INFORME DE AUDITORÍA INTERNA
DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
ISO/IEC 27001:2013

EMPRESA AUDITADA:
INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DEL CAUCA

AUDITOR LIDER: MSC. KATERINE MÁRCELES VILLALBA

AUDITORES DE APOYO: FABIÁN HURTADO MOSQUERA

OBJETIVO DE LA AUDITORIA: Evaluar el cumplimiento de los controles del estándar ISO/IEC 27001:2013 gestionados desde el área Tic de la Institución Colegio Mayor del Cauca

ALCANCE: Validar el estado actual de cada unos de los dominios que contempla el estándar ISO/IEC 27001:2013 implementados desde el área Tic para la gestión de la seguridad en los procesos misionales de la Institución Colegio Mayor del Cauca

FECHA DE LA AUDITORÍA: Agosto 2 al 5 de 2022
Agosto 23 al 24 de 2022

NÚMERO DE HOJAS DEL INFORME: 41

Tabla de contenido

Dominio 5. Política de la Seguridad de la Información 4

Dominio 6. Organización de la seguridad de la información 5

Dominio 7: Seguridad ligada a los recursos humanos.....7

Dominio 8. Gestión de activos.....9

Dominio 9. Control de acceso 11

Dominio 10. Criptografía.....14

Dominio 11. Seguridad Física y del entorno.....15

Dominio 12. Procedimiento Operacionales y Responsabilidades.....18

Dominio 13. Gestión de la seguridad en las redes.....22

Dominio 14. Requisitos de seguridad de los sistemas de información.....24

Dominio 15. Seguridad de la información con los proveedores.....26

Dominio 16. Gestión de incidentes y mejoras en la seguridad de la información 27

Dominio 17. Continuidad de seguridad de la información 28

Dominio 18. Cumplimiento.....29

Documentación básica del modelo de privacidad de la seguridad de la información - MSPI.....31

Análisis porcentual de cumplimiento de los dominios 33

Referencias 41

Listado de Figuras

Figura 1. Seguridad en el cableado 17
Figura 2. Documentación básica del MSPI 32
Figura 3. Cumplimiento del dominio 5 33
Figura 4. Cumplimiento dominio 6 33
Figura 5. Cumplimiento dominio 7 34
Figura 6. Cumplimiento dominio 8 34
Figura 7. Cumplimiento dominio 9 35
Figura 8. Cumplimiento dominio 10 35
Figura 9. Cumplimiento dominio 11 36
Figura 10. Cumplimiento dominio 12 36
Figura 11. Cumplimiento dominio 13 37
Figura 12. Cumplimiento dominio 14 37
Figura 13. Cumplimiento dominio 15 38
Figura 14. Cumplimiento dominio 16 38
Figura 15. Cumplimiento dominio 17 39
Figura 16. Cumplimiento dominio 18 40
Figura 17. Porcentaje de Cumplimiento general de los Dominios 41

Dominio 5. Política de la Seguridad de la Información

Conformidades:

5.1.1 – 5.1.2 La Institución Universitaria Colegio Mayor del Cauca, cuenta con una política de seguridad de la información, el cual ha sido aprobada y socializada a la comunidad académica y administrativa, esto se puede evidenciar a través de los registros de asistencia de las charlas y/o encuentros realizados por parte de la persona encargada de la Seguridad digital desde el área de TIC.

No Conformidades: Ninguna

Observaciones:
Se sugiere desarrollar estrategias de socialización de manera lúdica para llegar a interiorizar e impactar un poco más la política del Sistema de Gestión de Seguridad de la Información a los estudiantes y docentes, dado que una vez por semestre la política es socializada solo a estudiantes de primer semestre.

Dominio 6. Organización de la seguridad de la información

Conformidades:

6.1.1. – 6.1.2 Se tiene un documento donde se evidencia que se encuentran definidas los roles y responsabilidades en cuanto a la seguridad de la información donde se especifican claramente las responsabilidades en cuanto al tratamiento y seguridad que se le debe dar a los activos de información, dependiendo al perfil que desempeñan (última actualización 2 de Diciembre 2019). Así mismo, se cuenta con un responsable de seguridad digital, quien tiene como función mantener el modelo de seguridad y privacidad de la información.

6.1.3 – 6.1.4 La Institución Universitaria Colegio Mayor del Cauca, tiene un procedimiento establecido a través del documento Gestión de incidentes de Seguridad y privacidad de la Información y reporte de incidentes, donde se establece la trazabilidad del mismo para tomar las acciones necesarias en cuanto a qué organismo, comunidad o autoridad contactar en caso que se requiera.

6.1.5 En lo que respecta a la seguridad de la información en la gestión de proyectos se contempla dentro de las cláusula de las resoluciones contractuales y en los lineamientos internos para dar un tratamiento seguro de la información dentro de los proyectos que se desarrollan tanto en lo académico y administrativo. Destacando que todo proyecto que se gestiona se le evalúa la viabilidad y el componente de seguridad.

6.2.1 La Institución Universitaria Colegio Mayor del Cauca, tiene una política y medidas de seguridad de soporte para los riesgos introducidos por el uso de dispositivos móviles de uso Institucional.

6.2.2 Si existe una política acerca del teletrabajo, el cual se encuentra vigente y se implementó durante la pandemia, además de una solución lógica por medio de una Red privada virtual (VPN) haciendo uso del firewall implementado para brindar seguridad perimetral a los usuarios que requerían acceder a la información de la institución.

No Conformidades: Ninguna

Observaciones:

6.1.1 – 6.1.2 A pesar de que fueron incluidas cláusulas para el aseguramiento de la información para los empleados y contratistas dentro de su proceso contractual, se hace necesario anexar el tiempo para mantener la confidencialidad y especificar la no transferencia de la información durante y luego de finalizar su periodo de contratación.

6.1.3 Dado que se cuenta con un formato de gestión de incidentes se hace necesario incluir un control de cambios a éste tanto a la hoja de reporte como a la de gestión, de esa manera se podrá tener la trazabilidad de los ajustes y/o actualización del mismo.

6.2.1 Se recomienda revisar, actualizar la política abarcando el aseguramiento de los dispositivos móviles tipo BYOD, dado que podrían colocar en riesgo el aseguramiento de la red interna de la institución y publicar en lugar visible (sitio web) la política relacionada con dispositivos móviles

6.2.1 – 6.2.2 A pesar de contar con política de dispositivos móviles y teletrabajo, éstas no se encuentran totalmente socializadas a la comunidad, por ello se sugiere colocarlas en lugares visibles como por ejemplo en la página web.

Dominio 7: Seguridad ligada a los recursos humanos

Conformidades:

7.1.1 Antes de realizar una contratación se verifican los antecedentes de todos los candidatos mediante la verificación de los antecedentes judiciales, contraloría, procuraduría por parte del área de talento humano.

7.2.2. Se le brinda a los empleados y contratista otros espacios diferentes a la de socialización de políticas y procedimientos con el fin de apropiarse de la importancia del manejo seguro de la información.

No conformidades:

7.1.2. No en todas las resoluciones de contratación se contempla un lineamiento o acuerdo de confidencialidad y/o no divulgación sobre la información, como también la de protección por propiedad intelectual, dado a esto se revisaron varios contratos entre ellos: DR 101-2022, DR 069-2022, PSMC-017-2022, resolución de nombramiento de un cargo profesional y un docente ocasional código 783-2022.

7.2.1. Tanto al personal de planta, ocasional y contratista se les informa mediante la resolución de contratación su rol y/o responsabilidades generales, más no se le especifican claramente lo relacionado con la seguridad de la información antes de otorgarle cualquier tipo de información con su quehacer.

7.2.3. A pesar de que se tiene solamente el procedimiento de actas de entrega de Paz y Salvo para el personal de planta, no se tiene un procedimiento claro para los docentes en modalidad ocasional, ya que éstos no realizan ninguna entrega formal. En cuanto a los contratistas el encargado de realizar seguimiento es el respectivo supervisor. Además no se cuenta con un proceso formal establecido en caso de emprender algún proceso disciplinario.

7.3.1. Luego de una terminación o contratación del empleo solamente se le realiza una desactivación del sistema a los docentes de planta y se le es informado

al área Tic para la realización de éste proceso; sin embargo, no se cuenta con un procedimiento formal para docentes ocasionales, contratistas y personal administrativo que permita el poder llevar a cabo un proceso disciplinario en caso de incumplir algún lineamiento cláusula, dado a que no se contempla ninguna dentro de las resoluciones de contratación.

Observaciones:

7.1.2. En todas las resoluciones de contratación se debe contemplar un lineamiento o acuerdo de confidencialidad y/o no divulgación sobre la información. En virtud de lo anterior, ese lineamiento debe aplicar durante y luego de terminar la contratación quedar vigente por al menos los tres años siguientes.

7.2.1. Tanto al personal de planta, ocasional y contratista se le debe informar mediante la resolución de contratación su rol y/o responsabilidades generales con la seguridad de la información antes de otorgarle cualquier tipo de información.

