MEMORANDO

Medellin 2017-11-02 16:43:21
Rad 2017301932
Institución Universitaria
Colegio Mayor de Antioquia
profesional2controlinterno

2.2

Medellín, 02 de noviembre de 2017

PARA: Bernardo Arteaga Velasquez, Rector

DE: Profesional2 Control Interno

ASUNTO: Informe de auditoría proceso de Gestión de Tecnología e Informática.

A continuación se hace entrega del informe de la auditoría realizada al proceso de Gestión de Tecnología e Informática de la Institución Universitaria Colegio Mayor de Antioquia, sobre Técnicas de la Seguridad. Sistemas de Gestión de la Seguridad de la Información – Requisitos (Norma Técnica Colombina NTC-ISO-27001), elaborado por la Oficina de Control Interno.

Cualquier aclaración e información adicional estaremos a su disposición

Atentamente,

Marysol Varela Rueda

MARY SOL VARELA RUEDA

Anexos: Informe definitivo

INFORME DE AUDITORIA

INFORME DEFINITIVO AUDITORIA AL PROCESO DE GESTIÓN DE TECNOLOGÍA E INFORMÁTICA

La Auditoría Interna se constituye en una herramienta de gestión liderada por la Dirección de Control Interno, por medio de la cual se analizan las debilidades y fortalezas de los controles del proceso, donde se desarrollan actividades de evaluación y verificación de datos, para identificar posibles riesgos en el cumplimiento de las metas y los objetivos propuestos, con el ánimo de que a partir de las observaciones basadas en evidencias objetivas se permitan ajustes en la operación del proceso, facilitando la toma de decisiones a fin que se obtengan los resultados esperados.

En este informe se consigna la información correspondiente a los resultados de la actividad de auditoría interna, la cual incluye los análisis del auditor, teniendo como alcance la verificación de su objetivo y el avance en el cumplimiento de los requisitos y controles de la NTC-ISO-27001:2013.

Para esta auditoria se contó con la herramienta de autodiagnóstico de la norma ISO 27001:2013, la cual tiene distribuido el ciclo PHVA para la implementación de requisitos y controles, esta herramienta fue contestada por el líder del proceso de TI y la cual arrojo los siguientes puntajes, en cuanto a lo ejecutado dándole una meta más alta al que hacer.

FASE	META	TOTAL EJECUTADO
PLANEAR	30%	15.0%
HACER	40%	30.1%
VERIFICAR	15%	8.8%
ACTUAR	15%	10.0%
TOTAL	100%	63.8%

Después de analizar la información entregada por el líder se concluye que los porcentajes de ejecución son los siguientes:

FASE	META	TOTAL EJECUTADO
PLANEAR	30%	11.2%
HACER	40%	29.3%
VERIFICAR	15%	3.8%
ACTUAR	15%	1.3%
TOTAL	100%	45.5%

1. IDENTIFICACIÓN EN EL PLAN DE DESARROLLO

El proceso de Gestión de Tecnología e Informática en el Plan de Desarrollo 2016 – 2020 se encuentra en el Eje temático N° 6: Gestión Administrativa y Financiera, Componente 4: Infraestructura para el mejoramiento académico y el bienestar institucional, programa de necesidades físicas y tecnológicas para la enseñanza y el bienestar institucional y Plataformas y sistemas de información institucionales integradas.

Cuenta con dos indicadores de producto a los cuales se le hacen seguimiento por medio del plan indicativo, encontrando que:

Herramientas tecnológicas para la enseñanza incorporadas al desarrollo académico: En el seguimiento a este indicador se observa una meta del 90% del 2016 al 2019, la cual para el seguimiento al 2017 el indicador se encuentra en un 11% indicando actualización de los equipos correspondientes a 234 unidades.

Sistemas de información integrados (financiero y académico): En el seguimiento a este indicador se observa una meta de 2 (número) del 2016 al 2019, la cual para el seguimiento al 2017, se encuentra en un 0.5% de cumplimiento, indicando que se contrató la integración de los sistemas financiero y académico en el 2017-2.

2. SISTEMA DE GESTIÓN INTEGRAL

Se observa en el informe de auditoría interna del sistema de gestión integrado (GM-FR-04) vigencia 2016, que para el proceso de Gestión de Tecnología e Informática se registran una (1) observación, así:

A. En la caracterización del proceso GT-CA-001, versión 6, se hace referencia al Plan Estratégico de TIC, PETL, el cual se encuentran en proceso de construcción. No se debería referenciar allí hasta que no esté aprobado. Requisito NTCGP1000: ISO9001 NUMERAL 5.4.

Fecha proyectada de cierre: 16 de diciembre de 2016
Fecha de cierre: 21 de diciembre de 2016
Cerrada por: Profesional de Calidad

3. SISTEMA DE CONTROL INTERNO (MECI)

3.1 MODULO: Evaluación y seguimiento.

COMPONENTE: Auditoria interna.

3.2 PRINCIPIOS MECI:

Al consultar con el auditado sobre la aplicabilidad que le dan a los principios MECI, las respuestas fueron las siguientes:

AUTOCONTROL

- Evaluación Trabajo
- Correctivos, se realizan procesos correctivos ante una situación de prevención.
- Se realizan Comités de Técnicos.
- Se realizan mejoras al proceso cuando se requieren cambios en las plataformas.

AUTORREGULACIÓN

- Sensibilización Valores Institucionales
- Sensibilización Códigos Buen gobierno
- Políticas de TI

AUTOGESTIÓN

- Plan de Riesgos
- Competencias Laborales, Planes de trabajo personal.
- Supervisión, Plan de necesidades anuales

3.3 AUTOEVALUCION MECI

- Se realiza encuestas de satisfacción de usuarios, mediante el sistema de Mesa de Ayuda.

- Se realiza proceso de autoevaluación mediante las plataformas y aplicaciones (Naonquest) las cuales nos permiten obtener resultados de la Gestión interna a nivel técnico y operativo.

4. SITUACIÓN CONTEXTUAL DEL PROCESO O ACTIVIDAD

DEBILIDADES:

- Debilidad en la aplicación de la norma técnica NTC-ISO-27001.

OPORTUNIDADES:

- Apoyo de la Alta Dirección.
- Existencia de un marco normativo para la identificación de requisitos Y controles.

FORTALEZAS:

- Líder del proceso con fortalezas técnicas y operativas.
- Equipo de trabajo fortalecido.

AMENAZAS:

- Cambios constantes en la normatividad o requisitos.
- Falta de recursos.
- Aumento en la exposición a riesgos.

5. DESCRIPCIÓN DE HALLAZGOS Y OBSERVACIONES DEL EJERCICIO

5.1 Matriz de hallazgos

N° Y MARCA DE CLASE	HALLAZGO	ACCIÓN A SEGUIR POR PARTE DEL RESPONSABLE	RESPONSABLE
1. ☞	**Contexto de la organización:** No se cuenta con el contexto interno y externo de la institución que visibilice los factores que pueden exponer a riesgos la entidad en el manejo de la información, lo que evidencia Incumplimiento del numeral 4.1 de la NTC ISO 27001:2013. Lo anterior, impide identificar la afectación de lograr los resultados previstos en el sistema de gestión de la seguridad de la información.	Construcción del plan de mejoramiento con las acciones correctivas a definir o en su defecto las pruebas que justifiquen el cumplimiento total del requisito referenciado, por lo que se demuestra la inaceptación del hallazgo.	Líder de Gestión de Tecnología e Informática.
2 ☞	**Definición de marco de seguridad y privacidad de la entidad**. No se cuenta con los siguientes productos/requisitos de la norma:	Construcción del plan de mejoramiento con las acciones correctivas a definir o en su defecto las pruebas que justifiquen el cumplimiento total del requisito referenciado, por	Líder de Gestión de Tecnología e Informática.

N° Y MARCA DE CLASE	HALLAZGO	ACCIÓN A SEGUIR POR PARTE DEL RESPONSABLE	RESPONSABLE
	a) Plan inicial del proyecto con objetivos y aprobación por la alta dirección. b) Un comité de seguridad de la información. c) Una definición del alcance y los límites de seguridad de la información. d) Un documento de roles, responsabilidades y autoridades en seguridad de la información. e) Declaración de aplicabilidad que contenga los controles requeridos por la entidad. f) Modelo de comunicaciones internas como externas. g) El Sistema de Seguridad de la Información debidamente documentada y controlada. Incumpliendo con los numerales: 4. Contexto de la Organización, 5. Liderazgo, 6. Planificación, de la norma NTC ISO 27001:2013. Lo que puede demostrar poco liderazgo y compromiso con respecto al Sistema de gestión de la Seguridad de la información e influir negativamente en la determinación de riesgos y oportunidades que deben ser tratados.	lo que se demuestra la inaceptación del hallazgo.	
3 ☛	**<u>Implementación del plan de seguridad y privacidad de la información</u>**	Construcción del plan de mejoramiento con las acciones correctivas a definir o en su defecto las	Líder de Gestión de Tecnología e Informática.

