1.a	5.1.a	Asegurando establecer Política y Objetivos SI, compatibles con la dirección estratégica	¿Se cuenta con una política y objetivos de SI aprobados?	no		✔					No se observa si se tiene.
5.1.b	5.1.b	Asegurando la Integración de los requisitos del SGSI en los procesos de la organización	¿Se cuenta con una matriz de requisitos para los procesos de la compañía?	no		✔					
5.1.c	5.1.c	Asegurando los recursos necesarios para el sistema de SGSI estén disponibles	¿Se cuenta con un presupuesto aprobado para el SGSI?	no		✔					No se observa si se tiene.
5.1.d	5.1.d	Comunicando la importancia de una SGSI eficaz y conforme con los requisitos del SGSI	¿Se evidencia la difusión del SGSI hacia los procesos?	no		✔					
5.1.e	5.1.e	Asegurando que el SGSI logre los objetivos previstos	¿Se evidencia el seguimiento realizado a la implementación y a la eficacia del SGSI por parte de la dirección?	no		✔					Se observan actividades marco de liderazgo y compromiso, falta alienarlos hacia un SGSI.
5.1.f	5.1.f	Dirigiendo y apoyando a las personas, para contribuir a la eficacia del SGSI		no		✔					
5.1.g	5.1.g	Promoviendo la mejora continua		pa				✔			
5.1.h	5.1.h	Apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad		no		✔					
5.2.	**5.2.**	**Política**		7	0	7	0	0	0%		
		La alta dirección debe establecer una política de la SI que:									
5.2.a	5.2.a	Sea adecuada al propósito de la organización	¿ Se ha definido la política de la SI con todos los requisitos de la norma?	no		✔					Al momento del Diagnostico se observa que existen Politicas de Calidad, no se observan desde el SGSI.
5.2.b	5.2.b	Incluya objetivos de SI o proporcione el marco de referencia para el establecimiento de los objetivos de SI		no		✔					Al momento del Diagnostico se observa que existen Politicas de Calidad, no se observan desde el SGSI.
5.2.c	5.2.c	Incluya el compromiso de cumplir los requisitos aplicables relacionados con la SI		no		✔					

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
5.2.d	5.2.d	Incluya el compromiso de mejora continua del SGSI		no		✔					Al momento del Diagnostico se observa que existen Politicas de Calidad, no se observan desde el SGSI.
5.2.e	5.2.e	Estar disponible como información documentada		no		✔					Al momento del Diagnostico se observa que existen Politicas de Calidad, no se observan desde el SGSI.
5.2.f	5.2.f	Comunicarse dentro de la organización	¿Se evidencia la difusión de la Política de SI a todas las partes interesadas?	no		✔					Al momento del Diagnostico se observa que existen Politicas de Calidad, no se observan desde el SGSI.
5.2.g	5.2.g	Estar disponible para las partes interesadas	¿La Política de SI esta disponible para quien lo requiera?	no		✔					Al momento del Diagnostico se observa que existen Politicas de Calidad, no se observan desde el SGSI.
5.3.	**5.3.**	**Roles, Responsabilidades y Autoridades en la Organización**		**2**	**0**	**3**	**0**	**0**	0%		
		La alta dirección debe asignar la responsabilidad y autoridad para:									
5.3.a	5.3.a	Asegurarse que el SGSI sea conforme con los requisitos	¿Se tiene definido los roles, responsabilidad y autoridad a cumplir en el proyecto de implementación del SGSI?	no		✔					Al momento del Diagnostico se observa que existen Politicas de Calidad, no se observan desde el SGSI.