7.2.2. Se debe propiciar otros espacios diferentes a la de socialización de políticas y procedimientos que le permita tanto a los docentes, estudiantes, administrativos y terceros apropiarse de la importancia del manejo seguro de la información. Además se debe guardar las evidencias de cada uno de estos procesos de sensibilización para posteriormente evaluar el impacto de la misma.

7.2.3. Generar un procedimiento claro para los docentes en modalidad ocasional, ya que éstos no realizan ninguna entrega formal de la información que manejan. En cuanto a los contratistas el encargado de realizar seguimiento es el respectivo supervisor, por lo que debe garantizar a través de un oficio la entrega formal de la información que éste debió generar.

7.3.1. Luego de una terminación o contratación del empleo no solamente se le debe realizar la desactivación del sistema a los docentes de planta sino a su vez al docente ocasional, por lo anterior urge determinar un procedimiento que evidencie la trazabilidad desde el inicio de la contratación hasta la finalización del mismo tanto para docentes ocasionales, contratistas y personal administrativo, el cual se carece de éste.

Dominio 8. Gestión de activos

Conformidades:

8.1.1. – 8.1.2 Se cuenta con un inventario de activos asociados con la información, propietario e ubicación de los mismos a través de la herramienta GLPI. Por otra parte, se cuenta con la herramienta de reporte que contiene el antiguo SIAG quien recibe el insumo de lo almacenado en el GLPI, el cual realiza la trazabilidad de los dispositivos e incidencias.

8.1.3 Se tiene documentado el uso aceptable de los activos de información mediante las directrices y lineamientos establecidos en la política de seguridad de la información.

8.2.1 – 8.2.2 Por el carácter público de la Institución, toda la información que se maneja al interior debe ser pública; sin embargo se cuenta con un formato llamado índice de información clasificada y reservada emitido el 9/08/2019, donde se especifican y se etiquetan las categorizaciones de los documentos.

8.2.3 Se cuenta documentado a través de a Ley de transparencia y del derecho de acceso a la información pública emanada a la ley 1712 de 2014, el cual establece los lineamientos de clasificación de la información que sigue la Institución.

No conformidades:

8.1.4 A pesar de que existe un formato de entrega de activos alineados a un Paz un Salvo, éste es solo para los docentes de planta más no para personal contratista y docentes ocasionales, lo cual podría estarce abriendo una brecha de seguridad en cuanto a los activos de información.

8.3.1 No existe un procedimiento para la gestión de medios removibles, solo se conoce que si se desea remover o desplazar un activo ya sea fuera de la institución se debe comunicar a la Secretaría General quien autoriza o No su traslado ó si el proceso es interno autoriza el área de Tic. Además, se identificó que actualmente se esta utilizando un formato de orden de entrada y salida de activos.

8.3.2 – 8.3.3 Cuando se requiere trasladar algún dispositivo físico, éstos deberán estar asegurados en virtud de lo anterior, la Institución cuenta con una póliza para los equipos por parte de la Previsora y cuando los equipos son trasladados internacionalmente se protegen con pólizas de aseguramiento; no obstante, no se tiene un procedimiento documentado relacionado con gestión de medios removibles que permita dar claridad en cuanto a las medidas para la protección de la información que manejan éstos. Es importante, mencionar que los equipos cuentan con las medidas de seguridad lógica para salvaguardar la información en caso de algún incidente a través del almacenamiento de la información en el Drive institucional.

Observaciones:

8.1.1. Se sugiere revisar de manera periódica el inventario de activos para mantener éste actualizado y asociar el propietario de cada activo de información, dado que al momento de la auditoría no todos los tenían asociado.

8.1.4 Generar algún tipo de formato o sistema que permita generar un Paz un Salvo, al terminar la contratación para aquellos docentes ocasionales que manejen algún tipo de proceso al interior de los programas, a los administrativos y a los terceros, de esta forma quedará evidencia de la entrega de los activos que cada uno de ellos tenía o tiene a su cargo al finalizar el contrato y a su vez se encuentre enmarcado dentro del procedimiento de seguridad de la información de contrataciones.

8.2.1 A pesar de que existe un documento donde se especifica la clasificación de los activos de información, la gran mayoría desconoce de éste, por lo que se sugiere establecer estrategias de socialización y que sea revisada de manera periódica con el fin de mantenerla actualizada si se requiere.

8.3.1 – 8.3.2 – 8.3.3 El formato de Orden de entrada y salida elementos tecnológicos, no cuenta con un control de cambios, por lo que se recomienda implementarlo para evidenciar la trazabilidad de los cambios que pueda tener éste y hacer un procedimiento para la gestión de medios.

Dominio 9. Control de acceso

Conformidades:

9.1.1 La Institución Universitaria Colegio Mayor del Cauca, tiene documentada y socializada la política de Control de Acceso, el cual se tienen como evidencia los registros de asistencia.

9.2.4 – 9.4.2 Se cuenta con un sistema de doble autenticación frente a la plataforma de Campus universitario, que permite identificar la identidad del usuario que realmente se encuentra ingresando al sistema, a través del envío de un código al correo electrónico.

9.2.5 Solamente a nivel de Campus, se realiza una revisión periódica de los derechos de acceso lógicos asignados y se validan los usuarios activos en la consola de administración del correo institucional.

9.2.6 Al terminar el contrato o acuerdo laboral entre el empleado y la Institución son retirados los derechos de acceso tanto del correo electrónico como a las plataformas que tienen acceso; cabe anotar, que éste proceso surge a cabalidad en los administrativos y docentes de planta. A partir de la realimentación de las facultades.

9.4.1 Es importante destacar que el acceso a la información mediante los accesos lógicos son controlados de acuerdo a la política de control de acceso y roles del usuario.

9.4.3 Se cuenta con un sistema interactivo para la gestión y seguridad en las contraseñas desde la plataforma del Campus como es el algoritmo SHA512 para cifrar las contraseñas.

9.4.4 Existe una restricción en cuanto al uso de programas utilitarios, el cual solamente podrá instalarse con previa autorización por parte del área Tic, de lo contrario no se está permitido, dado que el sistema solicita el ingreso de la contraseña de administrador, en los equipos del área Tic se encuentra haciendo un plan piloto en cuanto a la implementación de un Directorio activo con la política de restricción de instalaciones con el fin de desplegarlo posteriormente al área administrativa y luego sala de computo.

9.4.5 Se restringe y se tiene control acerca del acceso a los códigos fuente de los programas, el cual la Institución desarrolla y los que tiene con algún tercero.

No conformidades:

9.1.2 A pesar de que existe una política de control de acceso, no se tiene un control para identificar y permitir el acceso a las redes y servicios de red dentro de la Institución solo al personal autorizado, dado que las contraseñas de acceso a wifi de estudiante es pública y hasta algunos estudiantes tienen conocimiento de las contraseñas de las redes de servicios de wifi de docentes y administrativos también.

9.2.1 – 9.2.2 No existe un procedimiento formal de registro y de cancelación de usuarios documentado para la asignación de derechos de acceso a los sistemas lógicos con que cuenta la Institución, lo que deja abierta una brecha de seguridad, dado que en ocasiones desde el área de Tic no tienen forma de verificar la veracidad de la información.

9.2.3 – 9.3.1 La Institución Universitaria Colegio Mayor del Cauca, carece de un procedimiento formal para la entrega de los accesos de usuario y contraseña frente a toda la comunidad en general, dado que no se les indica la importancia de garantizar la confidencialidad de éstas.

Observaciones:

9.1.1 Se le sugiere actualizar de manera periódica la política, dado que la última revisión fue el 2 de diciembre del 2019.

9.1.2 Sería importante tener un mejor control en cuanto a la conexión del servicio de internet, donde se permitiera el acceso a éste solo aquellos estudiantes que estuvieran activos, asignándoles una cuenta de usuario, esto garantizaría un mejor aprovechamiento del ancho de banda y seguridad en la redes. Se sugiere revisar la herramienta openNAC y Packetfence.

9.2.6 – 9.2.1 – 9.2.2 Al tener un procedimiento formal de desvinculación de un docente ocasional, administrativo y/o tercero se evidenciará la trazabilidad de desactivación del acceso tanto del correo electrónico como a las plataformas que tienen acceso.

9.2.3 – 9.3.1 Implementación de un proceso formal a través de un oficio o mensaje emergente emitido a través de las plataformas u otro sistema que consideren adecuado para la entrega de los accesos de usuario y contraseña de toda la comunidad en general, donde se les especifique la importancia de garantizar la confidencialidad de éstas.

Dominio 10. Criptografía

Conformidades:

10.1.1 La Institución Universitaria Colegio Mayor del Cauca tiene una política emitida el 10 de septiembre de 2019, que garantiza la implementación en cuanto al uso de controles criptográficos para salvaguardar la información.

10.1.2 Se realiza una buena gestión en cuanto a la protección y tiempo de vida de las llaves criptográficas durante su ciclo de vida, mediante una herramienta llamada Keepass.