N° Y MARCA DE CLASE	HALLAZGO	ACCIÓN A SEGUIR POR PARTE DEL RESPONSABLE	RESPONSABLE
	No se cuenta con los siguientes controles de la norma: a) Políticas para la seguridad de la información con revisión a intervalos. b) Contactos con grupos de interés especial. c) Seguridad de la información tratada en la gestión de proyectos independiente del proyecto. d) La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. e) Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. f) Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	pruebas que justifiquen el cumplimiento total del requisito referenciado, por lo que se demuestra la inaceptación del hallazgo	

N° Y MARCA DE CLASE	HALLAZGO	ACCIÓN A SEGUIR POR PARTE DEL RESPONSABLE	RESPONSABLE
	g) Desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. h) Deben diseñar y aplicar procedimientos para trabajo en áreas seguras. i) Adoptar una apolítica de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información. Incumpliendo con el anexo A (normativo) objetivos de control y controles de referencia y que se debe de usar en el contexto con el numeral 6.1.3 para el tratamiento de riesgos de la seguridad de la información establecidos por la norma NTC ISO 27001:2013, impidiendo definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información		
4 ☞	**<u>Monitoreo y mejoramiento continuo</u>** No se cuenta con los siguientes productos/requisitos de la norma: a) Metodología para realizar seguimiento, medición y análisis de la seguridad de la información.	Construcción del plan de mejoramiento con las acciones correctivas a definir o en su defecto las pruebas que justifiquen el cumplimiento total del requisito referenciado, por lo que se demuestra la inaceptación del hallazgo	Líder de Gestión de Tecnología e Informática.

N° Y MARCA DE CLASE	HALLAZGO	ACCIÓN A SEGUIR POR PARTE DEL RESPONSABLE	RESPONSABLE
	b) Auditorías internas de gestión de seguridad de la información c) Programas de auditoria aplicable al sistema de gestión de seguridad de la información. d) Las revisiones periódicas al sistema de gestión de seguridad de la información y su retroalimentación sobre el desempeño de la seguridad de la información. e) En cuanto a las auditorías internas de gestión se derivan otras actividades las cuales no se han desarrollado por falta de la primera, estas son: f) Respuesta a las no conformidades referentes a la seguridad de la información presentadas en los planes de auditoria. g) Implementación de acciones a las no conformidades de seguridad de la información presentadas. h) Revisión de la eficiencia de las acciones correctivas tomadas por la presencia de una no conformidad de seguridad de la información. i) Realizar cambios al Sistema de Gestión de Seguridad de la Información después de las acciones tomadas.		

N° Y MARCA DE CLASE	HALLAZGO	ACCIÓN A SEGUIR POR PARTE DEL RESPONSABLE	RESPONSABLE
	j) realizar procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información Incumpliendo con los numerales: 9) evaluación del desempeño, 10) mejora, de la norma NTC ISO 27001:2013. Conllevando a que no se realice una evaluación del desempeño de la seguridad de la información y la eficacia del Sistema de Gestión de la seguridad de la información y su respectiva mejora.		

Fuente: Elaborado y adaptado por la Oficina de Control Interno e información suministrada por el proceso de Gestión de Tecnología e Informática.

MARCAS

MARCA **	EXPLICACIÓN
☞	Hallazgo de auditoria

5.2. Observaciones.

1. Se observa que no se cumplió con la fecha estipulada de cierre para la observación establecida en el software de calidad Isolucion con referencia 222 (fecha proyectada de cierre 16 de diciembre de 2016), además, esta acción fue cerrada por la profesional de calidad no por el líder del proceso, como es debido.

2. Sería importante fortalecer la interiorización de los principios MECI al igual que la autoevaluación del proceso, ya que no es evidente su implementación de manera permanente en su actuar.

3. Si bien se cuenta con el borrador de la política de seguridad de la información y los objetivos de seguridad de la información aún no se encuentra aprobada por la Alta Dirección ni socializada a la comunidad, tampoco se encuentra disponible para las partes interesadas, lo que puede conllevar al incumplimiento de los numerales 5.1 y 5.2 de la norma NTC-ISO 27001:2013.

4. Se cuenta con el borrador de los objetivos de seguridad de la información, sin embargo, no han sido socializados con la comunidad, lo que puede llevar a incumplir con el numeral 6.2 dela norma.

5. Si bien Planeación Institucional realiza la revisión al Sistema de Gestión de la Seguridad de la Información, no se evidencia un procedimiento sistemático y organizado para el seguimiento a las políticas y normas que sobre seguridad de la información existen, lo que expone la Institución a riesgos de incumplimiento de la norma, en su numeral 9.3.

6. En el primer componente de la definición de marco de seguridad y privacidad de la entidad se identificaron algunos requisitos implementados parcialmente, estos son:

   - Identificación de las partes interesadas necesidades y expectativas respecto a la seguridad de la información.

   - La evaluación de los objetivos y las necesidades con respecto a la seguridad de la información.

   - Un documento de la política de Seguridad de la información aprobada por la dirección.

   - la evaluación de las competencias de las personas que realizan un trabajo que afecte el desempeño de la seguridad de la información.

Se hace necesario que se retomen estos elementos y se les de la aplicación requerida.

7. En el segundo componente de la implementación del plan de seguridad y privacidad de la información se identificaron algunos requisitos implementados parcialmente, estos son:

   - Conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.

   - Adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

   - La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

   - Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

- Contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.

- Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.

- El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

- Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

8. En el tercer componente de monitoreo y revisión, se observa algunos requisitos no implementados y derivados de las auditorías internas al sistema de Gestión de la seguridad de la información, estas son:

   - Revisiones por la Alta Dirección al Sistema de Gestión de Seguridad de la información y debidamente documentadas.

   - Documentación de la información referente a las acciones correctivas con respecto a la seguridad de la información.

9. Se determina que la implementación de requisitos de la norma ISO 27001:2013, se encuentra en un 45.5% de avance, evaluación que fue realizada de acuerdo a la identificación y distribución en el ciclo PHVA, la cual es referenciada en el manual de Gobierno en Línea en el componente de seguridad y privacidad de la información.

5.3. Descripción del riesgo.

OPERATIVOS: Son donde se gestionan los recursos institucionales, comprende los riesgos de la parte técnica de la entidad, incluye los riesgos asociados con el funcionamiento de los sistemas de información.

RIESGOS DE CUMPLIMIENTO: se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales y compromisos en general ante la comunidad.

Los tipos de riesgo que se evidencian materializados en la operación, de acuerdo a la información gestionada durante el proceso de auditoría son operativos y de cumplimiento, por lo que queda demostrado que es necesario analizar y replantear controles, definir acciones de cumplimiento y fortalecer tanto los canales como las herramientas para el manejo de la información.

5.4 Resumen de hallazgos y observaciones

PROCESO Y/O SUBPROCESO RESPONSABLE	N° DE HALLAZGOS	N° DE OBSERVACIONES
Gestión de Tecnología e Informática	4	9
TOTAL	**4**	**9**

Se adjunta la herramienta utilizada para el autodiagnóstico.

6. CONCLUSIONES.

1. Se observan que el contrato de suministro de mínima cuantía - MC017-17, cumple con los requisitos y obligaciones, además se cuenta con el compromiso 1487 por $17.911.500 y el siguiente movimiento:
   OP 1861 del 29 de marzo y CE 1995 por $ 660.389.
   OP 4094 del 26 de mayo y CE 4245 por $ 1.249.500.
   OP 7232 del 8 de agosto y CE 7772 por $7.721.910
   Quedando un saldo por cancelar de $8.279.701

2. Se diligenció el autodiagnóstico de seguridad de la información, para medir el avance en la entidad en cuanto al Sistema de Gestión de Seguridad de la Información, información que fue analizada por la profesional de control interno y con la cual se realizó el presente informe.

3. El objetivo del autodiagnóstico es determinar el nivel de madurez que presenta la entidad respecto a los temas relacionados con la seguridad de la información.

4. El autodiagnóstico se dividió en tres partes, así:

   1: Definición del Marco de Seguridad y Privacidad de la Entidad. Tiene un peso porcentual del 30% del total del componente, llegando a una implementación del 11.2%.

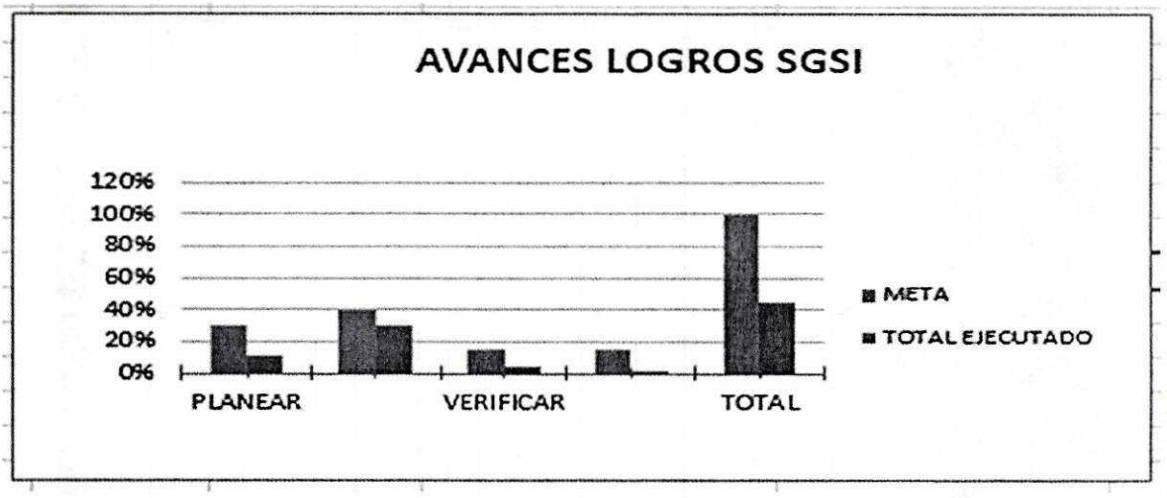
   2: Implementación del Plan de Seguridad y Privacidad, con un peso porcentual del 40% del total del componente, con una implementación del 29.3%.