5.3.b	5.3.b	Informar a la alta dirección sobre el desempeño del SGSI	¿Se tiene definido los roles, responsabilidad y autoridad a cumplir en el mantenimiento del SGSI (Perfiles de cargos o manuales de funciones)?	no		✔					
6..	**6..**	**Planificación**		32	0	16	0	16	25%	25%	
6.1.	**6.1.**	**Acciones para tratar riesgos y oportunidades**		6	0	0	0	6	**50%**		
6.1.1	**6.1.1**	**Generalidades**			–	–	–	–			
6.1.1.a	6.1.1.a	Asegurar que SGSI pueda lograr los resultados		pa				✔			Se observa el enfoque de riesgos observado esta definido en marco del proceso de calidad, y se observa parcial para el SGSI. La declaraciones de aplicabilidad no se observan
6.1.1.b	6.1.1.b	Prevenir o reducir efectos indeseados		pa				✔			
6.1.1.c	6.1.1.c	Lograr la mejora continua		pa				✔			
		La Organización de planificar:									
6.1.1.d	6.1.1.d	Las acciones para tratar estos riesgos y oportunidades		pa				✔			
6.1.1.e.1	6.1.1.e.1	La manera de integrar e implementar estas acciones en sus procesos de SGSI		pa				✔			
6.1.1.e.2	6.1.1.e.2	La manera de evaluar la eficacia de estas acciones		pa				✔			
6.1.2	**6.1.2**	**Valoración de Riesgos de la Seguridad de la información**		10	0	0	0	10	50%		
6.1.2.a.1	6.1.2.a.1	Establecer y mantener criterios de aceptación riesgo de la Seguridad de la Información		pa				✔			
6.1.2.a.2	6.1.2.a.2	Establecer y mantener criterios par realizar valoración de riesgos se la SI		pa				✔			
6.1.2.b	6.1.2.b	Asegure que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables		pa				✔			
6.1.2.c.1	6.1.2.c.1	Identificar los riesgos de SI asociados con la perdida de Confidencialidad, Integridad y Disponibilidad de información dentro del alcance	¿Se tiene una metodología para la gestión de los riesgos?	pa				✔			
6.1.2.c.2	6.1.2.c.2	Identificar los dueños de los riesgos		pa				✔			
6.1.2.d.1	6.1.2.d.1	Valorar las consecuencias potenciales que resultan si se materializan los riesgos identificados		pa				✔			
6.1.2.d.2	6.1.2.d.2	Valorar la probabilidad realista de que ocurran los riesgos identificados		pa				✔			
6.1.2.d.3		Determinar los niveles de riesgo		pa				✔			
6.1.2.e.1	6.1.2.e.1	Comparar los resultados del análisis de riesgo con los criterios de riesgo establecidos		pa				✔			
6.1.2.e.2	6.1.2.e.2	Priorizar los riesgos analizados para el tratamiento de riesgos		pa				✔			
6.1.3	**6.1.3**	**Tratamiento del Riesgo de la Seguridad de la Información**		6	0	6	0	0	0%		

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
6.1.3.a	6.1.3.a	Seleccionar las opciones apropiadas de tratamiento de riesgo de la SI, teniendo en cuenta los resultados de la valoración del riesgo		no		✔					
6.1.3.b	6.1.3.b	Determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la SI		no		✔					
6.1.3.c	6.1.3.c	Comparar los controles determinados con el Anexo A		no		✔					
6.1.3.d	6.1.3.d	Declaración de aplicabilidad		no		✔					no se observo.
6.1.3.e	6.1.3.e	Plan de tratamiento de riesgo		no		✔					No se observo desde el SGSI
6.1.3.f	6.1.3.f	Aprobación y aceptación de los riesgos residuales de la SI		no		✔					
6.2.	**6.2.**	**Objetivos de Seguridad de la Información y Planes para Lograrlos**		10	0	10	0	0	0%		
6.2.a	6.2.a	Los objetivos de SI deben ser coherentes con la política de SI	¿Los Objetivos son coherentes con la política de SI?	no		✔					Al momento del Diagnostico no se observa.
6.2.b	6.2.b	Medibles	¿Se ha definido los objetivos de SI incluyendo la forma de medición y su periodicidad?	no		✔					
6.2.c	6.2.c	Tener en cuenta los requisitos de SI aplicables, y los resultados de valoración y tratamiento de los riesgos		no		✔					
6.2.d	6.2.d	Ser comunicados	¿Han sido comunicados y documentados?	no		✔					
6.2.e	6.2.e	Ser actualizados, según sea lo apropiado	¿Se ha definido los objetivos de SI incluyendo la planificación para lograrlos?	no		✔					Al momento del Diagnostico no se observa.
