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: ING. JHON JAIRO PERAFAN
FABIÁN HURTADO MOSQUERA

OBSERVADOR: ING. MILDRED CAICEDO

OBJETIVO DE LA AUDITORIA: Evaluar el cumplimiento de los controles del estándar ISO/IEC 27001:2013 en los diferentes procesos de la institución colegio mayor del Cauca

ALCANCE: Realizar un diagnóstico del estado actual de cada unos de los dominios que contempla el estándar ISO/IEC 27001:2013 2013 en los diferentes procesos institucionales de la institución colegio mayor del Cauca

FECHA DE LA AUDITORÍA: Diciembre 10 al 19 de 2019
Enero 9 del 2020

NÚMERO DE HOJAS DEL INFORME: 43

Tabla de contenido

Dominio 5. Política de la Seguridad de la Información

Conformidades:
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 desde el área de TIC. Además ésta es revisada de manera periódica para incluirle actualizaciones de acuerdo a las necesidades, por lo que el 2 de Diciembre de 2019 se llevó a cabo la primera actualización en cuanto al alcance y el objetivo.

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.

Dominio 6. Organización de la seguridad de la información

Conformidades:

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.

No conformidades:

6.1.1. A Pesar de que se encuentran definida y asignadas las responsabilidades en cuanto al quehacer de cada rol, no se especifican claramente las responsabilidades en cuanto al tratamiento y seguridad que se le debe dar a la información dentro de las resoluciones de contratación.

6.1.2 Los empleados de la Institución Universitaria Colegio Mayor del Cauca tienen los deberes y roles definidos; sin embargo, en cuanto al acceso del área a su labor asignada se encuentra un poco vulnerable (Oficinas – Salones de clase), dado que el único medio de protección son los mostradores y/o escritorios y no existen lineamientos que determine o no el ingreso del personal no autorizado.

6.1.5 En lo que respecta a la seguridad de la información en la gestión de proyectos no se contempla ninguna cláusula en las resoluciones contractuales y tampoco en los lineamientos internos en lo que respecta al tratamiento seguro de la información dentro de los proyectos que se desarrollan tanto en lo académico y administrativo.

6.2.1 La Institución Universitaria Colegio Mayor del Cauca, no cuenta con una política y medidas de seguridad de soporte para los riesgos introducidos por el uso de dispositivos móviles.

Observaciones:

6.1.1 – 6.1.2 Es importante definir y asignar claramente las responsabilidades en cuanto a la seguridad de la información tanto en las resoluciones contractuales como en el manual de roles y funciones; por lo anterior sugiero revisar y apoyarse de la guía de seguridad (CCN-STIC-801) "Esquema Nacional De Seguridad Responsabilidades y Funciones", el cual pueden acceder a través de este enlace: https://cutt.ly/wrxpx8k

6.1.5 En lo que respecta a la seguridad de la información en la gestión de proyectos se sugiere contemplar una cláusula en las resoluciones contractuales y en los lineamientos internos en lo que respecta al tratamiento seguro de la información dentro de los proyectos que se desarrollan tanto en lo académico y administrativo.

6.2.1 Se sugiere establecer una política formal para adoptar las medidas de seguridad adecuadas para la protección contra los riesgos que son derivados del uso de los recursos de dispositivos móviles.

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.

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.

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.

7.2.2. No se le brinda a los empleados y contratista otros espacios diferentes a la de socialización de políticas y procedimientos que le permita apropiarse de la importancia del manejo seguro de la información.

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 Siag, 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, 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 desactualizado y que no corresponde al proceso y subproceso que realmente debería, una evidencia de ello se muestra en la figura 1.

Figura 1. Formato de traslado de equipos.

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 tienen medidas para la protección de la información que manejan éstos y tampoco durante éste proceso se aseguran que el equipo cuente con las medidas de seguridad lógica para salvaguardar la información en caso de algún incidente. Por otra parte se identificó que no todos los activos físicos tienen una cuenta de inicio se sesión como por ejemplo el Pc de admisiones, lo cual lo hace vulnerable.

Observaciones:

8.1.1. Se sugiere revisar de manera periódica el inventario de activos para mantener éste actualizado, dado que se encontraron unas pantallas que no estaban etiquetadas por tanto no se encontraban registradas en el aplicativo en el momento de la auditoría.

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 que se especifica la clasificación de los activos de información, la gran mayoría desconoce de éste, por lo que se sugiere establecer estrategias de socialización.