   3: Monitoreo y mejoramiento continuo, con un peso porcentual del 30% del total del componente, repartido en: 15% - Actividades de seguimiento, medición, análisis y evaluación y 15% - Revisión e Implementación de Acciones de Mejora, encontrando una implementación del 5.0%.

   La norma referente para esta herramienta es: NTC-ISO-IEC 27001:2013

5. En la tabla que se ven a continuación se puede hacer el comparativo de la fase, la meta y el total ejecutado por componente, además del grafico de avance.

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	11.2%
LOGRO2	HACER	40%	29.3%
LOGRO3	VERIFICAR	15%	3.8%
	ACTUAR	15%	1.3%
	TOTAL	100%	45.5%



En cuanto a los controles se determinan por dominio de control, identificando que de los 114 controles, nos aplican 107 de los cuales se han implementado 66, parcialmente 25, no cumplen 16.

RESUMEN LOGRO 1		
	CONTROLES	
	66	24.7%
114	25	4.7%
	16	0.0%
	7	2.8%
	No. Controles que le aplican	107
	TOTAL	29.3%

POR DOMINIO DE CONTROL						
NOMBRE DOMINIOS DE CONTROL	CONTROLES QUE APLICAN	PESO CONTROLES IMPLEMENTADOS Y PARCIALMENTE IMPLEMENTADOS	IMPLEMENTADOS	PARCIALMENTE	NO CUMPLE	NO APLICA
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	2	0.5	0	1	1	0
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	7	3.5	3	1	3	0
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	6	3	2	2	2	0
DOMINIO 8 - GESTIÓN DE ACTIVOS	10	7	6	2	2	0
DOMINIO 9 - CONTROL DE ACCESO	14	13	12	2	0	0
DOMINIO 10 - CRIPTOGRAFÍA	2	1	1	0	1	0
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	14	9	7	4	3	1
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	14	13.5	13	1	0	0
DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	6	4.5	3	3	0	1
DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	8	7.5	7	1	0	5
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	5	2.5	1	3	1	0
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	7	5.5	5	1	1	0
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	4	3.5	3	1	0	0
DOMINIO 18 - SEGURIDAD DE LAS COMUNICACIONES	8	4.5	3	3	2	0
	107		66	25	16	7

7. GLOSARIO

Autocontrol: Capacidad que deben desarrollar todos y cada uno de los servidores públicos de la organización, independiente de su nivel jerárquico para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para el adecuado cumplimiento de los resultados que se esperan en el ejercicio de su función[1].

Autogestión: Capacidad de toda organización publica para interpretar, coordinar, aplicar y evaluar de manera efectiva, eficiente y eficaz la función administrativa que le ha sido asignada por la constitución, la ley y sus reglamentos [1].

Autorregulación: capacidad de cada una de las organizaciones para desarrollar y aplicar en su interior métodos, normas y procedimientos que permitan el desarrollo, implementación y fortalecimiento continúo del sistema de control interno en concordancia con la normatividad vigente [1].

Autoevaluación: Es aquel componente que le permite a cada responsable del proceso, programas y/o proyectos y sus funcionarios medir la efectividad de sus controles y los resultados de la gestión en tiempo real, verificando su capacidad para cumplir las metas y los resultados a su cargo y tomar las medidas correctivas que sean necesarias para el cumplimiento de los objetivos previstos por la entidad [1].

Elaboró: Marysol Varela Rueda
Marysol Varela Rueda
Profesional de Control Interno
Fecha: Septiembre 28 de 2017

Revisó y Aprobó:
Edit Yohana Palacio Espinosa
Directora Operativa de Control Interno
Fecha: Octubre 13 de 2017

AUTODIAGNÓSTICO SGSI LOGRO 1: DEFICINIÓN DE MARCO DE SEGURIDAD Y PRIVACIDAD DE LA ENTIDAD (30%)

Por favor, conteste la siguiente encuesta de acuerdo con el instructivo.

Estado	DESCRIPCIÓN
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona.
No cumple	No existe y/o no se está haciendo.

RESUMEN LOGRO 1		
TOTAL	PESO	
1	1.5%	
6	4.6%	
6	0.0%	
1	5.0%	Autodiagnóstico
1	0.0%	Plan de trabajo
TOTAL	11.2%	

		PLANEAR		
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
1	La entidad cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI (Sistema de Gestión de Seguridad de la información?	Cumple satisfactoriamente	Se tiene formato diligenciado en actas de gobierno en línea. Se diligencio este diagnostico en su totalidad.	Diligenciar autodiagnóstico de seguridad de la información.
2	La entidad creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	No cumple		Crear caso de estudio o plan inicial del proyecto que incluya prioridades y objetivos del SGSI, estructura del SGSI.
3	La entidad contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	No cumple		Debe existir un documento preliminar de aprobación firmado por parte de la dirección donde se aprueba el inicio del proyecto.
4	La entidad ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la información?	No cumple	Mediante Matriz de Riesgos, identificación y Control, Causas. No se evidencia en la matriz de riesgos los factores interno y externos que afecten el SGSI.	Se deben identificar los temas tanto externos como internos que pueden afectar el desarrollo de los resultados del sistema.
5	La entidad ha identificado las partes interesadas, necesidades y expectativas de estas respecto al Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente		Se requiere que se identifiquen las partes interesadas tanto internas como externas, detallando cuáles son sus necesidades y expectativas en la implantación del Sistema de Gestión de Seguridad de la Información.
6	La entidad ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	Cumple parcialmente	Mediante la Política. La política no se encuentra aprobada ni socializada con la comunidad.	Realizar la identificación de los objetivos y las necesidades que tiene la entidad respecto a la seguridad de la información.
7	En la entidad se ha definido un Comité de Seguridad de la Información?	No cumple		Definir mediante acto administrativo el comité de seguridad de la información que describa las responsabilidades de los integrantes, reuniones entre otros.
8	La entidad cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	No se evidencia el alcance y los límites del sistema.	Crear un documento de alcance del Sistema de Gestión de Seguridad de la Información y sus respectivos límites en cuanto a TIC, límites físicos, temas internos y externos.
9	En la entidad existe un documento de política del Sistema de Gestión de Seguridad de la información, el cual ha sido aprobado por la Dirección?	Cumple parcialmente	Se tiene Política. Falta Socializar	Crear un documento que defina la política general del Sistema de Gestión de Seguridad de la Información y sus respectivos límites. Tener en cuenta objetivos del SGSI, marco regulatorio, el cual debe estar debidamente documentado y socializado.
10	En la entidad existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	Cumple parcialmente	Planes de trabajo. No se cuenta con la definición de roles y responsabilidades en la etapa de implementación del sistema.	Se deben definir roles y responsabilidades para cada etapa de la implementación.
11	La entidad tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	Cumple satisfactoriamente	Plan de Riesgos. Si bien se cuenta con el mapa de riesgos, no se observan riesgos que tengan que ver con el sistema de seguridad de la información.	Se debe seleccionar una metodología para gestionar los riesgos y describir en una matriz de riesgos los resultados de acuerdo a los criterios de aceptación de los mismos. Nota: Si la entidad ya tiene una matriz de riesgos, se deben identificar los riesgos que apunten a la seguridad de la información.
12	La entidad ha realizado una declaración de aplicabilidad que contenga los controles requeridos por la entidad?	No cumple		Crear documento de declaración de aplicabilidad donde se justifique la inclusión y exclusión de controles del Anexo A de la norma ISO27001 versión 2013.
13	La entidad ha evaluado las competencias de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la seguridad de la Información?	Cumple parcialmente	Planes de autoevaluación. Se cuenta con las hojas de vida de los funcionarios que están en el proceso de TI.	Se debe conservar la información que evidencie las competencias del personal que se encuentre involucrado con la seguridad de la información de la entidad. Se debe definir un plan de capacitación con el fin de que dichas personas adquieran las competencias respectivas.
14	La entidad tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	No cumple		Se debe desarrollar un modelo que indique el contenido de la comunicación; fechas, a quién se comunica y quién comunica.
15	La entidad tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	No cumple	Se tienen Políticas TI. Falta Socializar. No se cumple con los requisitos ni los controles de esta norma documentación	Toda la documentación generada del Sistema de Gestión de Seguridad de la Información debe estar debidamente documentada.

Fuente: NTC-ISO-IEC 27001:2013

AUTODIAGNÓSTICO SGSI LOGRO 2: IMPLEMENTACIÓN DEL PLAN DE SSEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (40%)

Por favor, contesta la siguiente encuesta, de acuerdo con el Instructivo.