No Conformidades: Ninguna

Observaciones:

10.1.1 Se sugiere socializar a la comunidad al menos a través de la página web la política criptográfica.

Dominio 11. Seguridad Física y del entorno

Conformidades:

11.1.1 En cuanto al perímetro de seguridad física de las instalaciones de la Institución Universitaria Colegio Mayor del Cauca, se resalta que cada uno de los pasillos se encuentran vigilados y monitoreados a través de un circuito cerrado de televisión y cada una de las oficinas y/o recintos de información cuentan con puertas y ventanas aseguradas, lo que minimiza el riesgo a cualquier robo físico de los activos de información. Es importante mencionar que a partir del año 2020 se actualizó el sitema de cámaras por unas con mayor resolución centralizadas con un sistema de NVR de grabación, el cual se tiene acceso de forma remota y en cada sede se tienen medios de almacenamiento. Actualmente los sensores del sistema de alarma son vía celular.

11.1.4 Se cuenta con una infraestructura adecuada frente amenazas externas y ambientales como por ejemplo: un detector de humo, sistema de refrigeración adecuada al igual que la iluminación, se tienen extinguidores vigentes y de tipo clase C. En gestión documental se hizo un cambio con el fin de minimizar el riesgo de humedad. En el Centro de procesamiento de datos (CPD) ubicado en Bicentenario se realizó una plancha con el fin de aislar la humedad, en el CPD ubicado en la sede de encarnación se mejoró el sistema de refrigeración y acceso.

11.1.5 Existen lineamientos de seguridad que permiten garantizar el trabajo seguro en la áreas mediante la implementación de las políticas de seguridad de la información.

11.2.1 Los equipos de computo cuentan con un entorno adecuado en cuanto a su ubicación y protección en lo que respecta a las oficinas y salas de computo.

11.2.2 Todos los equipos cuentan con una fuente de conexión energética alterna y regulada, se puede apreciar a través de los tomas de corrientes naranja que se presentan.

11.2.4 Desde el área de Tic realizan de manera periódica mantenimiento preventivo a los equipos, en cuanto a los equipos de las salas de computo cada 6 meses y los administrativos de acuerdo a las solicitudes.

11.2.5 -11.2.6 Se cuentan con pólizas de seguro para los equipos de computo cuando esto son retirados fuera de la Institución, se tiene como mecanismo lógico

de aseguramiento de la información que el dispositivo contiene las herramientas de google como el Drive.

11.2.7 El área de Tic realiza un proceso de disposición y/o reutilización de equipos de manera segura; así mismo, cada uno de los equipos cuenta con software licenciado.

11.2.8 Los equipos tienen configuradas salvapantallas en su equipos con claves, al igual que los diferentes sistemas como la plataforma del campus el cual permite su bloqueo o cierre de sesión al pasar una inactividad sobre él por al menos unos 3 minutos.

11.2.9 El principio de escritorio limpio y pantalla limpia en los diferentes equipos que se encuentran en los departamentos administrativos y académicos se cumple.

No conformidades:

11.1.2 - 11.1.3 Al interior de las oficinas no se cuenta con los suficientes recursos de seguridad física que pueda garantizar tanto la seguridad de los dispositivos de hardware como la seguridad de las personas, siendo activos de información importante para la Institución. A pesar, de que se logró implementar un acceso biométrico solo al centro de datos y aseguramiento de las puertas colocando un sellamiento como un primer filtro. Sin embargo, para ingresar a las oficinas administrativas y académicas no se cuenta con un sistema de registro y/o acceso a ellas.

11.2.3 La Institución Universitaria Colegio Mayor del Cauca no todos los equipos cuentan con las protecciones adecuadas para el cableado del entorno en donde se encuentran, como se evidencia en la siguiente figura.

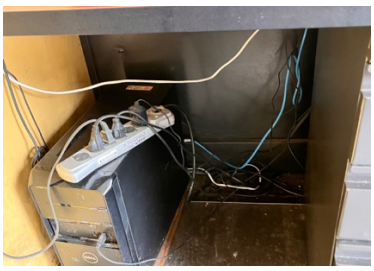

Figura 1. Seguridad en el cableado

Observaciones:

11.1.2 - 11.1.3 Entre las medidas de seguridad física que podrían implementarse en las áreas son: cámaras de seguridad, algún sistema biométrico y/o lector de tarjeta que garantice el ingreso correcto de las personas autorizadas. Además, realizar ajustes en las cerraduras de algunas puertas y/o cambio de las mismas. Por otra parte, mejorar el sistema de ingreso de los estudiantes por el alto riesgo de falsificación del carnet, lo que podría tener acceso a las instalaciones personal mal intencionado.

11.1.5 Se sugiere seguir realizando de manera periódica actividades que permitan interiorizar y apropiar las buenas prácticas de trabajo seguro establecidas en la política.

11.1.4 Se recomienda tener un sistema de alarma o sensor que indique las condiciones de temperatura adecuada en el área del centro de procesamiento de datos que permita el monitoreo de manera remota.

11.2.3 Estructurar el sistema de cableado bajo un sistema estandarizado y organizado en todas las áreas.

11.2.6 Salvaguardar la información mediante mecanismos de almacenamiento en la nube en especial la información que contienen los servidores.

11.2.9 Seguir reforzando el principio de escritorio limpio y pantalla limpia en los diferentes equipos que se encuentran en los departamentos administrativos y académicos.

11.1.6 Debido a la naturaleza de la institución no presentan área de carga y descarga.

Dominio 12. Procedimiento Operacionales y Responsabilidades

Conformidades:

12.1.1 El área de Tic cuenta con un Plan Estratégico de las Tecnologías de Información – PETI, donde reposan los proyectos que se tienen planeados desarrollar tanto los relacionados con la seguridad de la información y por ende éstos son articulados al Poa.

12.1.2 Al realizar algún ajuste en los sistemas de procesamiento de la información, éste se realiza a partir de un requerimiento ya sea solicitado por una dependencia en específica, al realizar los ajustes correspondientes desde el área de desarrollo se lleva un formato para evidenciar la gestión de los cambios del mismo. Por otra parte, cualquier cambio y/o ajuste ya sea en las instalaciones o proyectos son documentados desde el área de Tic y del área de desarrollo. Cabe anotar, si los requerimiento tienen un alcance grande se maneja a través de proyectos.

12.1.3 Desde el área de Tic se realiza seguimiento al uso de los recursos, lo que le permite hacer ajustes y proyecciones de los requerimientos que podrían necesitarse con el fin de garantizar una continuidad del sistema. Es importante mencionar, que a través del invetanrio de medios educativos se hace un análisis de cuales son los equipos que requieren ser cambiados y de esa manera justificar los cambios y/o reemplazos.

12.2.1 La Institución ha adquirido plataformas para protección de la información contra códigos maliciosos, las cuales se encuentran actualizadas y monitoreadas por el personal Tic. Se tiene Software de protección anti espía, antimalware y antivirus para todos los equipos de uso administrativo y académico como es el UTM (Plataforma de administración unificada contra amenazas) de Hillstone con quien se logró tener una alta disponibilidad. Es importante anotar que el servicio de antivirus se tiene con Heimdal Security, el cual se tienen 500 licencias y para los equipos de prestamo se cuenta con antivirus de software libre. Cabe precisar, que este licenciamiento también cobijan a los servidores que se encuentran en el área de procesamiento de datos; además, con el software Pereception Point plataforma de seguridad para gestión de correos electrónicos, actualmente abarca 75 buzones se está pendiente en hacer el despliegue a los demás a partir del estudio económico.

12.4.1 El sistema de información (Campus) que administra y gestiona la información de la Institución cuenta con un módulo o registro de auditoría, éste es consultado a través de la base de datos, el cual permite revisar las actividades de los usuarios, frente alguna falla, evento y/o incidente que se presente en el sistema.

12.4.3 Las actividades de administrador en sistemas de red y de información están registradas en servidores y plataformas de protección como el sistema Hillstone, Heimdal Security y Pereception Point. Además se tienen programadas las alertas automáticas a los correo de los administradores. Es importante mencionar que la revisión de los registros de estados de actualizaciones de seguridad no se aplican automáticamente sino de manera manual, en virtud de que no se tiene un laboratorio de prueba como tal. Es de resaltar, que a los servidores de producción y los servidores que están virtualizados (Campus, Glpi, Repositorio Unimayor - Pruebas,Celeste, Autorvaluación, Dhcp), se les realiza una revisión diaria a través de consola.

12.4.4 Los equipos del área administrativa y académica se encuentran sincronizados, al igual que los relojes de los equipos de procesamiento de datos.

12.5.1 Existe una política que controla y supervisa la instalación de software en los sistemas operativos de los dispositivos, esta es: la Política de uso de salas de sistemas y laboratorios.

12.6.2 Se implementan restricciones para la instalación de software por parte de los usuarios a través de la Política de uso de salas de sistemas y laboratorios.

12.7.1 Se realizan revisiones a través de la soluciones de seguridad implementadas al sistema, con el fin de evaluar las estrategias que permitan minimizar las interrupciones.

No Conformidades:

12.1.4 Se realizan pruebas funcionales a los desarrollos propios que se construyen, éstas se documentan. Sin embargo, no se realizan unas pruebas de seguridad que evidencien claramente el estado de vulnerabilidad o aseguramiento de los sistemas de información que la institución maneja.

