# INFORME AVANCE PLAN TECNOLÓGICO

Para la vigencia 2017 no fueron asignados recursos por proyecto de inversión para continuar con el proyecto de modernización tecnológica, por este motivo se adelantaron las actividades de ajustes y capacitaciones sobre el plan anual de adquisiciones en los contratos de licenciamiento y soporte.

Como actividades adelantadas se tienen:

SEDE COLEGIO DE LA CGR

- Se acondiciono el cuarto de equipos con la instalación del RACK de servidores y datos.

- Se acondiciono, se cableo y se realizó las conexiones eléctricas de la UPS de 20 KVA para el suministro de energía regulada a las salas de sistemas.

- Se fortalecieron las políticas de navegación y de accesos a la información en las salas de sistemas.

- Se extendió la cobertura de la red inalámbrica del Colegio de la CGR, con la instalación de dos AP y la redistribución de los existentes.

- Actualización del firewall CHECKPOINT.

- Contratación del servicio del software de gestión académica para el colegio de la CGR.

SEDE CENTRO MÉDICO

- Se extendió la cobertura de la red inalámbrica del Centro médico, con la instalación de un AP.

- Actualización del firewall CHECKPOINT.

- Ajuste de la rede de datos con la segmentación de la red de datos.

- Ajuste del software para efectuar conexiones seguras mediante SSL.

SEDE ADMINISTRATIVA

Estudio de vulnerabilidades mediante análisis GAP de las tres sedes;

Ajuste del mapa de riesgos existente.

Configuración de navegación segura de dominio para los aplicativos: ALFANET, CREDITO Y CARTERA y PORTAL INSTITUCIONAL.

Reinstalación de tres servidores conforme se ajusta la infraestructura de la sede administrativa.

Ajuste de la cobertura inalámbrica en la sede administrativa e instalación de servicios sobre servidores CENTOS.

Ajuste de las políticas del dominio fbscgr.local.

Aumento de la capacidad de los correos de la entidad y aseguramiento de la información manejada en el correo.

APP móvil del portal institucional.

Capacitación en el uso del módulo de auditoría del sistema de crédito y cartera, capacitación administrativa de la consola del correero electrónico.

DATACENTER EXTERNO

El DATACENTER externo, se encuentra bajo modificación de infraestructura tanto a nivel lógico como físico. Se adelantaron actividades de reforzamiento de seguridad web, escritorios remotos y optimización de aplicaciones. Todo esto con el fin de mitigar los intentos de accesos a la información que se presentan.

Se ha optimizado las actividades con la modificación de servidores Microsoft a servidores Linux, con el fin de asegurar la correcta protección de la información.

El aumento del tamaño de las bases de datos se ha aumentado el tiempo de generación de los backup´s de aplicaciones, por lo cual se ha requerido de un escalamiento de servicios para asegurar el acceso a la información.