Estado	Significado
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
Cumple parcialmente	Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió pero no se gestiona.
No cumple	No existe y/o no se está haciendo.
No aplica	El control no es aplicable para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

	RESUMEN LOGRO 1	
	CONTROLES	
	66	24.7%
114	25	4.7%
	16	0.0%
	7	2.8%
	No. Controles qué le aplican	107
	TOTAL	29.3%

		ANEXO		ESTADO	EVIDENCIA
	A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION			
	A5.1	Orientación de la dirección para la gestión de la seguridad de la información			
	Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes				
1	A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Cumple parcialmente	Se tiene la política, hace falta aprobación. La aprobación la realiza el consejo directivo, solo se cuenta con el borrador.
2	A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	[redacted]	Al no tener la política aprobada y socualizada no se revisa para su adecuación.
	A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION			
	A6.1	Organización interna			
	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				
3	A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Cumple satisfactoriamente	Se tienen definidos los roles desde los planes de trabajo del personal de TI
4	A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	Cumple satisfactoriamente	Se tienen definidos los roles desde los planes de trabajo del personal de TI
5	A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	[redacted]	
6	A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	[redacted]	
7	A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	[redacted]	
	A6.2	Dispositivos móviles y teletrabajo			
	Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles				
8	A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Cumple parcialmente	Reglas y Políticas en dispositivo de seguridad perimetral para mitigar las amenazas informáticas con dispositivos móviles. Evidencia. Diseño de la red
9	A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	Cumple satisfactoriamente	Reglas y Políticas en dispositivo de seguridad perimetral acceso seguro por VPN. Evidencia. Diseño de la red
	A7	SEGURIDAD DE LOS RECURSOS HUMANOS			
	A7.1	Antes de asumir el empleo			
	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
10	A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	Cumple satisfactoriamente	En el momento de la contratación el funcionario aporta los antecedentes (policía, contraloría, procuraduría).
11	A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Cumple parcialmente	Desde el area Jurídica. En el momento de la contratación se dejan consignados en la minuta las actividades a desarrollar y sus responsabilidades, pero no se especifica cuales son las responsabilidades en cuanto al tema de seguridad de la información.
	A7.2	Durante la ejecución del empleo			
	Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				
12	A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	[redacted]	
13	A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	[redacted]	
14	A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Cumple parcialmente	
	A7.3	Terminación y cambio de empleo			
	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo				
15	A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Cumple satisfactoriamente	
	A8	GESTION DE ACTIVOS			
	A8.1	Responsabilidad por los activos			
	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.				

16	A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Cumple satisfactoriamente	Se tienen Inventarios de activos institucionales, con su respectivo identificador. No se observa un inventario de instalaciones de procesamiento de información e instalaciones.
17	A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	Cumple satisfactoriamente	Se tiene inventario con responsable. No se observa un inventario de instalaciones de procesamiento de información e instalaciones, por lo tanto no se observa responsable del mismo.
18.04	A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Cumple parcialmente	Desde el documento de Politicas de TI. Falta socializar. Politica que se encuentra en borrador, no esta aprobada por el consejo directivo ni socializada ante la comunidad.
19	A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Cumple satisfactoriamente	El control se realiza desde el proceso de Bienes y Servicios. El procesos de TI, revisa todo los activos que tienen que ver con TI y da su visto bueno para el paz y salvo
	A8.2	Clasificación de la información			
	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
20	A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Cumple parcialmente	La información importante es protegida y clasificada y se tiene controles por permisos de lectura y modificación en sistemas de información, servidores de archivo, y bases de datos
21	A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	[redacted]	
	A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	[redacted]	
	A8.3	Manejo de medios			
	Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios				
22	A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Cumple satisfactoriamente	Se tienen controles automaticos desde el Sisetma Antivirus para gesitonar los medios removibles. Ver Politica en Antivirus
23	A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Cumple satisfactoriamente	Se tiene un proceso de custodia de cintas de backup. El cual es utilizado cuando se requiere el servicio. Ver procedimiento de copias.
24	A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Cumple satisfactoriamente	Copias de seguridad en medios magnéticos en custodia en sitio externo son protegidos con un algoritmo de cifrado de clave simétrica utilizando software Veeam Backup & Replication 9.5. evidencia en plan de contingencias
	A9	CONTROL DE ACCESO			
	A9.1	Requisitos del negocio para el control de acceso			
	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				
25	A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Cumple satisfactoriamente	Perfiles de usuario, sólo acceso mediante autenticacion. Ver procedimiento creacion de cuentas.
26	A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Cumple satisfactoriamente	Se tienen segmentada la red de datos por VLANs (administrativos, estudiantes y docentes.). Las cuentas de red solo acceden a los recursos red previamente autorizados en sistemas de información, servidores centralizados de archivos, bases de datos, etc. Evidencias en diseño de red.
	A9.2	Gestión de acceso de usuarios			
	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
27	A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Cumple satisfactoriamente	Perfiles de usuario, sólo acceso mediante autenticacion. Ver procedimiento creacion de cuentas
28	A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Cumple satisfactoriamente	Perfiles de usuario, sólo acceso mediante autenticacion. Ver procedimiento creacion de cuentas
29	A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Cumple satisfactoriamente	Perfiles de usuario, sólo acceso mediante autenticacion. Ver procedimiento creacion de cuentas
30	A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Cumple satisfactoriamente	Se tiene definido procedimiento de solicitud de cuentas de usuario. Ver procedimiento solicitud de servicios.
31	A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Cumple parcialmente	Los lideres de los procesos son los encargados de solicitar creación de cuentas o el personal desognado.
32	A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Cumple satisfactoriamente	Las cuentas de red de los empleados con contrato a término fijo o provisional caduca en la misma fecha del contrato. Evidencias en diseño de red.
	A9.3	Responsabilidades de los usuarios			
	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				

33	A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Cumple satisfactoriamente	Mediante los procedimientos de creación de cuentas de usuario se definen y crean los perfiles en lo servidores. Se iinforma y divulga sobre la importancia del uso de las contrseñas.
	A9.4	Control de acceso a sistemas y aplicaciones			
	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				
34	A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Cumple satisfactoriamente	Se definen mediante los perfiles de usuario.
35	A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Cumple parcialmente	Se debe documentar los procesos de ingreso seguro
36	A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Cumple satisfactoriamente	Permiten la interacción con los usuarios, políticas de contraseña.
37	A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Cumple satisfactoriamente	Los equipos informáticos están controlados desde los Dominios de trabajo. Las políticas de usuario en el Sistema, no permite instalar software. Ver procedimiento de creación de cuentas de usuario.
38	A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	Cumple satisfactoriamente	Los códigos fuente están protegidos sólo con acceso de los usuarios autorizados.
	A10	CRIPTOGRAFIA			
	A10.1	Controles criptográficos			
	Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información				
39	A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Cumple satisfactoriamente	Políticas de creación de cuentas de usuario
40	A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	[redacted]	
	A11	SEGURIDAD FISICA Y DEL ENTORNO			
41	A11.1	Áreas seguras			
	Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
42	A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	Cumple satisfactoriamente	Se tiene definido los Pc que pueden ser vulnerables a ataques. Por ejemplo. Equipo que realizan pagos desde financiera.
43	A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Cumple parcialmente	El centro de datos y los cuartos de cableado cuenta con restricción de acceso de solo personal autorizado. Evidencias en diseño de red.
44	A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..	No aplica	
45	A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Cumple satisfactoriamente	Se definen como por ejemplo la protección física del Data Center, Planta eléctrica, UPS y circuito regulado.
46	A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	[redacted]	
47	A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Cumple satisfactoriamente	Los cuartos técnicos y Data Center están aislados de las oficinas de trabajo. Sólo se permite acceso a personal autorizado.
	A11.2	Equipos			
	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
48	A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Cumple parcialmente	El centro de datos y los cuartos de cableado cuenta con restricción de acceso de solo personal autorizado. Evidencias en diseño de red.
49	A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Cumple satisfactoriamente	La institución cuenta con un suministro de energía alterno por UPS y Planta Eléctrica. Evidencias en diseño de red.
50	A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Cumple satisfactoriamente	El cableado viaja por bandejas Portacables por la parte superior de las rutas del cableado. Evidencias diseño de red.
51	A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Cumple satisfactoriamente	Se cuenta con mantenimientos programados para servidores, dispositivos, y estaciones de trabajo de usuario final.
52	A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	Cumple parcialmente	Se cuenta con control de salida e ingreso de equipo por las porterías de la IUCMA. Las cuentas de red de los empleados no cuentas con permisos administrativos sobre las estaciones de trabajo para instalar o desinstalar componentes.
53	A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Cumple parcialmente	Se realiza registro de salidas de equipos.
54	A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.	Cumple satisfactoriamente	Los usuarios de Dominio, no tienen acceso a instalar o desinstalar software.
55	A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	[redacted]	
56	A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	[redacted]	
	A12	SEGURIDAD DE LAS OPERACIONES			
	A12.1	Procedimientos operacionales y responsabilidades			
	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
57	A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Cumple satisfactoriamente	Procedimientos en software isolucion.
58	A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Cumple satisfactoriamente	Procedimientos en software isolucion.