6.2.f	6.2.f	Determinar lo que se va a hace		no		✔					
6.2.g	6.2.g	Los recursos que se requiere		no		✔					
6.2.h	6.2.h	Quien será el responsable		no		✔					
6.2.i	6.2.i	Cuando se finalizará		no		✔					
6.2.j	6.2.j	Como se evaluaran los resultados		no		✔					
7..	**7..**	**Soporte**		24	0	10	0	14	29%	18%	
7.1.	**7.1.**	**Recursos**		1	0	1	0	0	0%		
7.1.	7.1.	Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI	¿Se cuenta con un cronograma que incluya el personal requerido para la implementación de SGSI? ¿Se cuenta con un presupuesto aprobado para la implementación del SGSI? ¿Se ha definido el recurso humano para el mantenimiento y mejora del SGSI? ¿Se cuenta con un presupuesto aprobado para el mantenimiento y mejora del SGSI?	no		✔					Al momento del Diagnostico no se observa.
7.2.	**7.2.**	**Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información**		4	0	1	0	3	38%		
7.2.a	7.2.a	Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información	¿Se ha definido el perfil del cargo para las personas que realizan actividades que afecta directamente el SGSI, basado en la formación, educación o experiencia adecuada?	pa				✔			Seobserve que se establece a traves del manual de funciones. Se han dictado charlas sobre ISO27001. Actualmente durante el diagnostico habia personal en capacitacion SENA. No se informo si habia personal del área TICs
7.2.b	7.2.b	Asegurarse de que estas personas sean competentes (educación, formación o experiencia)	¿Se han tomado acciones para adquirir o mejorar la competencia?	pa				✔			
7.2.c	7.2.c	Cuando se aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de acciones tomadas	¿Se cuenta con documentación que de evidencia de la competencia?	no		✔					
7.2.d	7.2.d	Conservar la información documentada apropiada, como evidencia de la competencia		pa				✔			
7.3.	**7.3.**	**Toma de Conciencia**		3	**0**	**0**	**0**	**0**	0%		
7.3.a	7.3.a	Tomar conciencia de la política de SI	¿Se cuenta con evidencia de sensibilización sobre el SGSI al personal?	no		✔					Al momento del Diagnostico no se observa.
7.3.b	7.3.b	Contribución a la eficacia del SGSI, beneficios de una mejora del desempeño de la SI		no		✔					
7.3.c	7.3.c	Las implicaciones de la no conformidad con los requisitos del SGSI		no		✔					

Validación de Cumplimiento TI bajo la Norma NTC-ISO/IEC 27001:2013

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
7.4.	**7.4.**	**Comunicación**		5	**0**	**0**	**0**	**0**	0%		
		La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGSI, que incluya:									
7.4.a	7.4.a	Del contenido de la comunicación	¿Se cuenta con una matriz de comunicaciones de SI?	no		✔					Al momento del Diagnostico no se observa.
7.4.b	7.4.b	Cuando Comunicar		no		✔					
7.4.c	7.4.c	A quien comunicar		no		✔					
7.4.d	7.4.d	Quien debe comunicar		no		✔					
7.4.e	7.4.e	Los Proceso para llevar la comunicación		no		✔					
7.5.	**7.5.**	**Información Documentada**		11	0	0	0	11	**50%**		
7.5.1	**7.5.1**	**Generalidades**	¿Se cuenta con un proceso de control de la documentación internos y externos, aplicados al SGSI?								
7.5.1.a	7.5.1.a	Incluir la información documentada requerida por esta Norma		pa				✔			
7.5.1.b	7.5.1.b	Incluir la información documentada que la organización ha determinado para la eficacia del SGSI		pa				✔			
7.5.2	**7.5.2**	**Creación y actualización**									Se observan los procesos de control de documentos, pero estos tienen el enfoque desde ISO9001 y NTGCP1000
7.5.2.a	7.5.2.a	Asegurar la identificación y descripción		pa				✔			
7.5.2.b	7.5.2.b	Asegurar el formato y sus medios de soporte		pa				✔			
7.5.2.c	7.5.2.c	La revisión y aprobación con respecto a la idoneidad y adecuación		pa				✔			
7.5.3	**7.5.3**	**Control de la Información Documentada**									
7.5.3.a	7.5.3.a	Asegurarse que este disponible y adecuada para el uso, donde y cuando se necesite		pa				✔			Se observan los procesos de control de documentos, pero estos tienen el enfoque desde ISO9001.