12.3.1 A pesar de realizar las copias de seguridad una vez al mes a los servidores, éstos presentan un alto riesgo dado a que las copias son almacenadas

en el servidor de respaldo. Por otra parte se identificó que no se respalda la información en su totalidad a docentes(Ocasionales – Planta), solamente si éstos han almacenado la información en el Drive. Se destaca que se ha designado un responsable para realizar seguimiento o control del proceso de copias de respaldo.

12.4.2 Las instalaciones y la información no se encuentran correctamente protegida contra alteraciones y accesos no autorizados, dado que no se han implementado controles de seguridad adecuados que permita minimizar el riesgo a que ésta quede vulnerable como por ejemplo: Pruebas de concepto a los servidores de manera periódica e implementar medidas de seguridad pasiva más eficiente en cuanto a la seguridad física.

12.6.1 Oportunamente no se cuenta con información de las vulnerabilidades que presentan los sistemas de información de la Institución, por lo que es imposible evaluar y medir el impacto de éstas para poder tomar medidas preventivas, ya que solo se actúa en el momento de presentarse la incidencia más las que son registradas en el módulo GLPI.

Observaciones:

12.1.4 – 14.4.2 Se sugiere hacer pruebas de concepto de manera periódica a los servidores que dispone la institución, con el fin de tomar acciones y evaluar la efectividad de los controles implementados.

12.3.1 Se sugiere migrar a un sistema de respaldo de información con mayor capacidad de almacenamiento como la nube, así sea de manera progresiva y selectiva frente a los tipos de archivo a respaldar.

Dominio 13. Gestión de la seguridad en las redes

Conformidades:

13.1.1 Desde el área Tic se gestionan y controlan el acceso a las redes. Además se utiliza la herramienta Ruckus para gestionar el acceso a la red wifi, la Institución cuenta con 27 AP y se tiene la solución para el manejo de amenazas llamada Hillstone (UTM). Las subredes de la Institución están segmentadas lógica y físicamente, cuenta con Vlans y una adicional para la gestión de cámaras de seguridad, tiene asignación de IP única por direcciones físicas MAC en IPv4 y DUID en IPv6, también se asignan roles, permisos, puertos o servicios para los usuarios de sistemas de información. Así mismo, se evidencia la aplicación de controles y políticas en el UTM.

13.1.2 Se tienen documentados los servicios de red internos y externos mediante un diagrama de red que permite visualizar como están las Vlans, se tiene un canal de respaldo para internet y un canal de interconexión entre las sedes: Bicentenario, Casa Obando y Encarnación; mientras solo un canal de internet para Betlemitas. Actualmente se está haciendo el proceso de transición con Renata dado que brinda un canal de 300 megas. En cuanto a la separación de redes cada uno tiene habilitados sus servicios a los cuales tienen acceso; así como también la política de análisis de tráfico de entrada y salida.

13.1.3 En lo que respecta a la separación de las redes: la red es una y se administra solo desde la sede principal, se tiene documentado que son ocho subredes: financiera, administración, salas de computo, red wifi, servidores, DMZ, biblioteca, laboratorios, servicio de cámaras .

13.2.3 Se protege la información que se encuentra incluida en la mensajería electrónica a través de los servicios de seguridad que brinda el proveedor en este caso Perception point, acompañado con las buenas prácticas de seguridad que debe aplicar el usuario a partir de las políticas de control de acceso y seguridad de la información.

No conformidades:

13.2.1 No se cuenta con controles, políticas y procedimientos para transferencia de información por cualquier tipo de medio externa o internamente.

13.2.2 No existen acuerdos de transferencia de información externa e internamente, entre proveedores y/o contratistas.

13.2.4 No todas las resoluciones de contratación incluyen acuerdos de confidencialidad donde garantice y refleje la no divulgación de las necesidades e información de la Institución. Cabe anotar que se identificó esta falencia tanto a contratos de docentes, personal administrativos, contratistas y/o terceros. Un ejemplo de ello el contrato del servicio de sistema médico ocupacional, chofer, desarrolladores, entre otros no contemplan una cláusula donde especifiquen la seguridad y el tratamiento adecuado de la información luego de finalizar la contratación.

Observaciones:

13.2.1 13.2.2 En virtud de que no se cuenta con controles, políticas y procedimientos para transferencia de información por cualquier tipo de medio externa o internamente. Se propone ajustar este control mediante la implementación de los lineamientos del estándar ISO/IEC 27010, ya que proporciona controles y orientaciones que permiten mantener y mejorar la seguridad de la información en cuanto a las comunicaciones.

13.2.4 Incluir en todas las resoluciones de contratación acuerdos de no transferencia y duración de la cláusula de confidencialidad donde garantice la no divulgación de las necesidades e información de la Institución.

Dominio 14. Requisitos de seguridad de los sistemas de información

Conformidades:

14.1.1 En cuanto al análisis y especificaciones de requisitos de seguridad de la información se aplican controles básicos como control: el cifrado en cuanto al almacenamiento de las contraseñas y la validación de ingreso de datos.

14.1.2 – 14.1.3 En lo que respecta a la seguridad de los servicios y aplicaciones en redes públicas se fortaleció con la implementación del protocolo HTTPS en los módulos del campus que están de cara a Internet y se mejoró la gestión de contraseñas mediante el módulo de restauración sino también a través de un token de acceso. Lo relacionado con la protección de transacciones de los servicios se tercerizó a través de un portal que provee el ACH para realizar el pago PSE de la matricula finaciera de los estudiantes.

14.2.1 Existe una política de desarrollo seguro aplicado en el área de desarrollo.

14.2.2 Los sistemas de información se les realiza un control de cambio mediante un procemiento formal, en virtud de que los desarrolladores están autorizados a tomar requerimientos y a emplear el GitHub para registrar los cambios que se le realicen al sistema.

14.2.4 La Institución tiene restricciones en cuanto a la gestión de los cambios en los sistemas de información, dado que se realiza a través de un proceso formal.

14.2.6 El área de desarrollo establece adecuadamente los ambientes de desarrollo e integración de sistemas durante todo el ciclo de vida del sistema.

No conformidades:

14.2.3 No se evidencia las pruebas de seguridad cuando se registran cambios en las plataformas y sistemas de información.

14.2.5 No se tienen lineamientos de construcción de software seguro de manera muy clara, pese a que cualquier personal del área de desarrollo no cuenta con la especifidad de estándares o lineamientos que permitan validar la seguridad del mismo.

14.2.7 El área de Tic no supervisa y hace seguimiento de las actividades de desarrollo que se contratan externamente, por lo que el contrato del sistema de información financiero es desarrollado por un proveedor externo (empresa Celeste Team), el cual es supervisado por la encargada del área de financiera.

14.2.8 – 14.2.9 – 14.3.1 No se evidencia prueba funcional de seguridad, de aceptación y de protección de datos de pruebas.

Observaciones:

14.1.1 Se sugiere incluir módulo de auditoría, lo cual permitirá conocer la trazabilidad de los acceso de los usuarios sin necesidad de requerir un acceso a la bases de datos para poder identificar ésto. Por otra parte, se debe adoptar una metodología de desarrollo que incluya todos los componentes de seguridad para cumplir con la política de desarrollo seguro.

14.2.1 Se sugiere realizar una revisión y actualización a la política de desarrollo seguro.

14.2.5 Se sugiere que no solo se limiten a tomar y a especificar los requerimientos en cuanto a lo funcional sino a su vez se determinen los requisitos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.

14.2.7 Es importante que el área Tic se apropie de cada uno de los desarrollos que realicen proveedores externo, para poder determinar las pruebas de seguridad ha implementarse y de esta manera minimizar el riesgo frente alguna amenaza.

14.2.3 - 14.2.8 – 14.2.9 – 14.3.1 Se debe implementar un sistema automatizado o manual que cumpla las características de un ambiente de desarrollo seguro para pruebas de funcionalidad, aceptación y proteger los datos de prueba.

Dominio 15. Seguridad de la información con los proveedores

Conformidades:

15.1.1 La Institución Universitaria Colegio Mayor del Cauca, cuenta con una política de seguridad de la información para las relaciones con los proveedores.

15.2.1 Desde el área que corresponda la contratación del servicio externo, se le asigna un supervisor quien es la persona que realiza el seguimiento y revisa la ejecución de las actividades prestadas por el proveedor.

No conformidades:

15.1.2 – 15.1.3 A pesar de que se incluyen acuerdos o claúsulas de confidencialidad a los contratos con proveedores, desde el área Tic no se tiene definido los requisitos de seguridad de la información en cuanto a la no transferencia o tiempo de no divulgación al momento de la adquisición de un producto y/o servicio de Tecnología de la información y comunicaciones (Se tiene solamente unas obligaciones de seguridad que son iguales para todos los contratos).

15.2.2 No se realizan ajustes o cambios a las cláusulas y/o contratos de suministro de servicios, de acuerdo a la revaloración de los riesgos cuando es requerido.

Observaciones:

15.1.1 Se deben implementar algunas estrategias de socialización de la Politica de seguridad de la información para las relaciones con los proveedores, dado que no es muy operativa por su desconocimiento y contenido.

15.1.2 – 15-1-3 Implementar el requisito de seguridad en las resoluciones de contratación, así como también tener definidos los párametros o pruebas de seguridad aplicar al producto o servicio nuevo ha adquirir.