8.3.1 – 8.3.2 – 8.3.3 Actualizar el formato que emplean para retirar los dispositivos fuera de la Institución. Así como también implementar medidas de almacenamiento en la nube ya sea gratuito a través del almacenamiento de drive que brinda el sistema de mensajería electrónico y/o el uso de herramientas libres como Dropbox, entre otras, que permitan salvaguardar la información de los equipos de computo que son retirados fuera de la Institución.

Dominio 9. Control de acceso

Conformidades:

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

9.2.5 Solamente a nivel de Siag, se realiza una revisión periódica de los derechos de acceso lógicos asignados.

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.

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 como el algoritmo MD5 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.

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 tiene de 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 proceso formal de registro y de cancelación de usuarios 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 proceso 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.

9.2.4 – 9.4.2 No se cuenta con un sistema de doble autenticación frente al Siag, que permita identificar la identidad del usuario que realmente se encuentra ingresando al sistema, como por ejemplo preguntas de seguridad o el envío de algún ping a los medios de mensajería que tenga asociada con la plataforma.

Observaciones:

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 y/u otro sistema 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.

9.2.4 – 9.4.2 Implementar un sistema de doble autenticación frente al Siag, que permita identificar la identidad del usuario que realmente se encuentra ingresando al sistema, como por ejemplo preguntas de seguridad o el envío de algún ping a los medios de mensajería que tenga asociada con la plataforma.

Dominio 10. Criptografía

Conformidades:

10.1.2 A pesar de que no se tenga establecida como política si 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:

10.1.1 La Institución Universitaria Colegio Mayor del Cauca carece de una política que garantice la implementación en cuanto al uso de controles criptográficos para salvaguardar la información.

Observaciones:

Se sugiere documentar y enmarcarla dentro de la política de criptografía los parámetros y gestión que se le dan a las llaves, por lo pueden consultar el modelo de ejemplo de políticas propuesto por Sans en el enlace: https://cutt.ly/orxgpoo

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. A continuación se evidencia una muestra de lo anterior en la figura 2.

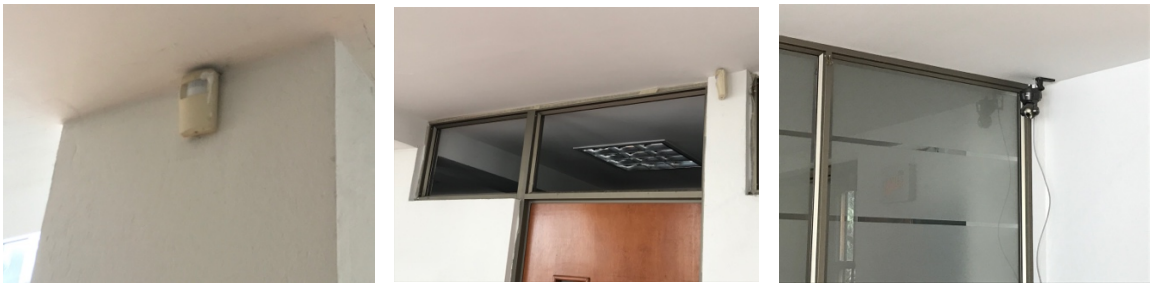


Figura 2. Perímetro de seguridad.

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.

11.2.2 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, ver figura 3.

Figura 3. Fuentes de energía alterna.

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.

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

No conformidades:

11.1.2 La Institución Universitaria Colegio Mayor del Cauca, todas sus áreas carecen de controles de acceso físico que garantice el acceso autorizado, que permita proteger los activos de información que integran ésta; No obstante, solamente se cuenta con un carnet, el cual permite el ingreso a toda la Institución sin llevar un registro de quien ingresa y a que hora sale de la misma sin ningún mecanismo que le permita validar la autenticidad del carnet.

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. En la siguiente figura se presenta una muestra de lo expuesto, lo cual se evidencia la insuficiencia en cuanto cierres y material físico de puertas y ventanas.

Figura 4. Áreas inseguras físicamente.

11.1.4 No se cuenta con una infraestructura adecuada frente amenazas externas y ambientales como por ejemplo: un detector de humo, dado que en la mayoría de las áreas se carecen(Solamente poseen área de comunicaciones y CPD), así mismo un sistema de alarma o sensor que indique las condiciones de temperatura adecuada en el área del centro de procesamiento de datos, ya que

se detecto que no todos los equipos reciben las mismas condiciones de enfriamiento y por ende se encuentran vulnerable frente alguna circunstancia de inundación, ya que ésta área no presentan ningún escalón frente al nivel del piso, cómo también se evidencio en el área de gestión documental. Ver figura 5.