7.5.3.b	7.5.3.b	Asegurarse que este protegida (contra perdida de confidencialidad, uso adecuado, perdida de integridad)		pa				✔			
7.5.3.c	7.5.3.c	Tratar actividades de distribución, acceso, recuperación y uso		pa				✔			
7.5.3.d	7.5.3.d	Tratar actividades de almacenamiento y preservación, incluida la preservación de la legibilidad		pa				✔			Se observan los procesos de control de documentos, pero estos tienen el enfoque desde ISO9001.
7.5.3.e	7.5.3.e	Control de cambios (ej.. versión)		pa				✔			
7.5.3.f	7.5.3.f	Retención y disposición		pa				✔			
8..	**8..**	**Operación**		3	0	10	0	0	33%	33%	
8.1.	**8.1.**	**Planificación y Control Operacional**		1	0	0	0	1	**50%**		
8.1.	8.1.	Planificación y Control Operacional	Como se planifican , controlan los procesos necesarios para cumplir los requisitos de seguridad de la información. (Gestión de Activos, Backups) Como se controlan para implementar las acciones del numeral 6.1 Como se controla que se implemente planes para asegurar el cumplimento de los objetivos de seguridad de la información.	pa				✔			Se observan los procesos de Planificación y Control, pero estos tienen el enfoque desde ISO9001.
8.2.	**8.2.**	**Valoración de Riesgos de la Seguridad de la Información**		1	0	0	0	1	**50%**		
8.2.	8.2.	Valoración de Riesgos de la Seguridad de la Información	¿Se ha realizado la valoración de los riesgos según la metodología definida?	pa				✔			Se observa valoracion de riesgos bajo una metodologia. No se informa que se realizaseguimiento.
8.3.	**8.3.**	**Tratamiento del Riesgos de la Seguridad de la Información**		1	**0**	**10**	**0**	**14**	0%		
8.3.	8.3.	Tratamiento del Riesgos de la Seguridad de la Información	¿Se ha elaborado el plan de tratamiento del SGSI según la metodología definida?	no		✔					
9..	**9..**	**Evaluación del Desempeño**		22	0	11	0	11	25%	24%	
9.1.	**9.1.**	**Seguimiento, Medición, Análisis y Evaluación**		6	**0**	**1**	**0**	**3**	0%		

Validación de Cumplimiento TI bajo la Norma NTC-ISO/IEC 27001:2013

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
9.1.a	9.1.a	Hacer seguimiento y medir lo necesario, incluidos los procesos y controles de SI	¿Se cuenta con la matriz de objetivos e indicadores del SGSI?	no		✔					
9.1.b	9.1.b	Los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados validos	¿Se ha diligenciado la Matriz de objetivos e indicadores del SGSI?	no		✔					Al momento del Diagnostico no se observa.
9.1.c	9.1.c	Cuando se debe llevar a cabo el seguimiento y medición	¿Se ha determinado como medir la eficacia de los controles y su periodicidad?	no		✔					
9.1.d	9.1.d	Quien debe llevar a cabo el seguimiento y la medición	¿Se ha medido la eficacia de los controles?	no		✔					
9.1.e	9.1.e	Cuando se debe analizar y evaluar los resultados del seguimiento		no		✔					Al momento del Diagnostico no se observa.
9.1.f	9.1.f	Quien debe analizar y evaluar estos resultados		no		✔					
9.2.	**9.2.**	**Auditoria Interna**		7	0	0	0	7	**50%**		
9.2.a	9.2.a	Conforme con los propios requisitos de la organización para su SGSI	¿Se han definido programa de auditoria interna para el SGSI?	pa				✔			Se observa que se realizan las auditorias desde CONTROL INTERNO hacia el macroproceso de Gestion de TICs, se debe dar orientación hacia el SGSI.