15.2.2 Implementar claúsulas en los contratos de terceros en cuanto a la seguridad de la información, lo que permitirá no tener que realizar un nuevo contrato sino realizar un ajuste y/o cambio en la respectiva claúsula alineanda a los procedimientos y políticas de seguridad.

Dominio 16. Gestión de incidentes y mejoras en la seguridad de la información

Conformidades:

16.1.1 – 16.1.2 – 16.1.3 Se han establecido responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada frente a los incidentes de seguridad de la información; así como también los canales apropiados para el reporte de los diferentes eventos.

16.1.4 Los eventos de seguridad de la información se evalúan para decidir si se clasifican como incidentes de seguridad apoyados de las soluciones Perception Point y Hendial.

16.1.5 – 16.1.7 Frente a las respuesta a incidentes de seguridad de la información se tiene un formato para reportar y documentar el tipo de soporte que se brinda a dicha incidencia. Cabe anotar, que en este mismo formato se relacionan la respectiva recolección de las evidencias. Lo anterior, reposa en el área de Tic.

16.1.6 Posterior a un incidente de seguridad se realiza un análisis, lo que permite reducir la posibilidad o el impacto de incidentes futuros.

No Conformidades: Ninguna

Dominio 17. Continuidad de seguridad de la información

Conformidades:

17.1.1 – 17.1.2 – 17.1.3 Se tiene definido un plan de continuidad de información para eventualidades críticas, así como también se ha documentado e implementado mediante la política de continuidad del negocio seguridad y privacidad de la información, la cual fue expedida el 2 de Diciembre de 2019.

No conformidades:

17.2.1 Actualmente las instalaciones de procesamiento de información no presentan la redundancia suficiente para cumplir con los requisitos de disponibilidad, por lo que no se cuenta con un mecanismo de almacenamiento en la nube eficiente y con capacidad suficiente de respaldar la información almacenada en los servidores y demás equipos que se considere primordial garantizar la seguridad en la información.

Observaciones:

17.2.1 Debe implementarse una medida adecuada de almacenamiento de respaldo en la nube, lo que permitirá garantizar un aseguramiento externo de la información en caso de alguna eventualidad y/o falla en los servidores o discos de respaldos.

Dominio 18. Cumplimiento

Conformidades:

18.1.4 La Institución Universitaria Colegio Mayor del Cauca, cuenta con una política sobre la privacidad y la protección de datos personales, el cual ha sido socializada y se encuentra pública en la página web Institucional.

18.1.5 La Institución hace uso de controles criptográficos dando cumplimiento a la reglamentación pertinente, para que la información que circula en las redes internas no viaje en texto claro.

18.2.1 Se ha realizado un proceso externo para la revisión del aseguramiento, continuidad, educación y eficacia en cuanto a la seguridad de la información a través de la seguradora solidaria.

No conformidades:

18.1.1 - 18.1.2 Teniendo en cuenta el enfoque de la Institución, tienen identificados, documentados todos los requisitos estatutarios, reglamentarios y contractuales para cada sistema de contratación. Sin embargo actualmente no se es muy claro la necesidad de incluir en todas las resoluciones contractuales algunas cláusulas de seguridad de la información; así como también la de derechos de propiedad intelectual, reconociendo que desde la Institución se produce software, el cual no se encuentran protegidos sus derechos.

18.1.3 Desde el área Tic, no se cuenta con esquema de clasificación de los registros, así como también no existe un procedimiento y manejo de medios usados para el almacenamiento de éstos y no se tiene un sistema que permita la recuperación de los datos almacenados en tiempo y formato aceptable.

18.2.2 – 18.2.3 No se revisa con regularidad el cumplimiento de las políticas desde el comité establecido por la dirección, con el propósito de actualizar éstas para que estén alineadas a las necesidades y además no se actualiza desde el sitio web con las vigentes.

Observaciones:

18.1.1 – 18.1.2 Involucrar dentro de los requisitos contractuales el componente de seguridad de la información y si es requerido el de propiedad intelectual.

18.1.3 Implementar un mecanismo de almacenamiento eficiente de mayor capacidad como la nube que permita salvaguardar los registros, así como definir un procedimiento para el manejo y almacenamiento de los registros.

18.2.1 Se sugiere continuar con las dinámicas de evaluación externa al sistema de gestión de seguridad de la información, dado que permite tener una mirada más objetiva del avance del sistema de gestión de seguridad de la información.

Documentación básica del modelo de privacidad de la seguridad de la información - MSPI

NO.	DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN Lista de información BASICA a solicitar	NOMBRE DEL DOCUMENTO ENTREGADO	SE TIENE		ESTADO	OBSERVACIONES
			SI	NO		
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)	Tipo de entidad y plazos. docx Respuesta MinTic Clasificación y plazos.pdf	x		Vigente	Entidad de orden territorial
2	Misión	Misión Unimayor.docx	x		Vigente	
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.	Plan de tratamiento de riesgos de seguridad y privacidad de la información V5- 27-01-22	x		Vigente	Revisar y validar el documento, porque el entregado en el MSPI, se encuentra uno NO vigente
4	Mapa de Procesos	D5-MAPA_DE_PROCESOS_V4.pdf	x		Vigente	
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	https://unimayor.edu.co/web/images/TalentoHumano/2022/ORGANIGRAMA_FUNCIONAL_2022.pdf	x		Vigente	
6	Políticas de seguridad de la información formalizada y firmada	https://unimayor.edu.co/web/images/TIC/2019/Seguridadinformatica/D3-POL%C3%8DTICA_DE_SEGURIDAD_Y_PRIVACIDAD_DE_L	x		Vigente	Se requiere revisar, validar y actualizar todas las políticas relacionadas con seguridad de la información
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	http://190.5.199.19/sgi/documentos/D9-_ROLES_Y_RESONSABILIDADES_V5.pdf	x		Vigente	Actualizado 23-06-2022
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección	http://190.5.199.19/sgi/documentos/PLAN_Y_ESTRATEGIA_DE_TRANSICI%C3%93N_DE_IPv4_A_IPv6_V1.pdf	x		Vigente	Actualizado 15-08-2020
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección	MSPI Actualizado 2020	X		No Vigente	Desactualizado, debe hacerse de forma periódica al menos 1 vez al año
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección	Estratificación de la entidad.Docx	X		Vigente	Verificar.
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	Plan de tratamiento de riesgos de seguridad y privacidad de la información V5- 27-01-22	x		Vigente	Revisar y validar el documento, porque el entregado en el MSPI, se encuentra uno NO vigente
12	Procedimientos de control documental del MSPI	Pendiente por documentar		x	No documentado	
13	Metodología de Gestión de riesgos	Plan de tratamiento de riesgos de seguridad y privacidad de la información V5- 27-01-22	x		Vigente	Revisar y validar el documento, porque el entregado en el MSPI, se encuentra uno NO vigente
14	Riesgos identificados y valorados de acuerdo a la metodología	Plan de tratamiento de riesgos de seguridad y privacidad de la información V5- 27-01-22		x	No documentado	En proceso.. Sin embargo, el presentado en el Mspi.. No dá respuesta el documento relacionado
15	Planes de tratamiento de los riesgos	Plan de tratamiento de riesgos de seguridad y privacidad de la información V5- 27-01-22		x	No documentado	En proceso.. Sin embargo, el presentado en el Mspi.. No dá respuesta el documento relacionado
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información	Contratos de contratistas y Proveedores		X	No Documentado	Tiene claúsulas generales. Pero éstas no cubren o blindan la seguridad de la información de la institución.
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad	http://190.5.199.19/sgi/documentos/P1-_SELECCION_Y_VINCULACION_V10.pdf	X		Vigente	Revisar y validar el documento, porque el entregado en el MSPI, se encuentra uno NO vigente
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	Pendiente por documentar		x	No documentado	
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información	Pendiente por documentar		x	No documentado	
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección	Identificación y clasificacion de activos Información.xlxs Está pendiente la aprobación por la alta dirección	x		Vigente	Actualizarlo anualmente, Según el Mspi pendiente por aprobación
21	Inventario de áreas de procesamiento de información y telecomunicaciones	Plataforma GLPI donde registran los activos	X		Vigente	Actualizarlo anualmente, Según el Mspi no presentan pero en el proceso de auditoría se evidención que cuentan con éste a través de la gestión en plataforma GLPI
22	Diagrama de red de alto nivel o arquitectura de TI	interconexion.pdf	x		Vigente	
23	Inclusión de la seguridad de la información en la gestión de proyectos	Se implementó la confidencialidad en los contratos de prestacion de servicio y docentes ocasionales	X		Vigente	
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad	Pendiente por documentar		x	No documentado	
25	Formato de acuerdo de transferencia de información	formato único de inventario documental Cód: 201.06.03.02.R.01		x	No documentado	El presentado en MSPI no dá respuesta
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden	Se obtiene del sistema CELESTE		x	No documentado	Relacionar en un documento el inventario de proveedores.
27	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.	R19-FORMATO_INCIDENTES_SEG._DE_LA_INFORMACIÓN_V2.xlxs	x		Vigente	Se cuenta con el reporte de incidentes.
28	Plan de continuidad de la Entidad aprobado	CONTINUIDAD_DE_NEGOCIO_V2.pdf	x		Vigente	
29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información	D8-NORMOGRAMA_TIC_V10.pdf	x		Vigente	
30	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad	La entidad ha realizado una auditoria de seguridad y privacidad de la informacion. INFORME DE AUDITORIA INTERNA_KM.pdf	x		Vigente	Elaborar un plan de auditoría interna y externa y diseñar un programa de auditoría
31	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION V4.pdf ROLES Y RESONSABILIDADES V2.pdf PLAN_SENSIBILIZACIÓN V2.pdf POLITICA DE CONTROL DE ACCESO_V2.pdf POLÍTICA DE DESARROLLO SEGURO V2.pdf POLÍTICA DE GESTIÓN DE ACTIVOS V2.pdf POLÍTICA PARA PROVEEDORES V2.pdf PLAN DE SEGURIDAD Y PRIVACIDAD_v2.pdf PLAN DE TRATAMIENTO DE RIESGO_v2.pdf GESTIÓN DE INCIDENTES V2.pdf CONTINUIDAD DE NEGOCIO V2.pdf REPORTE INCIDENTES SPI V2.pdf MATRIZ ANALISIS DE RIESGOS DE SPI V2.pdf DECLARACIÓN DE APLICABILIDAD V2.pdf	X		Vigente	
32	Indicadores y métricas de seguridad de la información definidos.	http://190.5.199.19/sgi/documentos/D18-INDICADORES_DE_GESTION_V1.pdf	x		No Vigente	El sitio web se presenta uno no actualizado, se sugiere semestralmente validar, aparece hasta el año 2020
33	Declaración de aplicabilidad	R21-_FORMATO_DECLARACIÓN_DE_APLICABILIDAD_V1.xlxs	x		No Vigente	Revisar el documento de aplicabilidad, en cuanto a la efectividad de los controles propuestos, está desactualizado presenta año 2019
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos	D16-PLAN_DE_GESTIÓN_DE_RIESGOS_V1.pdf	x		No Vigente	Revisar requerimiento porque el presentado en el sitio web está desactualizado hasta el año 2019
	Lista de información para aquellas entidades que hayan avanzado en la fase de IMPLEMENTACIÓN					
35	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	PETI	X		vigente	No hay seguimiento del los proyectos propuestos, el cual deben estar articulados a los indicadores de gestión del SGSI
36	Avance en la ejecución del plan de tratamiento de riesgos	Pendiente por documentar		x	No documentado	Presentan una evidencia que no dá respuesta
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	Pendiente por documentar		x	No documentado	Presentan una evidencia que no dá respuesta
	Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO					
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	Pendiente por documentar		x	No documentado	Presentan una evidencia que no dá respuesta
39	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	PLAN_AUDITORIA SEGURIDAD.docx INFORME DE AUDITORIA INTERNA_KM.pdf	X		Vigente	
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.	Pendiente por documentar		x	No documentado	
	Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA					
41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.	Pendiente por documentar		x	No documentado	En proceso
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidaes de mejora se subsanen, para asegurar la mejora continua.	Pendiente por documentar		x	No documentado	En proceso