Área de gestión documental

Área de Centro de procesamiento de datos (CPD)

Figura 5. Infraestructura frente amenazas externas y ambientales

11.2.1 Pese a que algunos equipos cuentan con un entorno correcto en cuanto a su ubicación y protección éstos son solos los ubicados en las oficinas, porque no todos se encuentran en las mismas condiciones, ya que se encontraron equipos ubicados en el suelo sin ninguna base y sin ninguna restricción de seguridad como se evidencia en la siguiente figura.

Figura 6. Ubicación y protección de los equipos.

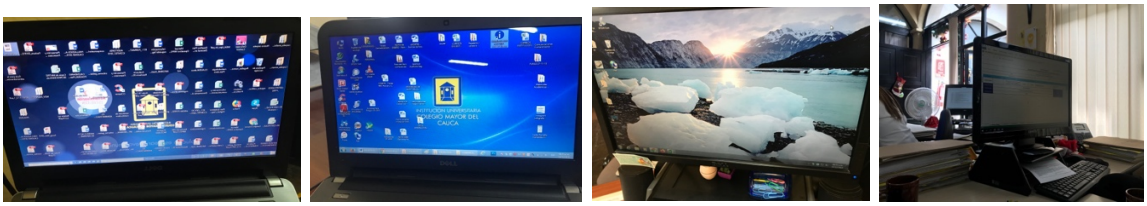
11.2.3 La Institución Universitaria Colegio Mayor del Cauca no cuenta con las protecciones adecuadas para el cableado del entorno en donde se encuentran sus equipos, como se evidencia en la siguiente figura.

Figura 7. Seguridad en el cableado

11.2.5 -11.2.6 A pesar de que se cuentan con pólizas de seguro para los equipos de computo cuando esto son retirados fuera de la Institución, no existe ningún mecanismo que permita garantizar el aseguramiento de la información que el dispositivo contiene, ya que el proceso de almacenamiento en la nube mediante el aplicativo OwnCloud es para el personal administrativo.

11.2.8 Dado que en la mayoría de los equipos tienen configuradas salvapantallas en su equipos con claves, aún algunos como el área de admisiones no presenta esta medida de seguridad, al igual que los diferentes sistemas como el Siag el cual permita su bloqueo o cierre de sesión al pasar una inactividad en él por al menos unos 3 min.

11.2.9 Por lo general el principio de escritorio limpio y pantalla limpia en los diferentes equipos que se encuentran en los departamentos administrativos y académicos no se cumple en su totalidad, como se evidencia en la siguiente figura.



Pantalla de escritorio no limpia Sin logo institucional Escritorio no Limpio

Figura 8. Escritorio limpio y pantalla limpia

Observaciones:

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.

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

11.1.4 Implementar medidas de seguridad frente amenazas de incendio como por ejemplo: un detector de humo, a las áreas que no lo tienen, así mismo un sistema de alarma o sensor que indique las condiciones de temperatura adecuada en el área del centro de procesamiento de datos, construcción de un escalón en la entrada del CPD y área de gestión documental.

11.2.1 Ubicar adecuadamente y con protección los equipos de computo, empleando bases y/o soportes.

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 para la comunidad de docentes y administrativos.

11.2.9 Implementación del principio de escritorio limpio y pantalla limpia en los diferentes equipos que se encuentran en los departamentos administrativos y académicos que cumplen en su totalidad.

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 correspondiente 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.

12.1.3 Desde el área de Tic 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.

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). Es importante anotar que el servicio de antivirus se tiene con la empresa Eset. Cabe precisar, que este licenciamiento también cobijan a los servidores que se encuentran en el área de procesamiento de datos, excepto los servidores con plataforma Linux; Sin embargo, éstos están protegidos por el filtrado del UTM y el antivirus de verisón libre Clamav. Los equipos con sistema operativo Linux son 3: el servidor de aplicaciones web que contiene el sistema de reservas el glpi, el de autoevaluación y talento humano.

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 ESET y el UTM. 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

ambiente de prueba. Es de resaltar que a los servidores nuevos se les realiza una revisión diaria a través de consola y a los otros dos veces por semana.

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 control de la Política de uso de salas de sistemas y laboratorios.

No Conformidades:

12.1.4 Se realizan pruebas funcionales, éstas se documentan pero no se realiza en ambientes separados ni controlados. Además no se tiene el procedimiento documentado para este control. Por consiguiente no se realizan pruebas de seguridad.