59	A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Cumple satisfactoriamente	La plataforma tecnológica cuenta con herramientas para monitorear el estado de los recursos, disponibilidad y planeación de la capacidad. Evidencias en diseño de red
60	A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se desen separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Cumple satisfactoriamente	La plataforma tecnológica cuenta un ambiente de laboratorio aislado de el de producción. Evidencias en diseño de red
	A12.2	Protección contra códigos maliciosos			
	Objetivo: Asegurarse de que la información y las instalaciones ce procesamiento de información estén protegidas contra códigos malicioso.				
61	A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Cumple satisfactoriamente	La entidad cuenta con software antivirus instalado en los servidores y estaciones de trabajo para detectar, remover y prevenir software para fines maliciosos o intrusivos. Evidencias en diseño de red
	A12.3	Copias de respaldo			
	Objetivo: Proteger contra la perdida de datos				
62	A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Cumple satisfactoriamente	La entidad cuenta con copias de seguridad programadas de la plataforma tecnológica, de tipo full e incrementales. Evidencias en diseño de red
	A12.4	Registro y seguimiento			
	Objetivo: Registrar eventos y generar evidencia				
63	A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Cumple satisfactoriamente	En la entidad se revisa y se audita los registros de servidores, aplicaciones, software antivirus, dispositivo de seguridad para detectar y prevenir fallas a los sistemas. Evidencias en diseño de red
64	A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Cumple satisfactoriamente	Solo los administradores de la plataforma pueden acceder en modo lectura o modificación a los registros. Evidencias en diseño de red
65	A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Cumple satisfactoriamente	Se cuenta con un documento de cambios y mejoras donde se documentan todos los procedimientos realizados sobre la plataforma tecnologica. Evidencias en diseño de red
66	A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Cumple satisfactoriamente	Se cuenta en la red interna con servidores NTP para atender los dispositivos de la entidad. Evidencias en diseño de red
	A12.5	Control de software operacional			
	Objetivo: Asegurarse de la integridad de los sistemas operacionales				
67	A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Cumple satisfactoriamente	Las cuentas de red de los empleados no cuentan con permisos administrativos sobre las estaciones de trabajo para instalar o desinstalar componentes.
	A12.6	Gestión de la vulnerabilidad técnica			
	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				
68	A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Cumple parcialmente	Regularmente se realizan procedimientos de actualización de firmwares, y software de la plataforma tecnológica según las mejores prácticas de los fabricantes.
69	A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Cumple satisfactoriamente	Solo el personal de soporte tiene los permisos de instalación de software autorizado. Las cuentas de red de los empleados no cuentas con permisos administrativos sobre las estaciones de trabajo para instalar o desinstalar componentes. Adicionalmente el software antivirus institucional opera como una capa adiciona.
	A12.7	Consideraciones sobre auditorias de sistemas de información			
	Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos				
70	A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Cumple satisfactoriamente	La entidad cuneta con mantenimientos programados de software y hardware para la plataforma tecnologia y las estaciones de trabajo.
	A13	SEGURIDAD DE LAS COMUNICACIONES			
	A13.1	Gestión de la seguridad de las redes			
	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
71	A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Cumple satisfactoriamente	Se realiza por medio de la gestión en los Sistemas de Seguridad
72	A13.1.2	Seguridad de los servicios de red	Control: Se ceben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos ce gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Cumple satisfactoriamente	La entidad cuenta con redes segmentadas y separadas por VLANs. Politicas de acceso, firewall perimetral, publicación segura de servicios en internet. Evidencia diseño de red.
73	A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Cumple satisfactoriamente	La entidad cuenta con redes segmentadas y separadas por VLANs. Politicas de acceso, firewall perimetral, publicación segura de servicios en internet. Evidencia diseño de red.
	A13.2	Transferencia de información			
	Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
74	A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Cumple parcialmente	Se tienen definidos procedimientos, hace falta realizar documentación y socialización.
75	A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio ente la organización y las partes externas.	Cumple parcialmente	Se tienen definidos procedimientos, hace falta realizar documentación y socialización.

76	A13.2.3	Mensajería Electronica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Cumple parcialmente	Desde las políticas de TI y Seguridad de la información. Falta socializar.
77	A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	No aplica	
	A14	Adquisición, desarrollo y mantenimiento de sistemas			
	A14.1	Requisitos de seguridad de los sistemas de información			
	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.				
78	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Cumple parcialmente	Desde las nuevas políticas de TI.
79	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	No aplica	
80	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Cumple satisfactoriamente	Los Servicios del UTM y seguridad Perimetral sirven de apoyo ante transacciones de aplicaciones
	A14.2	Seguridad en los procesos de Desarrollo y de Soporte			
	Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
81	A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	No aplica	No se desarrolla software internamente.
82	A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	No aplica	No se desarrolla software internamente.
83	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Cumple satisfactoriamente	Se tienen esquemas y plataformas replica de servidores para realizar pruebas. Primero se aplican cambios en pruebas y luego en producción.
84	A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	No aplica	
85	A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Cumple satisfactoriamente	Las reuniones de Necesidades entre procesos se informa, establece y prioriza sobre la seguridad e integración entre los Sistemas de Información
86	A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	No aplica	No se desarrolla software internamente.
87	A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Cumple satisfactoriamente	Se realizan reuniones y se efectuan informes de actividades.
88	A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Cumple satisfactoriamente	Se realizan
89	A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Cumple satisfactoriamente	Se tienen esquemas y plataformas replica de servidores para realizar pruebas.
	A14.3	Datos de prueba			
	Objetivo: Asegurar la protección de los datos usados para pruebas.				
90	A.14.3.1	Protección de datos de prueba	Control:Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Cumple satisfactoriamente	Se tienen esquemas y plataformas replica de servidores para realizar pruebas.
	A15	RELACIONES CON LOS PROVEEDORES			
	A15.1	Seguridad de la información en las relaciones con los proveedores.			
	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
91	A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Cumple parcialmente	Se tiene definido que el acceso de los proveedores a los equipos institucionales será por medio de VPN por medio de autenticaciones y validaciones de usuario en en los perfiles de trabajo de los usuarios. Hace falta documentar. Ver Dcto Proveedor Une.
92	A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Cumple parcialmente	Desde las reuniones de trabajo con proveedores externos
93	A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	[redacted]	
	A15.2	Gestión de la prestación de servicios de proveedores			
	Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
94	A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Cumple satisfactoriamente	Se tienen informes de seguimiento del mantenimiento de los aplicativos. Ver informes de seguimiento Software interno
95	A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	Cumple parcialmente	Desde las reuniones que se realizan, se verifican los servicios y parámetros de seguridad en los Sistemas, aplicaciones e informes en general. Ver informes de Casos de uso sobre desarrollo en integraciones.
	A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION			
	A16.1	Gestión de incidentes y mejoras en la seguridad de la información			
	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
96	A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Cumple satisfactoriamente	Los roles y responsabilidades están definidos desde los planes de trabajo para el actuar de los indicentes.
97	A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Cumple satisfactoriamente	Se ha tratado de socializar mediante Flash informativo sobre eventos y amenazas

98	A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Cumple parcialmente	Se ha tratado de socializar mediante Flash Informativo sobre eventos y amenazas
99	A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Cumple satisfactoriamente	Definidos en el Plan de Contingencia
100	A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Cumple satisfactoriamente	Definidos en el Plan de Contingencia
101	A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	Cumple satisfactoriamente	Los incidentes anteriores, se han mejorado los procedimientos en Copias de Seguridad, continuidad del negocio.
102	A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	[redacted]	
	A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO			
	A17.1	Continuidad de Seguridad de la información			
	Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
103	A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Cumple satisfactoriamente	Se tiene Plan de Continuidad del Negocio
104	A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Cumple satisfactoriamente	Se tiene Plan de Continuidad del Negocio
105	A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Cumple satisfactoriamente	Desde los respaldos y copias de sguridad de BD, aplicaciones. Servidores réplica.
	A17.2	Redundancias			
	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
106	A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Cumple parcialmente	Se tienen Copias de BD, Aplicaciones y servidores dentro del entorno de Insfraestructura.
	A18	CUMPLIMIENTO			
	A18.1	Cumplimiento de requisitos legales y contractuales			
	Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
107	A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	[redacted]	
108	A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Cumple parcialmente	Desde las Políticas nuevas de TI.
109	A18.1.3	Protección de registros	Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Cumple satisfactoriamente	Se tienen Políticas de Backup, Controles de Accesos no atorizados.
110	A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	[redacted]	
111	A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Cumple satisfactoriamente	Se tienen definido controles para el resguardo y atenticación de usuarios, definición de contraseñas.
	A18.2	Revisiones de seguridad de la información			
	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
112	A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Cumple parcialmente	Desde los comités y reuniones de trabajo con el personal de TI.
113	A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	Cumple satisfactoriamente	Desde los comités y reuniones de trabajo con el personal de TI.
114	A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Cumple parcialmente	Desde los comités y reuniones de trabajo con el personal de TI

Fuente: NTC-ISO-IEC 27001:2013

AUTODIAGNÓSTICO SGSI LOGRO 3: MONITOREO Y MEJORAMIENTO CONTINUO (30 %)

Por favor, conteste la siguiente encuesta de acuerdo con el instructivo.

Estado	DESCRIPCIÓN
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona.
No cumple	No existe y/o no se está haciendo.