RESULTADOS DEL ANÁLISIS GAP

| | | Determinación de Controles existentes | | Matriz de análisis de Riesgos | | | |
|---|---|---|---|---|---|---|---|
| | **RIESGOS** | **¿EXISTE ALGUN CONTROL?** | **¿ES LO MÁS APROPIADO?** | **PROBABILIDAD** | **IMPACTO** | **NIVEL DE RIESGO** | TRATAMIENTO SUGERIDO |
| A | Incumplimiento de los acuerdos establecidos en los pliegos de contratación por parte de los proveedores y contratistas. | SI | Si, ya que existe un supervisor experto en el área para revisar el cumplimiento de los acuerdos establecidos. | 5 | 5 | 25 | Ejecución de los Acuerdos de Nivel de Servicios o las sanciones contempladas en la ley 80 referente a contratación estatal, Se realiza la mitigación del riesgo. |
| B | Demoras en la gestión por parte de la administración en los trámites requeridos por el área de sistemas. | NO | No, este punto demuestra falta de relevancia para la administración de los trámites por parte de la administración | 5 | 5 | 25 | Aplicabilidad del manual de contratación de la entidad, Se realiza la mitigación del riesgo. |
| C | Disminución de la ǀasignación de porcentaje del presupuesto asignado por parte de la Contraloría General de la República. | SI | Es el único control implementarle. | 5 | 7 | 35 | Redistribución de los recursos asignados a los proyectos de inversión y registro de nuevos proyectos ante el DNP, Se realiza la mitigación del riesgo a través del manejo de proyectos de inversión. |
| D | Aumento de la cartera morosa. | SI | Se hace seguimiento en el área de cartera con el fin de realizar su recuperación y disminuir este índice. | 5 | 5 | 25 | Ejecución de las cláusulas a los morosos con el fin de recuperar esta cartera. Se realiza la mitigación del riesgo, esta actividad corresponde al área financiera y al grupo de cartera de la entidad. |
| E | Disminución de los aportes entregados por los funcionarios. | SI | No, porque no se puede aplicar un control sobre el manejo de los aportes que | 3 | 5 | 15 | Redistribución de fondos de funcionamiento. Se realiza la mitigación del riesgo. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | cada funcionario quiera entregar. | | | | |
| F | Robo de información por parte de los funcionarios. | SI | Se encuentra bloqueado la copia de cd y dvs, la información del sistema financiero se encuentra restringida a registro y acceso, más sin embargo el acceso por usb se encuentra habilitado, por lo tanto se vulnera la seguridad de la información al momento que los funcionarios se llevan los datos para continuar con su trabajo fuera de las instalaciones de la entidad. | 10 | 7 | 70 | Restricción de los medios de almacenamiento mediante bloqueos de periféricos. Revisión de la información substraída con el fin de determinar las implicaciones del robo. Se realiza la mitigación del riesgo con el ajuste de los sistemas de dominio y antivirus con el fin de implementar restricciones de dispositivos USB y la presentación de políticas de manejo de la información generada, entregada y manipulada en la entidad. |
| G | Traslado de archivos en medios extraíbles | NO | | 10 | 7 | 70 | Instalación de software de monitoreo de los equipos y bloqueo de accesos a USB, Se realiza la mitigación del riesgo. |
| H | Substracción de equipos. | SI | Se realiza la revisión y solicitud de autorizaciones por parte de la empresa de vigilancia contratada por la entidad. | 3 | 5 | 15 | Revisión del sistema de cámaras de seguridad y registro de acceso con el fin de determinar la ruta por la cual los equipos fueron retirados de las instalaciones, con base en esta información identificar a los implicados con el fin de aplicar las correspondientes medidas. Se realiza la mitigación del riesgo. |
| I | Terremotos | NO | | 3 | 10 | 30 | Se transfiere el riesgo. Mediante las pólizas de seguros. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| J | Tormentas eléctricas. | NO | | 5 | 5 | 25 | De acuerdo con la intensidad empezar la secuencia de apagado de equipos con el fin de evitar daños en la infraestructura de comunicaciones como en los equipos del FONDO DE BIENESTAR SOCIAL DE LA CGR. Se realiza la mitigación del riesgo. |
| K | Incendios. | NO | | 5 | 10 | 50 | Se realizó la solicitud a la administración para contratar la implementación de sistema de aviso y extinción de incendios. Se realiza la mitigación del riesgo con la solicitud que se dirigió a la gerencia de la entidad y la dirección administrativa y financiera. |
| L | Cambios a la normatividad en los procesos de contratación. | NO | | 3 | 3 | 9 | Realizar la correspondiente revisión de la normatividad modificada con el fin de verificar el impacto sobre los procesos existentes y si resultan ser afectados aplicar correctivos necesarios. Se acepta el riesgo. |