12.3.1 No existe política de copias de respaldo, se hace uso del sistema OwnCloud aunque se evidencio que ya no se tiene espacio para almacenamiento de información. Por otra parte se identificó que no se respalda la información de docentes(Ocasionales – Planta). No se ha designado un responsable para realizar seguimiento o control del proceso de copias de respaldo.

12.4.1 Los sistemas de información que administran la información de la Institución no cuentan con un módulo o registro de auditoría, que permita revisar las actividades de los usuarios, frente alguna falla, evento y/o incidente que se presente en el sistema. Por consiguiente, no se realiza de manera periódica solamente eventual la lectura de los logs a los servidores.

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 está 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.

12.4.4 A pesar que los relojes de los equipos del área administrativa y académica se encuentran sincronizados, se detectó que no se tienen sincronizados los relojes de los equipos de procesamiento de datos, lo que deja vulnerable al dispositivo frente a un incidente de seguridad por lo que no se va poder determinar la hora exacta y/o día en que ocurrio el evento.

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.

12.7.1 No se realizan revisiones constante de los registros de auditoría del sistema para evaluar las estrategias que minimicen las interrupciones, dado que por el momento este proceso no se tiene implementado.

Observaciones:

12.3.1 Se sugiere migrar a un sistema de respaldo de información con mayor capacidad de almacenamiento o incrementar la capacidad al sistema en uso.
Generar la política de Copias de respaldo, que incluya el filtrado de contenido y tipos de archivo a respaldar. Asignar un responsable para la administración del sistema de copias de respaldo.

12.4.1 Contemplar la implementación de un sistema para el análisis de logs de servidores, servicios, sistemas y aplicaciones como control para el registro de eventos.

12.1.4 Se realizan pruebas funcionales, éstas se documentan pero no se realizan en ambientes separados ni controlados, por lo cual se sugiere implementarlo. Además de generar un procedimiento documentado en cuanto a las pruebas de seguridad.

12.3.1 Generar una política de copias de seguridad que respalde la información de docentes(Ocasionales – Planta) y administrativos, se sugiere revisar la herramienta Cobian Backup.
En ese mismo sentido, designar un responsable quien realice el seguimiento o control del proceso de copias de respaldo.

12.4.1 Implementación de un módulo de auditoría del sistema de información. Por otra parte se sugiere que se realice de manera periódica la lectura de los logs a los servidores.

12.4.2 Realizar de manera periódica pruebas de concepto a los servidores e implementar medidas de seguridad pasiva más eficiente en cuanto a la seguridad física.

12.4.4 Sincronizar los relojes de los equipos del Centro de procesamiento de datos.

12.6.1 Analizar y medir el impacto de los incidentes de seguridad presentados, para tomar acciones frente a la efectividad de los controles implementados.

12.7.1 Realizar de manera periódica auditorías al sistema para evidenciar la efectividad de los controles implementados en el sistema.

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 wiffi, la Institución cuenta con 35 AP y se tiene el Fortiget 800C y en caso de eventualidad el Fortiget 200b. Las subredes de la Institución están segmentadas lógica y físicamente, creación de VLans, 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 el canal de internet para Betlemitas. Actualmente están haciendo un estudio de viabilidad con un proveedor. 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 dese la sede principal se tiene documentado que son ocho subredes: financiera, administración, salas de computo, red wifi, servidores, DMZ, biblioteca y laboratorios.

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 Google, 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.

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 biométrico no contempla una cláusula donde especifique la seguridad y el tratamiento adecuado del registro de huella, 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 confidencialidad donde garantice y refleje 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 Siag que estàn de cara a Internet y se mejoró la gestión de contraseñas mediante el módulo de restauración. Lo relacionado con la protección de transacciones de los servicios se tercerizó a través de un portal que provee el banco de Bogotá 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 (Gabriela y Camila) están autorizados a tomar requerimientos y a emplear el Task manager 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, pese a que cuaqluier personal del área de desarrollo está en capacidad de recibir los

requerimientos. Por lo anterior se sugiere que este procedimiento esté documentado.

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 Doctora Claudia Muñoz 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.

14.1.2 – 14.1.3 Se deben evaluar periódicamente la efectividad de los mecanismos de seguridad que dan cumplimiento a estos controles en todos los sistemas de información (No solo en SIAG) en las transacciones efectuadas en redes públicas.

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 implementarle y de esta manera minimizar el riesgo alguna frente alguna amenaza.