VERIFICAR		ACTUAR	
TOTAL	PESO	TOTAL	PESO
0	0.0%	0	0.0%
3	3.8%	1	1.3%
3	0.0%	5	0.0%
TOTAL	3.8%	TOTAL	1.3%

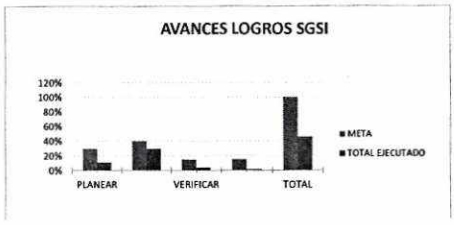
TOTAL LOGRO	5.0%

VERIFICAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
1	La entidad tiene una metodología para realizar seguimiento, medición y análisis permanente al desempeño de la Seguridad de la Información.?	No cumple		Se debe tener en cuenta que se desea medir, cuando, quien realizará la medición y cuando se analizaran los resultados.
2	La entidad ha realizado auditorías internas al Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	Desde las Auditorías internas. Sistemas de autodiagnóstico. No se han realizado auditorías al sistema de gestión de seguridad de la información, ya que este no se encuentra implementado.	Se deben programar auditorías en un intervalo de tiempo con el fin de evaluar y verificar la conformidad y cumplimiento del Sistema de Gestión de Seguridad de la Información.
3	La entidad cuenta con programas de auditorías aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?	No cumple	Desde las Auditorías internas. Sistemas de autodiagnóstico. No se han realizado auditorías al sistema de gestión de seguridad de la información, ya que este no se encuentra implementado.	Se debe planificar, establecer, implementar y mantener uno o varios programas de auditoría donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes.
4	La alta dirección realiza revisiones periódicas al Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	El rector no a realizado revisiones periódicas al SGSI, desde planeación se lleva un seguimiento de gobierno el línea.	Se deben realizar revisiones a intervalos planificados del Sistema de Gestión de Seguridad de la Información.
5	En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre el desempeño de la seguridad de la información?	No cumple	No se han realizado retroalimentaciones ya que no se hace revisión por la dirección.	
6	Las revisiones realizadas por la Dirección al Sistema de Gestión de Seguridad de la Información, están debidamente documentadas?	Cumple parcialmente	La alta dirección no realiza revisiones, las actas con las que se cuenta son las generadas desde planeación con el seguimiento de gobierno en línea.	Se debe documentar las revisiones realizadas por la Alta Dirección con el fin de verificar el estado del sistema de seguridad de la información, cambios que se presenten a nivel interno o externo que puedan afectar la seguridad de la información y evaluación de las

ACTUAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
7	La entidad da respuesta a las no conformidades referentes a la seguridad de la información presentadas en los planes de auditoría?	No cumple	No se cuenta con no conformidades en cuanto a la seguridad de la información, las no conformidades que se presentan son las relacionadas con el proceso de TI.	Se deben tomar acciones para eliminar las causas de las no conformidades, para que no vuelvan a ocurrir.
8	La entidad ha implementado acciones a las no conformidades de seguridad de la información presentadas?	No cumple	En el momento de realizar auditorías se deben entregar procesos con la actividades correctivas. No se han realizado auditorías a la seguridad de la información, por lo tanto no se implementan acciones.	Toda la información de acciones realizadas al Sistema de Gestión de Seguridad de la Información debe ser documentada.
9	La entidad revisa la eficiencia de las acciones correctivas tomadas por la presencia de una no conformidad de seguridad de la información?	No cumple	En el momento de realizar auditorías se deben entregar procesos con la actividades correctivas. No se han realizado auditorías a la seguridad de la información, por lo tanto no se implementan acciones y no se revisa la eficacia.	Se debe evaluar la eficacia de las acciones correctivas con el fin de verificar que la no conformidad no se vuelva a presentar.
10	La entidad realiza cambios al Sistema de Gestión de Seguridad de la Información después de las acciones tomadas?	No cumple	Se realizan cambios según pertinencia y posible asignación de recursos. No se han realizado auditorías a la seguridad de la información, por lo tanto no se implementan acciones y no se generan cambios.	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.

11	La entidad documenta la información referente a las acciones correctivas que toma respecto a la seguridad de la información?	Cumple parcialmente	Toda acción correctiva se debe documentar mediantes los sistemas de gestión. No se han realizado auditorias a la seguridad de la información, por lo tanto no se implementan acciones y no se documentan.	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
12	La entidad realiza procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información?	[redacted]	Se realizan contrataciones con personal experto, así mismo se adquieren equipos con la infraestructura necesaria. No se cuenta con información documentada en cuento al Sistema de Seguridad de la Información	Toda la información de mejora al Sistema de Gestión de Seguridad de la Información debe ser documentada.

Fuente: NTC-ISO-IEC 27001:2013



	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	11.2%
LOGRO2	HACER	40%	29.3%
LOGRO3	VERIFICAR	15%	3.8%
	ACTUAR	15%	1.3%
	TOTAL	100%	45.5%

POR DOMINIO DE CONTROL						
NOMBRE DOMINIOS DE CONTROL	CONTROLES QUE APLICAN	PESO CONTROLES IMPLEMENTADOS Y PARCIALMENTE IMPLEMENTADOS	IMPLEMENTADOS	PARCIALMENTE	NO CUMPLE	NO APLICA
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	2	0.5	0	1	1	0
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	7	3.5	3	1	3	0
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	6	3	2	2	2	0
DOMINIO 8 - GESTIÓN DE ACTIVOS	10	7	6	2	2	0
DOMINIO 9 - CONTROL DE ACCESO	14	13	12	2	0	0
DOMINIO 10 - CRIPTOGRAFÍA	2	1	1	0	1	0
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	14	9	7	4	3	1
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	14	13.5	13	1	0	0
DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	6	4.5	3	3	0	1
DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	8	7.5	7	1	0	5
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	5	2.5	1	3	1	0
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	7	5.5	5	1	1	0
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	4	3.5	3	1	0	0
DOMINIO 18 - SEGURIDAD DE LAS COMUNICACIONES	8	4.5	3	3	2	0
	107		66	25	16	7

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA	FORMATO CRITERIOS DE AUDITORÍA CI-FR-022		
	Versión: 01	Fecha: 29-01-2016	Página 1 de 1

CRITERIOS
AUDITORÍA GESTIÓN DE TECNOLOGÍA E INFORMÁTICA

Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN
			SI	NO	N/A	
1	Se cuenta con el contexto interno y externo que afecten la capacidad de lograr resultado previstos en el sistema de gestión de la seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *4. contexto de la organización, 4.1 conocimiento de la organización y su contexto.*		x		
2	Se tiene determinado las partes interesadas para el sistema de gestión de seguridad de la información y los requisitos de las mismas.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *4. contexto de la organización, 4.2 comprensión de las necesidades y expectativas de la partes interesadas*	x			La caracterización interacción de los procesos.
3	Se tiene definido los limites y la aplicabilidad de los sistemas de gestión de la seguridad de la información para establecer su alcance,	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *4. contexto de la organización, 4.3 determinación del alcance del sistema de gestión de la seguridad de la información.*	x			La caracterización se encuentra el alcance del proceso.
	Si la respuesta anterior es afirmativa:					
	Se consideran cuestiones externas e internas (4.1)			x		No se cuenta con la identificación de las partes externas e internas. Igual al punto 1
	Requisitos del numeral 4.2		x			Se cuenta con la interacción de los procesos en cuanto a las partes interesadas y a los requisitos de estas (entradas y salidas) identificadas en la caracterización.
	Las interfaces y dependencias entre las actividades realizadas por la organización y las que realizan otras organizaciones		x			La caracterización interacción de los procesos internos y externos.
	El alcance esta disponible como información documentada.		x			En la caracterización del proceso se puede identificar el avance.
4	Se cuenta con la implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información de acuerdo a esta norma.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *4. contexto de la organización, 4.4 sistema de gestión de la seguridad de la información*	x			Se tiene plan de mantenimientos preventivos para la Infraestructura Tecnológica. Soporte 1. Se tiene Manual de creación de Backups. MANUAL PARA REALIZAR BACKUPS Y RECUPERACIÓN DE DESASTRES INFORMÁTICOS GT-MA-002
	Se tiene establecido la política de seguridad de la información y los objetivos de la seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la*	x	x		Se cuenta con las Políticas Socializadas a los líderes de proceso. Ver Soporte 2. La Política de Seguridad de la Información cuenta con Objetivos generales y específicos. Ver Soporte 2.

CRITERIOS AUDITORÍA GESTIÓN DE TECNOLOGÍA E INFORMÁTICA						
Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN
			SI	NO	N/A	
5	Se cuenta con recursos necesarios para el sistema de gestión de la seguridad de la información.	*Información.* *5. Liderazgo, 5.1 liderazgo y compromiso*	x			Se cuenta con Equipos y Dispositivos que permiten un correcto desempeño de las TIC como: dispositivo de seguridad perimetral, Software de seguridad perimetral, Equipos para Backups, Talento humano que desempeña labores sobre este esquema. Recursos financieros aprobados por vigencia para dar continuidad a los procesos de contratación.
6	Se cuenta con una política de seguridad de la información que sea:	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *5. Liderazgo, 5.2 política*	x			Ver Soporte 2.
	adecuada para la institución		x			
	incluya objetivos o el marco de referencia para el establecimiento de los objetivos de la seguridad de la información.		x			
	incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información		x			
	La política esta disponible como información documentada		x	x		Está Documentada más no socializada
	se comunica en la organización			x		
	esta disponible para las partes interesadas,			x		
7	Se tienen definidos las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información, se asignen y se comuniquen.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *5. Liderazgo, 5.3 roles, responsabilidades y autoridades en la organización*	x			Se tiene definido un Plan de trabajo al personal de apoyo de TI para labores de Seguridad Informática. Ejemplo. Ver Soporte 3.
8	Se han determinado los riesgos y oportunidades en cuanto a la seguridad de la información	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *6. Planificación, 6.1 acciones para tratar riesgos y oportunidades* *6.1.1 generalidades*	x			Se tiene definido Matriz de riesgos. Soporte 4.
9	Se valoran los rasgos de la seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *6. Planificación, 6.1 acciones para tratar riesgos y oportunidades* *6.1.2 valoración de los riesgos de la seguridad de la*	x			Se tiene definido Matriz de riesgos. Soporte 4.