| M | Caída de los servidores | SI | Se realiza el registro de los eventos en el formato de operación de los servidores y se hace la corrección del evento, si es de hardware se adelanta el trámite de solicitud de soporte al contratista de mantenimiento y si es de software se realiza la revisión y el debido a acompañamiento por parte del proveedor de las aplicaciones montadas en los servidores | 10 | 10 | 100 | Utilizar el protocolo de mantenimiento referente al proceso de respaldo en cuanto a caída de servidores. Se realiza la mitigación del riesgo a través de la contratación de empresas de apoyo tanto para los sistemas Windows, Linux, bases de datos y demás sistemas implementados en los servidores. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| N | Ataques de virus, troyanos, gusanos y spyware. | SI | Se actualiza el antivirus y se mantienen parchados los sistemas a través de las consolas | 5 | 5 | 25 | Dependiendo de la severidad del ataque y la vulnerabilidad de los sistemas ejecutar rutinas de contención y utilización de antivirus con el fin de eliminar la infección o realizar su contención hasta lograr eliminarla de los equipos. Se realiza la mitigación del riesgo. |
| O | Mal diseño de la red de datos. | SI | No, porque se está utilizando software que no es el más funcional. | 3 | 3 | 9 | Revisión del plano lógico de la red de datos y diseñar los correctivos para solventar la falla en la transmisión de datos. Se realiza la mitigación del riesgo. |
| P | Desbalanceo de las cargas de la red eléctrica. | SI | No, porque no hay un sistema de monitoreo en la red eléctrica y se realizan reasignación de personal y áreas sin contar con el estudio previo de distribución de cargas. | 5 | 5 | 25 | Identificar la fuente del desbalanceo de cargas y redistribuirlas a fin de evitar caídas en el sistema. De presentarse caídas iniciar la secuencia de encendido para identificar la fuente del desbalanceo y corregirlo mediante el balanceo de cargas sobre el tablero eléctrico. Se realiza la mitigación del riesgo. |
| Q | Desactualización de manuales y planes de contingencia | NO | | 10 | 5 | 50 | Revisión de los procesos e identificación de las falencias de los manuales y los planes de contingencia de cada proceso con el fin de asegurar la continuidad del negocio, de no existir ni el manual ni el plan de contingencia este debe ser desarrollado. Se realiza la mitigación del riesgo. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| R | Sabotaje a la red. | NO | | 10 | 5 | 50 | Identificar la procedencia del sabotaje, determinar si es a nivel lógico o físico, si es a nivel lógico realizar el seguimiento del tráfico a través del software de monitoreo e identificar los alcances del sabotaje con base en estos alcances determinar la acción a tomar. Si es a nivel físico realizar la investigación debida para identificar a las personas implicadas y determinar la acción a ser tomada. En cualquier caso, se debe realizar un análisis para determinar las acciones correctivas para evitar futuros sabotajes. Se realiza la mitigación del riesgo. |
| S | Descontento de los funcionarios | NO | | 5 | 5 | 25 | Realizar reuniones de concertación e identificar las causas y posibles fuentes de desconcierto para tomar medidas correctivas, que pueden ir desde la modificación de funciones hasta el nivel de investigación interna con sus debidas implicaciones. Se realiza la mitigación del riesgo. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| T | Penetración indebida | SI | Se registra a través del acceso de firewall y con políticas de auditoria sobre los recursos compartidos del servidor. | 5 | 5 | 25 | Identificar el punto de acceso y determinar el grado de complicidad de los diversos funcionarios, con base en estos hechos realizar el proceso de investigación interna con las debidas implicaciones que esto conlleva, paralelamente se debe dar parte a las autoridades y entes de control, para identificar a los participantes en la acción y realizar el debido proceso legal, de igual forma se debe identificar las intenciones de dicha acción. Se debe verificar si el acceso fue consecuencia de un punto de acceso desprotegido y corregir dicha situación. Se realiza la mitigación del riesgo. |
| U | Cambio de las actividades establecidas en el manual de procesos. | NO | | 3 | 3 | 9 | Se debe realizar el ajuste de las normas de seguridad a las nuevas actividades, de ser necesario se deben ajustar las normas de seguridad a actividades o procesos nuevos. Se realiza la mitigación del riesgo. |
| V | Pérdida de la información almacenada tanto en medio físico como en medio magnético y óptico. | SI | A través de la consola antivirus, generación de backups y atención de solicitudes de recuperación. | 10 | 7 | 70 | Identificar la causa y de ser posible la restauración de la información de las copias de seguridad. Se realiza la mitigación del riesgo. |