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 Por lo general no se incluye acuerdos o claúsulas de confidencialidad a los contratos con proveedores, el área Tic no tiene definido los requisitos de seguridad de la información al verificar y aplicar en la adquisición de productos y/o servicios de Tecnología de la información y comunicaciones.

15.2.2 No se realizan ajustes o cambios a las claúsulas 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.

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:

16.1.5 – 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.

No conformidades:

16.1.1 – 16.1.2 – 16.1.3 No 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 tampoco son reportados los diferentes eventos de seguridad por los canales apropiados.

16.1.4 Los eventos de seguridad de la información no se evalúan para decidir si se clasifican como incidentes de seguridad.

16.1.6 Frente a un incidente de seguridad no se realiza ningún tipo de análisis posterior, lo que permita reducir la posibilidad o el impacto de incidentes futuros.

Observaciones:

16.1.1 – 16.1.2 – 16.1.3 Se deben establecer procedimientos documentados y responsabilidades en lo que respecta a la seguridad de la información para actuar frente algún incidente de seguridad; así mismo como establecer los canales apropiados para realizar el respectivo reporte.

16.1.4 Es importante que se documente el incidente de seguridad y se evalúe el impacto del mismo para establecer los controles necesarios y medidas preventivas y/o correctivas a tiempo.

16.1.6 Es prioridad luego de algún incidente de seguridad realizar el respectivo análisis del mismo para que se puedan tomar medidas que permitan reducir el impacto o posibilidad de que nuevamente vuelva ha ocurrir.

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. Es importante anotar, que la revisión de éstas políticas se realiza una vez al año generalmente.

No conformidades:

17.2.1 Actualmente las instalaciones de procesamiento de información no presentan la redundancia suficiente para cumplir 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.

18.2.1 Solo se ha realizado un proceso externo para la revisión del aseguramiento, continuidad, educación y eficacia en cuanto a la seguridad de la información.

18.2.2 – 18.2.3 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.

No conformidades:

18.1.1 - 18.1.2 Teniendo en cuenta el enfoque de la Institución, tienen identificados, docuemntados 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 claúsulas 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; ya que el OwnCloud por la capacidad de almcenamiento no es el adecuado.

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

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 que permita salvaguardar los registros, así como definir un procedimiento para el manejo y alamcenamiento de los registros.

18.1.5 Implementar reglamentación de controles criptográficos a las redes de datos e información que se considere crítica.