En virtud del análisis anterior se evidencia que el 55% de los documentos básicos que soportan el MSPI se encuentran vigentes, el 36% de la documentación que solicitan está pendiente por documentar y un 4% de los documentos están pendientes por ser actualizados.

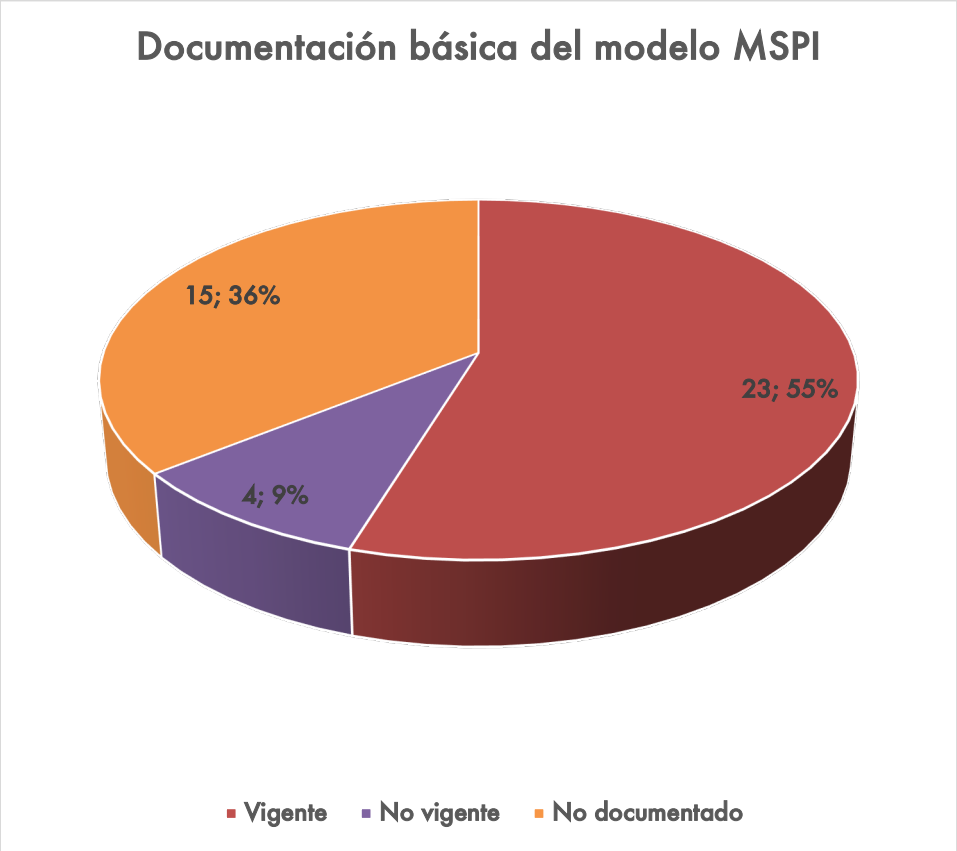

Figura 2. Documentación básica del MSPI

Análisis porcentual de cumplimiento de los dominios

Dominio 5. Política de seguridad de la información

Cumplimiento del dominio:

Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 100% como se muestra en la siguiente figura.

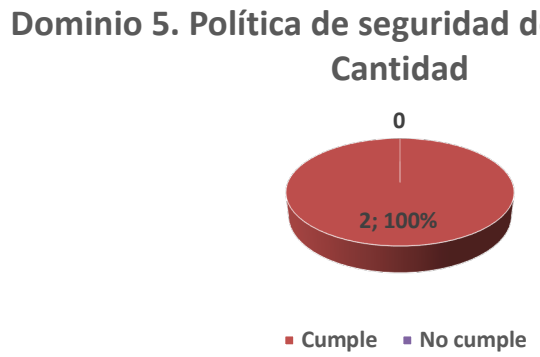

Figura 3. Cumplimiento del dominio 5

Dominio 6. Organización de la seguridad de la información

Cumplimiento del dominio:

Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 100% como se puede evidenciar en la siguiente figura.

Figura 4. Cumplimiento dominio 6

Dominio 7: Seguridad ligada a los recursos humanos

Cumplimiento del dominio:

Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 33%, con relación a 67% de no cumplimiento como se puede evidenciar en la siguiente figura.

Figura 5. Cumplimiento dominio 7

Dominio 8. Gestión de activos

Cumplimiento del dominio:

Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 60%, con relación a un 40% de no cumplimiento como se puede evidenciar en la siguiente figura.

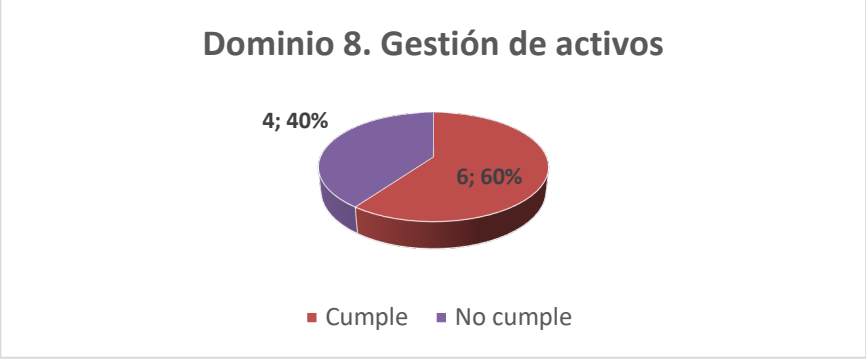

Figura 6. Cumplimiento dominio 8

Dominio 9. Control de acceso

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 64%, con relación a un 36% de no cumplimiento como se puede evidenciar en la siguiente figura.