CRITERIOS AUDITORÍA GESTIÓN DE TECNOLOGÍA E INFORMÁTICA						
Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN
			SI	NO	N/A	
	Se cuenta con información documentada acerca del proceso de valoración de los riesgos.	*seguridad de la información*	x			Se tiene definido Matriz de riesgos. Soporte 4.
10	Se define y aplica un proceso de tratamiento de riesgos de la seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *6. Planificación, 6.1 acciones para tratar riesgos y oportunidades*	x			Se tiene definido Matriz de riesgos. Soporte 4.
	Se cuenta con información documentada acerca del proceso de tratamiento de los riesgos de la seguridad de la información.	*6.1.3 tratamiento de los riegos de la seguridad de la información*	x			Se tiene definido Matriz de riesgos. Soporte 4.
11	Se tienen establecidos los objetivos de seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *6. Planificación, 6.2 objetivos de seguridad de la información y planes para lograrlos*	x			Se tiene definido una política con objetivos. Soporte 2.
	Se cuenta con información documentada sobre los objetivos de la seguridad de la información		x	x		Está Documentada más no socializada.
12	Se determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora del sistema de seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *7. Soportes, 7.1 Recursos*	x			Se cuenta con Equipos y Dispositivos que permiten un correcto desempeño de las TIC como: dispositivo de seguridad perimetral, Software de seguridad perimetral, Equipos para Backups, Talento humano que desempeña labores sobre este esquema. Recursos financieros aprobados por vigencia para dar continuidad a los procesos de contratación.
13	Se determina las competencias necesarias de las personas que realizan un trabajo que afecte la seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *7. Soportes, 7.2 competencia*	x			Se tiene definido un Plan de trabajo al personal de apoyo de TI para labores de Seguridad Informática. Ejemplo. Ver Soporte 3.
	Se cuenta con información documentada apropiada como evidencia de la competencia.		x			Se encuentran los soportes e idoneidad de las personas que participan del proceso.
14	Se determinan las necesidades de comunicación internas y externas pertinentes al sistema de gestión de la seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *7. Soportes, 7.4 Comunicación*	x			Se tiene definida en la interacción del proceso en la Caracterización del proceso en las entradas y salidas.
15	Se cuenta con la información documentada de esta norma	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *7. Soportes, 7.5 Información documentada, 7.5.1 generalidades*	X	X		Se cuenta con la herramienta de autodiagnóstico de la 27001:2013, la cual llega a un porcentaje de implementación o avance de 63.8 sobre los requisitos a cumplir.

CRITERIOS AUDITORÍA GESTIÓN DE TECNOLOGÍA E INFORMÁTICA						
Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN
			SI	NO	N/A	
16	La información cuando se crea o actualiza se asegura de:	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *7. Soportes, 7.5 Información documentada. 7.5.2 creación y actualización*				Se tiene procedimientos y formatos definidos en el Sistema de Calidad Isolucion para los diferentes procesos que realiza TI.
	La identificación y descripción		x			
	El formato		x			
	la revisión y aprobación		x			
17	Se controla la información documentada	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *7. Soportes, 7.5 Información documentada. 7.5.3 control de la información documentada*	x			
18	Se planifica, implementa y controla los procesos necesarios para cumplir con los requisitos de seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *8. Operación, 8.1 Planificación y control operacional*	x			Se tiene documentado procesos en donde se planifica la adquisición de Sistema de Seguridad y su implementación y control a través de reportes y estadísticas.
19	Se lleva a cabo la valoración de los riesgos de la seguridad de la información a intervalos planificados (6.1.2)	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *8. Operación, 8.2 valoración de riesgos de la seguridad de la información*	x			Se tiene definido Matriz de riesgos. Soporte 4.
	Se cuenta con información documentada de los resultados del tratamiento de los riesgos de seguridad de la información		x			Se tiene definido Matriz de riesgos. Soporte 4.
20	Se hace seguimiento a la evaluación al desempeño de la información y la eficacia del sistema de gestión de la seguridad de la información	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *9. Evaluación del desempeño, 9.1 Seguimiento, medición, análisis y evaluación*	x	x		Se puede observar en la Pagina Web de la Institución la evaluación del proceso de TI, Seguridad de la Información. Además de esto no se observa el seguimiento a la evaluación del desempeño.
	Se cuenta con información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.		x			Se puede observar en la Pagina Web de la Institución la evaluación del proceso de TI, Seguridad de la Información
21	Se lleva a cabo una auditoria interna a intervalo planificado para proporcionar la información acerca del sistema de gestión de la seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *9. Evaluación del desempeño, 9.2 auditoria interna*	x			Para esta vigencia la auditoria se realizará para el 21 de Septiembre de 2017.

CRITERIOS AUDITORÍA GESTIÓN DE TECNOLOGÍA E INFORMÁTICA						
Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN
			SI	NO	N/A	
22	La alta dirección revisa el sistema de gestión de la seguridad de la información de la organización a intervalos planificados para asegurarse de su conveniencia, adecuación y eficiencia continua.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *9. Evaluación del desempeño, 9.3 revisión por la dirección*		x		La alta Dirección no realiza la revisión del Sistema de Seguridad de la Información. La Realiza Planeación por medio del Informe de Autoevaluación y Control Interno por medio de Auditorias
	Se cuenta con información documentada como evidencia de los resultados de las revisiones por la alta dirección		x			Informe Autoevaluación por procesos.
23	Cuando ocurre una no conformidad se toman acciones para controlar y corregirla	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *10. Mejora, 10.1 no conformidades y acciones correctivas*	x			Se registra las acciones en el Sistema de Calidad Isolucion
	Se evalúa la necesidad de la acción para eliminar las causas		x			Se evalúa en el Sistema de Gestión de Calidad.
	Se cuenta con información documentada adecuada como evidencia de las no conformidades y las acciones tomadas y los resultados de las acciones correctivas.		x			En las auditorias internas y externas por los diferentes Entes que la realizan.
24	Se mejora continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información.	*NTC-ISO-IEC-27001:2013 Tecnología de la Información.* *10. Mejora, 10.2 mejora continua*	x			Se actualizan según la necesidad mediante formatos, procedimientos, Instructivos, Flash Informativos.
25	Evidenciar la elaboración de los proyectos pertinentes al proceso de la vigencia 2017.	*CARACTERIZACIÓN DEL PROCESO*	x			Se cuenta con un Plan de Necesidades y asignación de recursos. Ver Soporte 5.
26	Observar el registro de mantenimientos de hardware y software		x	x		Se observó la programación y ejecución del mantenimiento preventivo de los equipos de cómputo de la facultad de Ciencias Sociales, la cual se realizó en el mes de Junio pero no se encuentra actualizada en el formato de Cronograma de mantenimientos. Se evidencia el registro de los mantenimientos con el acta y firma del líder de proceso. ver soporte 6
27	se tiene soporte de las asesorías en la adquisición de TIC.		x			Se evidencia solicitud de Liliana Bienestar. Ver Soporte 7.
28	Donde se guardan los backups institucionales.		x			Se evidencia resguardo de los backups por medio de los formatos establecidos. Proveedor Iron Mountain. Se verifica el backup 11 septiembre.
29	Evidenciar el seguimiento a la ejecución de los proyectos y los programas de mantenimiento		x	x		Se observó la programación y ejecución del mantenimiento preventivo de los equipos de cómputo de la facultad de Ciencias Sociales, la cual se realizó en el mes de Junio pero no se encuentra actualizada en el formato de Cronograma de mantenimientos. Se evidencia el registro de los mantenimientos con el acta y firma del líder de proceso.
30	Evidenciar la evaluación de la satisfacción al usuario y al soporte técnico brindado.		x			Mediante el sistema de Calidad se evidencia Indicador de satisfacción del usuario. GT-FI-04_ SATISFACCION DEL USUARIO
31	evidenciar la ejecución de los backups		x			Se evidencia resguardo de los backups por medio de los formatos establecidos. Proveedor Iron Mountain. Se verifica el backup 11 septiembre.

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA	FORMATO CRITERIOS DE AUDITORÍA		
	Versión: 01	Fecha: 29-01-2016	Página 1 de 1

CRITERIOS
AUDITORÍA: GESTIÓN DE TECNOLOGÍA E INFORMÁTICA

Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN	
			SI	NO	N/A		
32	Verificar el manejo de los recursos asignados para la vigencia 2017-1 de acuerdo a la normatividad vigente.		X			Se observan el contrato de: _suministro de minima cuantia - MC017-17 , cumple con los requisitos y obligaciones, además se cuenta con el compromiso 1487 por $17.911.500 y el siguiente movimiento: _ OP 1861 del 29 de marzo y CE 1995 por $ 660.389. _ OP 4094 del 26 de mayo y CE 4245 por $ 1.249.500. _ OP 7232 del 8 de agosto y CE 7772 por $7.721.910 Quedando un saldo por cancelar de $8.279.701	Solicitar el total ejecutado en la vigencia 2017-1 relacionando el numero de los contratos.
33	Verificar los bienes devolutivos y de consumo que tiene asignado el líder del proceso en la vigencia 2016.	Inventario devolutivo y de consumo, suministrado por bienes y servicios de la institución. Acuerdo n° 009 del 29 de septiembre de 2014.			X	Para esta auditoria no se evidenciará el inventario devolutivo y de consumo.	