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	
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.	D16-PLAN_DE_GESTIÓN_DE_RIESGOS_V1.pdf	x		Vigente	Revisar documento y complementar el análisis del contexto.
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	Organigrama_Institucional.docx	x		Vigente	
6	Políticas de seguridad de la información formalizada y firmada	Política, alcance y objetivos de la seguridad de la información.pdf	x		Vigente	
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	D8-_ROLES_Y_RESONSABILIDADES_V1	x		Vigente	La comunidad e involucrados desconocen los lineamientos de seguridad de acuerdo a los roles asignados. La inclusión en el organigrama no se tiene.
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	Anexo 4 Reporte EjecutivoOWASP_SIAG.docx Anexo 5 Reporte Técnico_OWASP_SIAG.docx Reporte Ejecutivo Colmayor OWASP.pdf Reporte Tecnico Colmayor OWASP.pdf	x		No Vigente	Este proceso debe realizarce de manera periódica o anual. El reporte presentado no es Actual.
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	Pendiente por documentar		x	No documentado	
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección	Pendiente por documentar		x	No documentado	
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	D16-PLAN_DE_GESTIÓN_DE_RIESGOS_V1.pdf	x		Vigente	
12	Procedimientos de control documental del MSPI	Pendiente por documentar		x	No documentado	
13	Metodología de Gestión de riesgos	D16-PLAN_DE_GESTIÓN_DE_RIESGOS_V1.pdf	x		Vigente	
14	Riesgos identificados y valorados de acuerdo a la metodología	D16-PLAN_DE_GESTIÓN_DE_RIESGOS_V1.pdf Riesgos.xlxs	x		No Vigente	La ultima identificación y valoración fue en el año 2017.
15	Planes de tratamiento de los riesgos	D16-PLAN_DE_GESTIÓN_DE_RIESGOS_V1.pdf	x		No Vigente	Se sugiere relacionar en este aspecto el documento R20-Matriz de analisis de riesgo de SPI, el cual debe actualizarce dado que la última fecha fue en el año 2017.
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información	Pendiente por documentar		x	No documentado	
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad	P1-_SELECCION_Y_VINCULACION_V8.pdf		x	No documentado	Verificar dado que el documento que relacionan no se encuentra alineado a lo que solicitan
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y	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	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
21	Inventario de áreas de procesamiento de información y telecomunicaciones	Pendiente por documentar		x	No documentado	
22	Diagrama de red de alto nivel o arquitectura de TI	Interconexión_2018_2Semestre.jpg	x		Vigente	
23	Inclusión de la seguridad de la información en la gestión de proyectos	Pendiente por documentar		x	No documentado	
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	Pendiente por documentar		x	No documentado	
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_V1 .xlxs Nota: está pendiente por implementar y registrar los incidentes.	x		Vigente	Se cuenta con el reporte de incidentes emplementado.
28	Plan de continuidad de la Entidad aprobado	P5-_CONTINUIDAD_DE_NEGOCIO_V1.pdf	x		Vigente	
29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la	D8-NORMOGRAMA_TIC_V10.pdf	x		Vigente	
30	Listado de auditorias relacionadas con seguridad de la información realizadas en la entidad	Pendientes por realizar y documentar		x	No documentado	Elaborar un plan de auditoría interna y externa
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.	Pendiente por documentar		x	No documentado	Complementar
32	Indicadores y métricas de seguridad de la información definidos.	3. Indicadores_IUCMC.docx Nota: Está pendiente de aprobación	x		No Vigente	Alinearlo con el documento de indicadores Tic_2019, el cual debe ser actualizado semestralmente.
33	Declaración de aplicabilidad	R21- _FORMATO_DECLARACIÓN_DE_APLICABILIDAD_V1.xlxs	x		Vigente	Revisar el documento de aplicabilidad, en cuanto a la efectividad de los controles propuestos.
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos	D16-PLAN_DE_GESTIÓN_DE_RIESGOS_V1.pdf	x		Vigente	Revisar documento y alinearlo al requerimiento
	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.	Pendiente por documentar		x	No documentado	
36	Avance en la ejecución del plan de tratamiento de riesgos	Pendiente por documentar		x	No documentado	
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	Pendiente por documentar		x	No documentado	
	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	Pendiente por documentar		x	No documentado	
39	Documento con el plan de auditorias internas y resultados, de acuerdo a lo establecido en el plan de auditorías,	Pendiente por documentar		x	No documentado	
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta	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	
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado	Pendiente por documentar		x	No documentado	

En virtud del análisis anterior se evidencia que el 52% de los documentos básicos que soportan el MSPI se encuentran pendiente por documentar, el 38% de la documentación que se tiene se encuentra vigente y un 4% de los documentos están pendiente por ser actualizados.

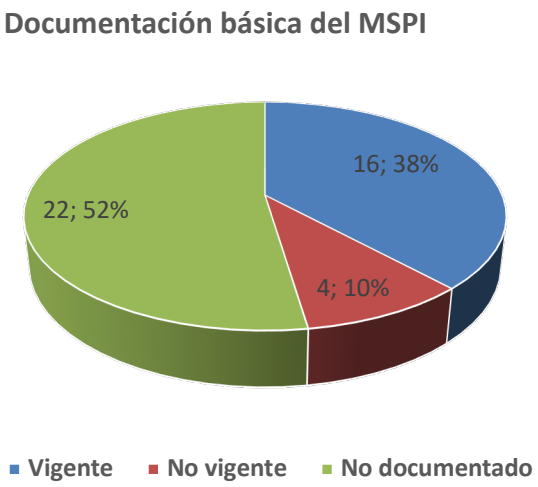


Figura 9. Documentación básica del MSPI

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.

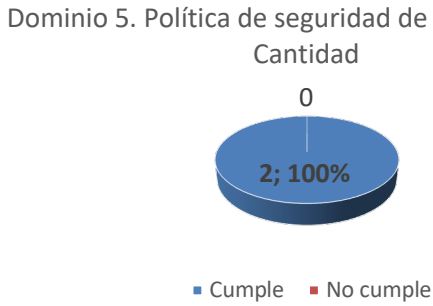


Figura 10. Cumplimiento del dominio 5

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 33%, con relación a 67% de no cumplimiento como se puede evidenciar en la siguiente figura.