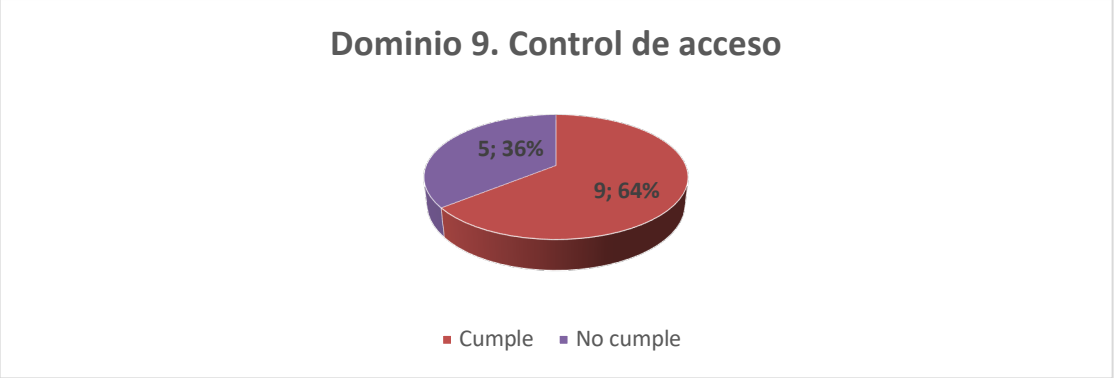

Figura 7. Cumplimiento dominio 9

Dominio 10. Criptografía

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 100% como se muestra en la siguiente figura.

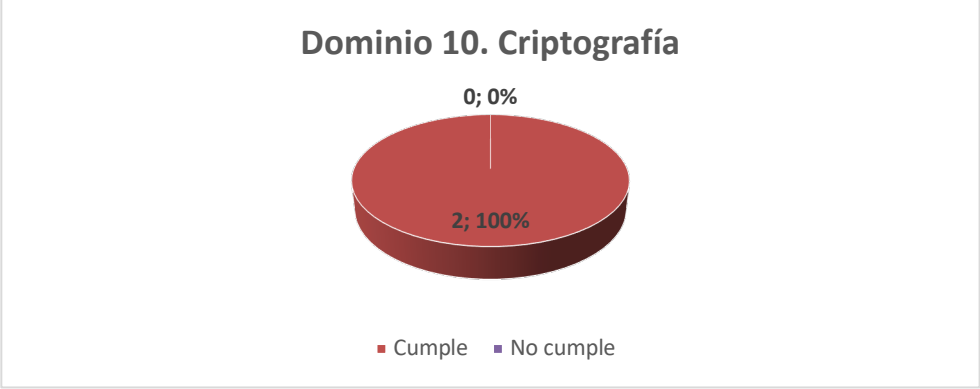

Figura 8. Cumplimiento dominio 10

Dominio 11. Seguridad Física y del entorno

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 79%, con relación a un 21% de no cumplimiento como se puede evidenciar en la siguiente figura.

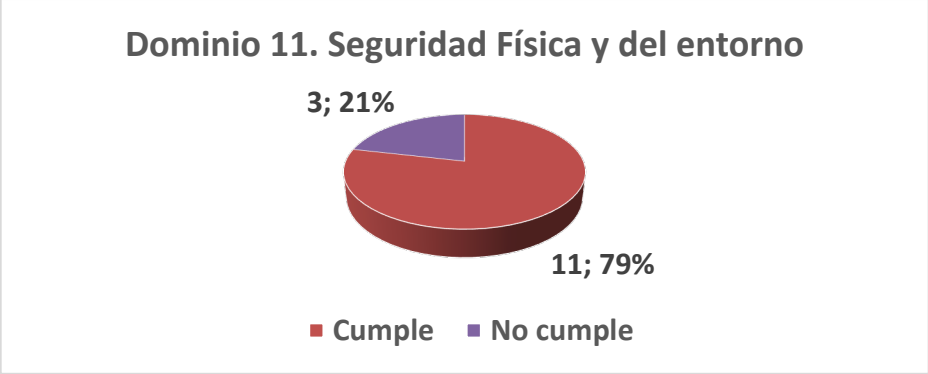

Figura 9. Cumplimiento dominio 11

Dominio 12. Procedimiento Operacionales y Responsabilidades

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 71%, con relación a un 29% de no cumplimiento como se puede evidenciar en la siguiente figura.

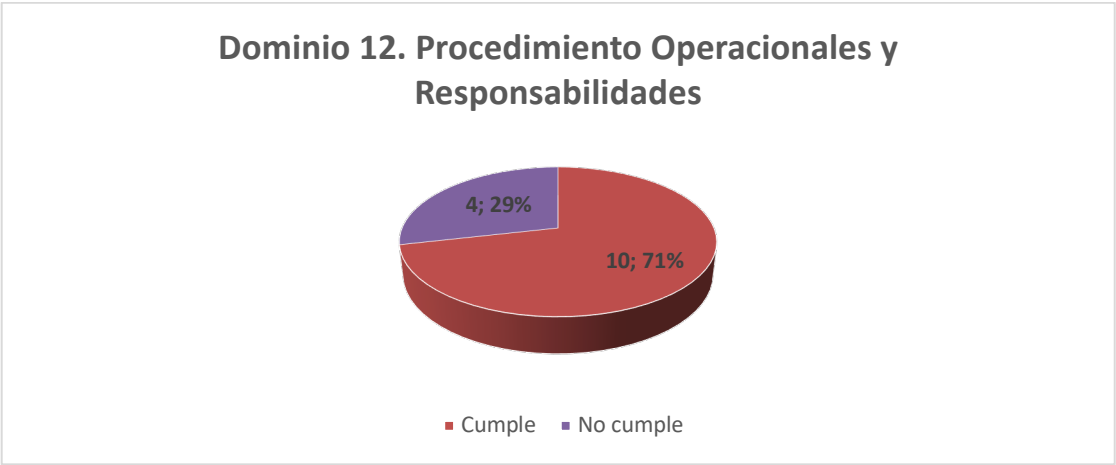

Figura 10. Cumplimiento dominio 12

Dominio 13. Gestión de la seguridad en las redes

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 57%, con relación a un 43% de no cumplimiento como se puede evidenciar en la siguiente figura.

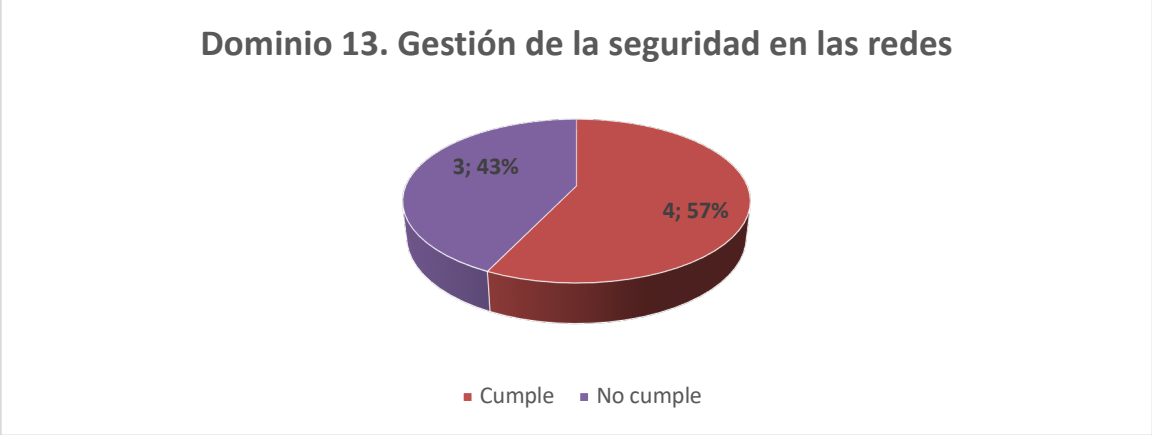

Figura 11. Cumplimiento dominio 13

Dominio 14. Requisitos de seguridad de los sistemas de información

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 54%, con relación a un 46% de no cumplimiento como se puede evidenciar en la siguiente figura.

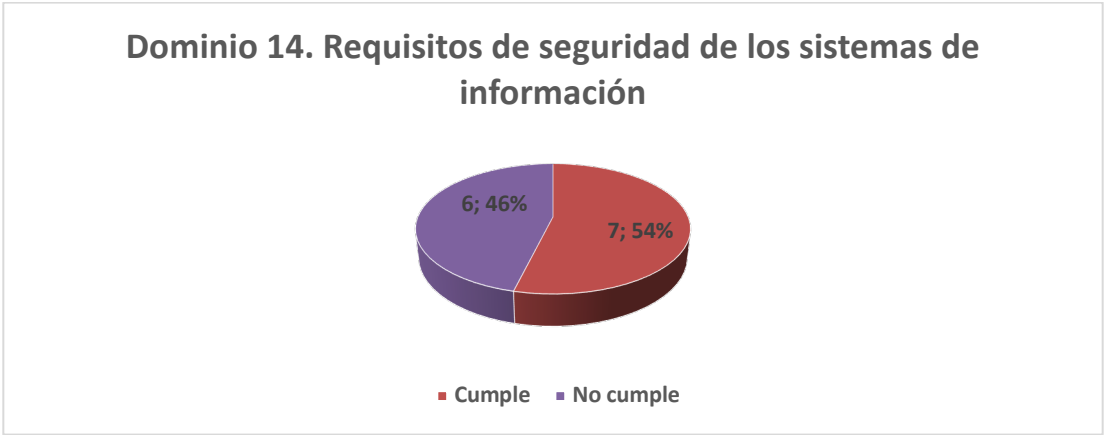

Figura 12. Cumplimiento dominio 14

Dominio 15. Seguridad de la información con los proveedores

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 40%, con relación a un 60% de no cumplimiento como se puede evidenciar en la siguiente figura.