CRITERIOS
AUDITORÍA: GESTIÓN DE TECNOLOGÍA E INFORMÁTICA

Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN
			SI	NO	N/A	
34	Realizar seguimiento a los indicadores del proceso auditado.	*Isolucion modulo de indicadores*	X			Se observan tres indicadores de efectividad/resultado y tres de eficacioa/producto, los cuales se describen a continuación.
EFECTIVIDAD - RESULTADOS						
	GR-FI-02 Computadores por docente.	*Isolucion modulo de indicadores*	**X**			Frecuencia de medición: semestral, realizada el 30 de Junio de 2017, con una meta del 1 y un resultado de 1.05 correspondiente a una medición mayor o igual que la tolerancia superior, no se visualiza soporte (anexos) socializados en ISOLUCION (verde).
	GR-FI-04 Satisfacción del usuario.		**X**			Frecuencia de medición: semestral, realizada el 30 de Junio de 2017, con una meta de 90 y un resultado de 95.85, correspondiente a una medición mayor o igual que la tolerancia superior, no se visualiza soporte (anexos) socializados en ISOLUCION (verde).
	GR-FI-08 Conexiónes de red por docente.		**X**			Frecuencia de medición: semestral, realizada el 30 de Junio de 2017, con una meta de 2 y un resultado de 4.79, correspondiente a una medición mayor o igual que la tolerancia superior, no se visualiza soporte (anexos) socializados en ISOLUCION (verde).

EFICACIA - PRODUCTO						
	GR-FI-03 Conexiones de red por estudiante.	*Isolucion modulo de indicadores*	X			Frecuencia de medición: semestral, realizada el 30 de Junio de 2017, con una meta de 1 y un resultado de 1.42, correspondiente a una medición mayor o igual que la tolerancia superior, no se visualiza soporte (anexos) socializados en ISOLUCION (verde).
	GR-FI-05 tiempo de atención a requerimientos.		X			Frecuencia de medición: semestral, realizada el 30 de Junio de 2017, con una meta de 85 y un resultado de 97, correspondiente a una medición mayor o igual que la tolerancia superior, no se visualiza soporte (anexos) socializados en ISOLUCION (verde).
	GR-FI-09 estudiantes por computador.		X			Frecuencia de medición: semestral, realizada el 15 de Agosto de 2017, con una meta de 5 y un resultado de 5.1, correspondiente a una medición mayor o igual que la tolerancia superior, no se visualiza soporte (anexos) socializados en ISOLUCION (verde).
35	Realizar seguimiento a los riesgos del proceso auditado.	*Matriz de riesgos publicada en la web*	X			Se observo en la matriz de riesgos de gestion publicada en la pagina web de la institución en el link de planeación, estos son: _ Posibilidad de no acceso a la plataforma tecnologica institucional. _ Posibilidad de perdida de infomación. _ Vulnerabilidad de plataforma tecnologica. _posibilidad de no actualización e integración de lsos sistemas informaticos y desarrollos tecnologico en la institución. Riesgos de corrupción: _ manipulación inapropiada de la plataforma tecnologica en beneficio propio o particular.

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA	FORMATO CRITERIOS DE AUDITORÍA		
	Versión: 01	Fecha: 29-01-2016	Página 1 de 1

CRITERIOS
AUDITORÍA: GESTIÓN DE TECNOLOGÍA E INFORMÁTICA

Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN
			SI	NO	N/A	
36	Verificar que actividades desarrolla el proceso en el cumplimientos de los principios MECI (autocontrol, autorregulación, autogestión).	*Decreto 943 de 2014, MECI, Departamento Administrativo de la Función Pública, Páginas 10-11.*				
	AUTOCONTROL: Capacidad que debe desarrollar todos y cada uno de los servidores públicos de la organización para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para el adecuado cumplimiento de los resultados.		x			_ Evaluación Trabajo, se realizan comités técnicos. _ Correctivos, se realizan procesos correctivos ante una situación de prevención. _ Se realizan Comités de Técnicos. _ Se realizan mejoras al proceso cuando se requieren cambios en las plataformas.
	AUTORREGULACION: Capacidad de cada una de las organizaciones para desarrollar y aplicar en su interior métodos, normas y procedimientos que permitan el desarrollo, implementación y fortalecimiento continuo del Sistema de Control Interno, concordante con la normatividad vigente.		X			_ Sensibilización Valores Institucionales _ Sensibilización Códigos Buen gobierno _ Políticas de TI
	AUTOGESTION: Capacidad de toda organización publica para interpretar, coordinar, aplicar y evaluar de manera efectiva, eficiente y eficaz de la función administrativa que le ha sido asignada por la constitución, la ley y sus reglamentos.		X			_Plan de Riesgos _Competencias Laborales, Planes de trabajo personal. _Supervisión, Plan de necesidades anuales
	Autoevaluación de Tecnologia e Informatica, (valoración de los propios conocimientos y aptitudes en cuanto al laboratorio de salud).					_ Se realiza encuestas de satisfacción de usuarios, mediante el sistema de Mesa de Ayuda. _ Se realiza proceso de autoevaluación mediante las plataformas y aplicaciones (Naonquest) las cuales nos permiten obtener resultados de la Gestión interna a nivel técnico y operativo.

37	El Líder de TI, realiza un monitoreo a las operaciones que realiza. Se tiene en cuenta los indicadores del proceso y el manejo de los riesgos y a los planes de mejoramiento entre otros.	***Decreto 943 de 2014, MECI, Departamento Administrativo de la Función Pública, Páginas 72-77.***	X			

Autoevaluación: mecanismo de verificación y evaluación que permite medirse a si mismo al proveer la información necesaria para establecer si esta funciona efectivamente o si existen desviaciones en su operación que afecten el objetivo para la cual esta creada.
control: es todo aquello que apoya a las personas en sus esfuerzos para alcanzar los objetivos de la organización: habilidades, procesos, información, sistemas, políticas, trabajo en equipo, liderazgo, recursos. Estructura, comunicación y procedimientos.

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA	FORMATO CRITERIOS DE AUDITORÍA		
	Versión: 01	Fecha: 29-01-2016	Página 1 de 1

CRITERIOS
AUDITORÍA: GESTIÓN DE TECNOLOGÍA E INFORMÁTICA

Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN
			SI	NO	N/A	
38	Verificar que las versiones vigentes y pertinentes de los documentos aplicables se encuentren disponibles en los puntos de uso.	*4.2.3 (d), Gestión documental. Norma NTCGP 1000:2009*	X			Se verifico que este proceso tuviera documentado en el sistema de calidad ISOLUCION documentación como: caracterización e instructivos, formatos y manuales etc.
39	Verificar si la acciones correctivas se encuentra cerradas en el sistema de calidad ISOLUCION.	*Informe de seguimiento al Sistema de Gestión de la Calidad*	X			Se observa en el informe de auditoría interna del sistema de gestión integrado (GM-FR-04) vigencia 2016, que para el proceso de Gestión de Tecnología e Informatica se registran una (1) observacion. La observacion es: 1. En la caracterización del proceos GT CA-001, version 6 se hace referencia al Plan Estartegico de TIC, PETL, el cual se encientran en procerso de construcción. No se deberia referenciar alli hasta qu no este aprobado. Requisito NTCGP1000: ISO9001 NUMERAL 5.4 La observacion con registro en ISOLUCION 222, tienen fecha proyectada de cierre 16 de diciembre de 2016. Esta acción fue cerrada por la profesional de calidad el 21 de diciembre de 2016, lo que evidencia que no se cumplio con la fecha estipulada.

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA	FORMATO CRITERIOS DE AUDITORÍA		
	Versión: 01	Fecha: 29-01-2016	Página 1 de 1

CRITERIOS
AUDITORÍA: GESTIÓN DE TECNOLOGÍA E INFORMÁTICA

Nº	CRITERIO	CITA NORMATIVA	CUMPLE			OBSERVACIÓN
			SI	NO	N/A	
40	Verificar en que línea del plan de desarrollo se encuentra el proceso de Gestión de Tecnologia e informarica (realizar los criterios del tema y los indicadores)	*Plan de Desarrollo 2016-2020, IUCMA Páginas 88 a la 89.*	X			El proceso de Gestión de Tecnologia e Informatica en el Plan de Desarrollo 2016 – 2020 se encuentra en el Eje temático N° 6: Gestión Administrativa y Financiera, Componente 4: Infreaestructura para el mejoramiento academico y el bienestar institucional, programa de necesidades fisicas y tecnologicas para la enseñanza y el bienetar institucional y Plataformas y sistemas de informacioón instiicioanels integradas.
Programa: Necesidades físicas y tecnológicas para la enseñanza y para el aprendizaje, atendidas, indicadores de producto pág. 88						
	Herramientas tecnologicas para la enseñanza incorporadas al desarrollo academico	*Plan de Desarrollo 2016-2020, IUCMA Página 88*	X			En el seguimiento a este indicador se observa en el plan indicativo con una meta del 90% del 2016 al 2019, la cual para el seguimiento al 2017 el indicador se encuentra en un 11% indicando que la actualización de los equipos correspondientes a 234 pc.
Programa: plataformas y sistemas de información institucional, integradas pág. 89, indicadores de producto						
	Sistemas de información integrados (financiero y academico)	*Plan de Desarrollo 2016-2020, IUCMA Página 89*	X			En el seguimiento a este indicador se observa en el plan indicativo una meta de 2 del 2016 al 2019, la cual para el seguimiento al 2017, se encuentra en un 0.5% indicando que se contrató la integración con el sistema financiero y académico en el 2017-2

NOMBRE AUDITOR:	**FIRMA:** Manuel Gabriela Rueda
NOMBRE LÍDER DEL PROCESO AUDITADO:	**FIRMA:**
NOMBRE DEL DIRECTOR OPERATIVO DE CONTROL INTERNO:	**FIRMA: Edith Yohana Palacio Espinosa**