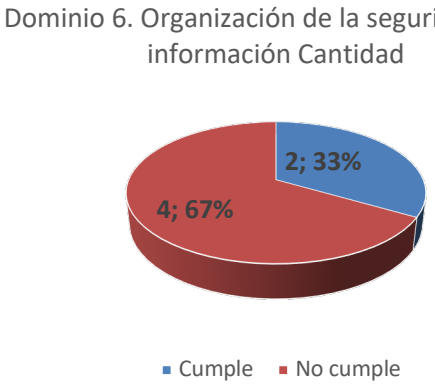


Figura 11. Cumplimiento dominio 6

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 17%, con relación a 83% de no cumplimiento como se puede evidenciar en la siguiente figura.

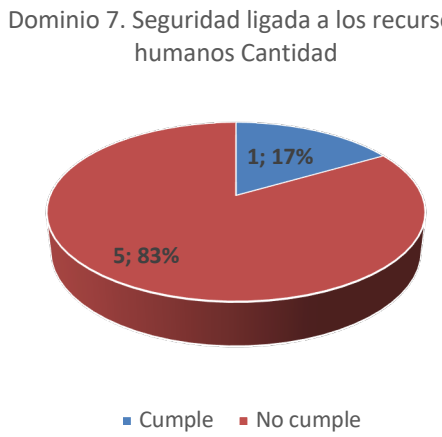


Figura 12. Cumplimiento dominio 7

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.

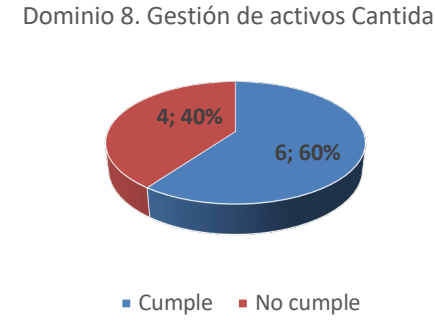


Figura 13. Cumplimiento dominio 8

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 50%, con relación a un 50% de no cumplimiento como se puede evidenciar en la siguiente figura.

Figura 14. 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 50%, con relación a un 50% de no cumplimiento como se puede evidenciar en la siguiente figura.

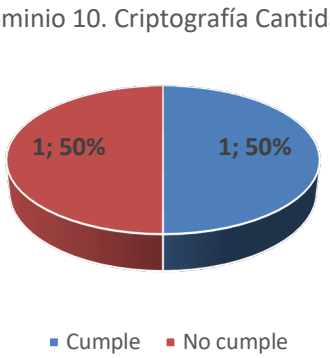


Figura 15. Cumplimiento dominio 10

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 36%, con relación a un 64% de no cumplimiento como se puede evidenciar en la siguiente figura.

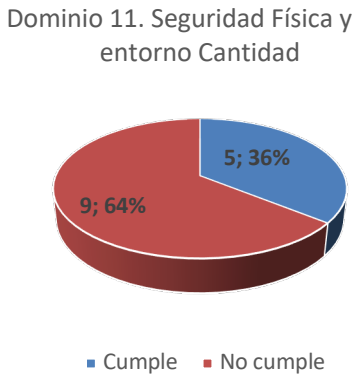


Figura 16. Cumplimiento dominio 11

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 50%, con relación a un 50% de no cumplimiento como se puede evidenciar en la siguiente figura.

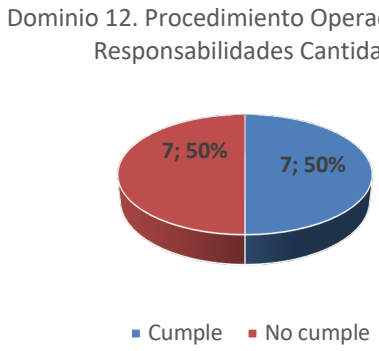


Figura 17. Cumplimiento dominio 12

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.

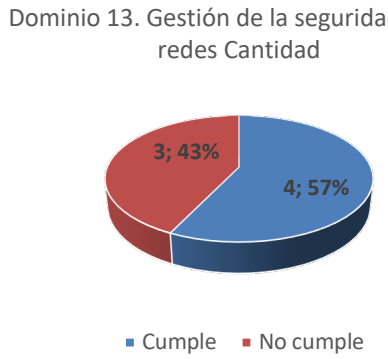


Figura 18. Cumplimiento dominio 13

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.

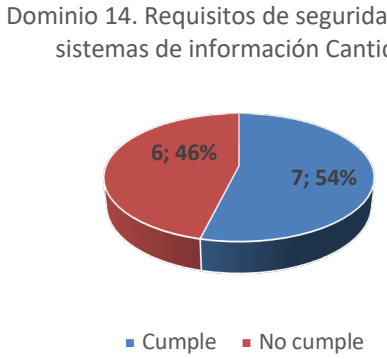


Figura 19. Cumplimiento dominio 14

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.