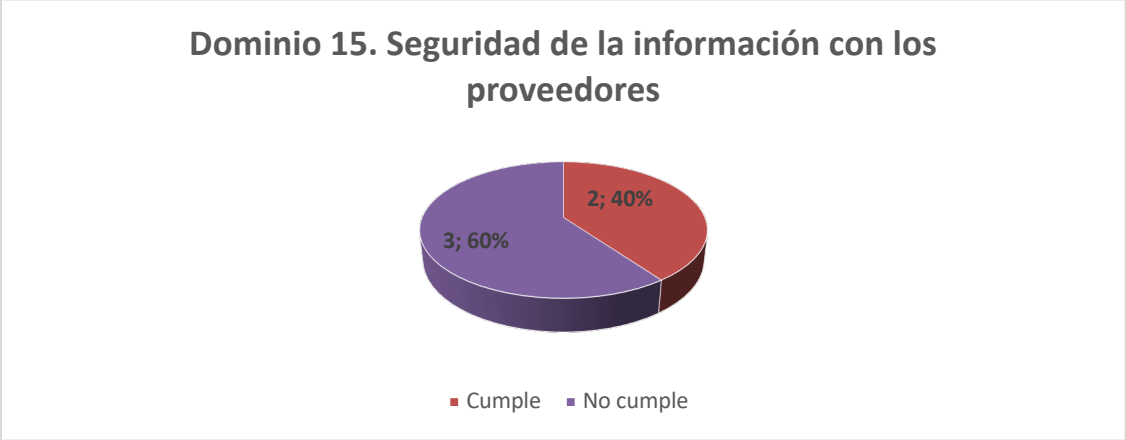

Figura 13. Cumplimiento dominio 15

Dominio 16. Gestión de incidentes y mejoras en la seguridad de la información

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 100% como se muestra en la siguiente figura.

Figura 14. Cumplimiento dominio 16

Dominio 17. Continuidad de seguridad de la información

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 75%, con relación a un 25% de no cumplimiento como se puede evidenciar en la siguiente figura.

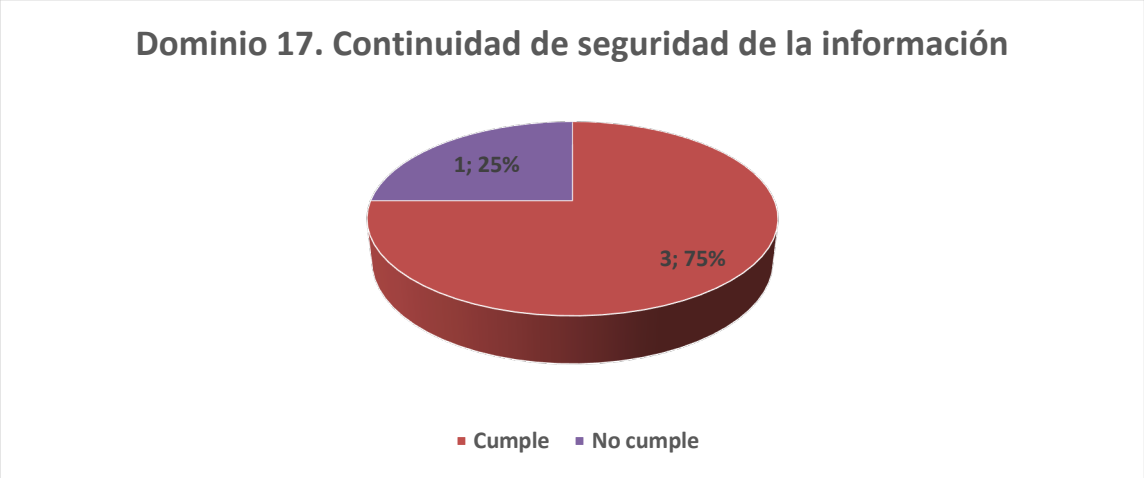

Figura 15. Cumplimiento dominio 17

Dominio 18. Cumplimiento

Cumplimiento del dominio:
Luego de la evaluación de los controles del dominio se determina que el cumplimiento de éste es de un 37%, con relación a un 63% de no cumplimiento como se puede evidenciar en la siguiente figura.

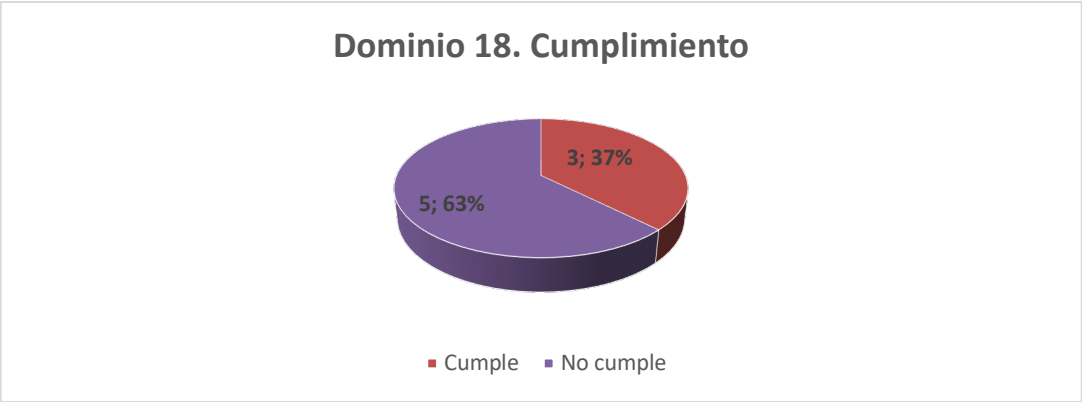

Figura 16. Cumplimiento dominio 18

A manera de conclusión se determina que los únicos dominios que tiene un cumplimiento de 100% son: 5,6,10 y 16, siguiendo el dominio 11 con un 79%, el dominio 17 con un 75%, dominio 12 con un 71%, el dominio 9 con un 64%, el dominio 8 con un 60% de cumplimiento, el dominio 13 con un 57%, dominio 14 con un 54%, el dominio 15 con un 40%, dominio 18 con un 37% y el dominio 7 con un 33% de cumplimiento en sus controles.

Con relación a los dominios que tienen un porcentaje de no cumplimiento más alto se encuentra el dominio 7 con un 67%, siguiéndole el dominio18 con 63%, el dominio 15 con un 60%, el dominio 14 con un 46%, así mismo el dominio 13 con un 43%, y el dominio 8 con un 40%; mientras que el dominio 9 presenta un incumplimiento del 36% y el dominio 12 con un incumplimiento del 29%, el dominio 17 con 25% y el dominio 11 con el 21% de No cumplimiento.

A partir de lo anterior, se concluye que el 66% lo que equivale a 75 controles del estándar ISO/IEC 27001:2013 cumplen de manera satisfactoria su implementación, mientras que el 33% equivalente a 38 controles no están implementados de manera adecuada por lo que se requieren acciones de mejora. No obstante es importante mencionar que se excluyó 1 control (11.1.6), dado a la naturaleza de la organización no aplican.

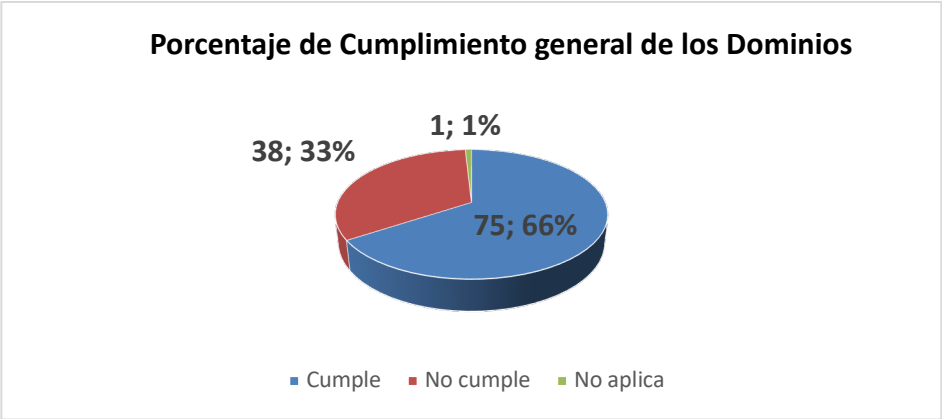

Figura 17. Porcentaje de Cumplimiento general de los Dominios

Referencias

ISO/IEC 27001:2013
ISO/IEC 27002:2013
LEY 1273 DE 2009
LEY 1581 DE 2012
DECRETO 1377 de 2013
LEY 527 DE 2009

Documento elaborado por: Katerine Márceles Villalba
Fecha: Agosto 28 de 2022

Revisado por: Fabián Hurtado Mosquera
Fecha: Agosto 29 de 2029