9.2.b	9.2.b	Conforme los requisitos de esta norma		pa				✔			
9.2.c	9.2.c	Planificar, establecer, implementar y mantener uno o varios programas de auditoria		pa				✔			
9.2.d	9.2.d	Definir los criterios y alcance de las auditorias		pa				✔			
9.2.e	9.2.e	Seleccionar los auditores y llevar a cabo auditorias para asegurar la objetividad e imparcialidad del proceso		pa				✔			
9.2.f	9.2.f	Asegurarse de los resultados de las auditorias se informan a la dirección pertinente	¿Se ha ejecutado el programa de auditoria interna según lo planificado?	pa				✔			
9.2.g	9.2.g	Conservar la información documentada apropiada, como evidencia de la implementación del programa de auditoria		pa				✔			
9.3.	**9.3.**	**Revisión por la dirección**		9	0	5	0	4	22%		
9.3.a	9.3.a	Debe incluir consideraciones sobre el estado de las acciones con relación a las revisiones previas por la dirección	¿Se ha definido un plan para la realización de la reunión de reunión por la dirección?	no		✔					Se observan los procesos de revision, pero estos tienen el enfoque desde ISO9001.
9.3.b	9.3.b	Los cambios interno y externo pertinentes al SGSI		no		✔					
9.3.c.1	9.3.c.1	Retroalimentar sobre: No conformidades y acciones correctiva	¿Se ha ejecutado la revisión por la dirección incluyendo los requisitos de norma?	pa				✔			
9.3.c.2	9.3.c.2	Seguimiento y resultado de las mediciones		pa				✔			
9.3.c.3	9.3.c.3	Resultados de la auditoria		pa				✔			
9.3.c.4	9.3.c.4	Cumplimiento de los objetivos		pa				✔			
9.3.d	9.3.d	Retroalimentación de las partes interesadas	¿Se evidencia la ejecución de la revisión por la dirección?	no		✔					
9.3.e	9.3.e	Resultados de la valoración de riesgo y estado del plan de tratamiento de riesgo		no		✔					
9.3.f	9.3.f	Las oportunidades de mejora continua		no		✔					
10..	**10..**	**Mejora**		11	0	1	0	10	**45%**	**48%**	
10.1.	**10.1.**	**No conformidades y Acciones Correctivas**		10	0	1	0	9	**45%**		
10.1.a.1	10.1.a.1	Reaccionar a la NC según sea aplicable tomar acciones para controlar y corregirla	¿Se cuenta con un procedimiento de no conformidades y acciones correctivas?	pa				✔			Se observan los procesos de no conformidades, pero estos tienen el enfoque desde ISO9001.
10.1.a.1	10.1.a.2	Hacerle frente a las consecuencias		pa				✔			
10.1.b.1	10.1.b.1	Evaluar la necesidad para eliminarlas las causas de la NC mediante la revisión de la NC		pa				✔			
10.1.b.2	10.1.b.2	La determinación de las causas de la NC		pa				✔			
10.1.b.3	10.1.b.3	La determinación de si existen NC similares, o que potencialmente podrían ocurrir		pa				✔			
10.1.c	10.1.c	Implementar cualquier acción necesaria		pa				✔			
10.1.d	10.1.d	Revisar la eficiencia de las acciones correctivas tomadas		pa				✔			
10.1.e	10.1.e	hacer cambios al SGSI		no		✔					

Validación de Cumplimiento TI bajo la Norma NTC-ISO/IEC 27001:2013

Ítem	M	Aspectos Requeridos del SGSI	Preguntas de Apoyo	RE	SI	NO	NA	PA	Objetivos/control	Dominios	Justificaciones
Ítem	**M**	**Controles**		**RE**	**SI**	**NO**	**NA**	**PA**	**Cumplimiento Control**	**Objetivos**	**Justificación**
10.1.f	10.1.f	Información documentada como evidencia de la naturaleza de las NC y cualquier acción posterior tomada	¿Se cuenta con información documentada de las acciones correctivas tomadas en el SGSI?	pa				✔			
10.1.g	10.1.g	Los resultados de cualquier acción correctiva		pa				✔			
10.2.	**10.2.**	**Mejora continua**		**1**	**0**	**0**	**1**	**0**	**50%**		
10.2.	10.2.	Mejora continua	¿se cuenta con un plan de acción de mejora continua con base en los resultados de la revisión por la dirección?	pa				✔			Se observa certificado ISO 9001, cumplimento MECI, se tiene establecido mejora continua desde la perspectiva de Calidad.
		TOTAL		**116**	**1**	**60**	**0**	**55**	25%	**26%**	