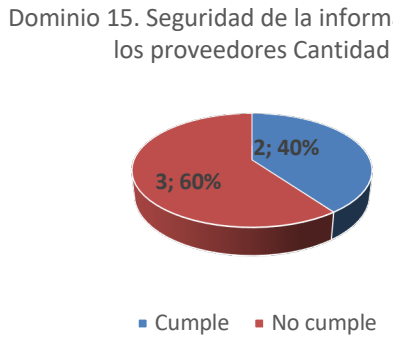


Figura 20. Cumplimiento dominio 15

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 29%, con relación a un 71% de no cumplimiento como se puede evidenciar en la siguiente figura.

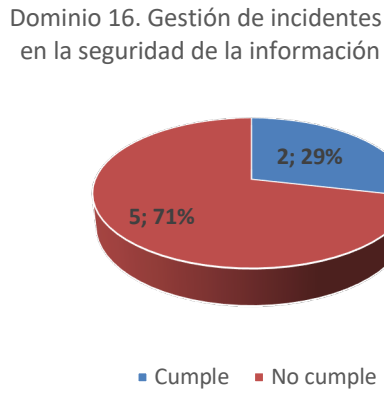


Figura 21. Cumplimiento dominio 16

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.

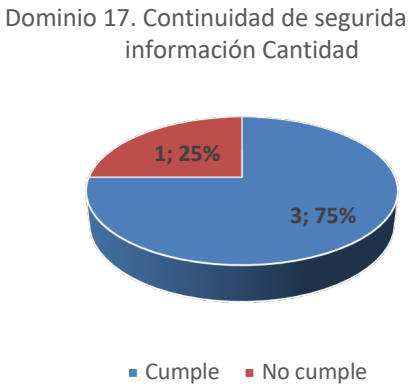


Figura 22. Cumplimiento dominio 17

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 50%, con relación a un 50% de no cumplimiento como se puede evidenciar en la siguiente figura.

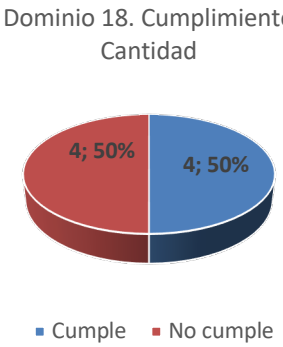
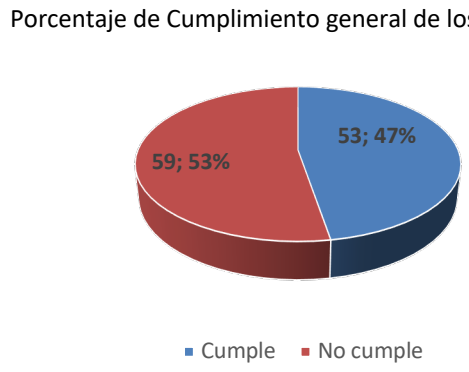


Figura 23. Cumplimiento dominio 18

A manera de conclusión se determina que el único dominio que tiene un cumplimiento de 100% es el dominio 5, siguiendo el dominio 17 con un 75%, el dominio 8 con un 60%, dominio 13 con un 57%, el dominio 14 con un 54%, el dominio 9,10,12 y 18 con un 50% de cumplimiento, el dominio 15 con un 40%, dominio 11 con un 36%, el dominio 6 con un 33%, dominio 16 con un 29% y el dominio 7 con un 17% 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 83%, siguiéndole el dominio 16 con un 71%, el dominio 6 con un 67%, así mismo el dominio 11 con un 64%, y el dominio 15 con un 60%; mientras que los dominios 9,10,12 y 18 presentan un porcentaje de no cumplimiento del 50%, seguidamente con los dominios que tienen un porcentaje menor de no cumplimiento están dominio 14 con un 46%, dominio 13 con un 43%, dominio 8 con un 40%, finalmente el dominio 17 con un 25% de No cumplimiento.

A partir de lo anterior, se concluye que el 47% lo que equivale a 53 controles del estándar ISO/IEC 27001:2013 se encuentran implementados, mientras que el 53% equivalente a 59 controles no están implementados por lo que se requieren acciones de mejora. No obstante es importante mencionar que se excluyeron 2 controles (6.2.2 – 11.1.6), dado a la naturaleza de la organización no aplican.



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: Enero 9 de 2020

Revisado por:
Fecha: Enero 10 de 2020