| W | Falta de compromiso de los funcionarios responsables de las áreas en las cuales se utilizan los sistemas de información de la entidad | NO | | 5 | 10 | 50 | Se debe adelantar reuniones de concientización sobre la importancia del manejo adecuado de la información e identificar las posibles falencias en los procesos y determinar la responsabilidad de los funcionarios en el proceso, se mitiga este riesgo. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| X | Comunicaciones informales sobre el manejo y acceso a la información sin la debida documentación requerida ni el registro pertinente | NO | | 5 | 10 | 50 | Se debe realizar el registro de toda información proveniente desde y hacia las áreas con el fin de poder medir la trazabilidad existente. Se debe realizar el registro en el sistema de gestión documental o a través de correos electrónicos, se mitiga este riesgo. |
| Y | Manejo indebido de los backup generados | NO | | 10 | 10 | 100 | Se generara un documento para el manejo de los backup´s de igual manera se realizará las pruebas de eficiencia y se verificará la salvaguarda de dichas copias de respaldo, se mitiga el riesgo. |
| Z | Ingreso por parte de los funcionarios a páginas web no autorizas | SI | Se realiza un seguimiento de las páginas no autorizadas, más sin embargo hace falta definir la acción pertinente al momento de presentarse reiteración en el acceso de páginas web o contenido no autorizado o con contenido no relevante para el desarrollo de las actividades al interior de la entidad. | 5 | 5 | 25 | Se aplican bloqueos a través del sistema firewall y sistema antivirus, de persistir el acceso indebido se procederá con el informe de esta situación a la dirección administrativa y financiera de la entidad, se mitiga ese riesgo. |
| AA | Ejecución de software portable en la red de la entidad | SI | Existen restricciones desde las gpo implementadas en la red y en el sistema antivirus de la entidad. Más sin embargo hace falta definir la acción pertinente al momento de presentarse reiteración en la ejecución de aplicativos portables. | 5 | 5 | 25 | Se bloquea el acceso y ejecución de medios portables. Se mitiga este riesgo. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AB | Préstamo indebido de contraseñas token´s | SI | El control del uso de este elemento toke´n o certificado de firma digital se encuentra asignado mediante acuerdo firmado por el funcionario ante CERTICAMARA S.A. De existir algún fallo o vulnerabilidad en este uso la responsabilidad recae enteramente en el funcionario que tiene asignado el toke´n o certificado de firma digital. | 10 | 7 | 70 | Como responsabilidad de los usuarios finales de los toke´s, contraseñas cuentas de usuarios se realizara un comunicado para dar a conocer los riesgos del préstamo y las implicaciones que conlleva esta actividad, se mitiga el riesgo. |
| AC | Debilidad en las contraseñas del aplicativo ALFANET | NO | | 10 | 3 | 30 | Se solicitara al administrador del aplicativo el refuerzo de la seguridad de contraseñas, se mitiga este riesgo. |
| AD | El sistema ALFANET no se está utilizando por parte de los funcionarios de la entidad | NO | | 10 | 5 | 50 | Se solicita a los funcionarios que manejan el sistema ALFANET la realización de capacitaciones y talleres de utilización del aplicativo con el fin de implementar las políticas de cero papel al interior de la entidad y sus sedes externas. |
| AE | La clasificación por organigrama dentro del aplicativo ALFANET no ha sido alimenta de forma adecuada | NO | | 10 | 3 | 30 | Se solicita al administrador del aplicativo ALFANET el registro correcto de las dependencias y los niveles de accesos requeridos, se mitiga este riesgo. |
| AF | implementado la política de cero papel | NO | | 10 | 7 | 70 | Se solicita al líder de implementación de GEL, los avances correspondientes, se mitiga este riesgo. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AG | Retraso de los procesos de contratación del área de sistemas | NO | | 10 | 7 | 70 | Este riesgo a pesar de ser identificado y de cumplir con los trámites al interior de la entidad solo se puede mitigar con el apoyo de la dirección administrativa y financiera y el apoyo del comité de contratación. |
| AH | No obtener la revisión ni aprobación de los procedimientos externos para las solicitudes Departamento Nacional de planeación | NO | | 10 | 7 | 70 | Generar los documentos en las fechas estipuladas y entregar al área de planeación para que adelante los trámites pertinentes. Este riesgo se Mitiga. |
| AI | Falta de avance en la implementación en la estrategia de Gobierno en Línea | NO | | 10 | 10 | 100 | Solicitar a los Lideres de GEL y las profesionales de cada grupo el avance de las actividades estipuladas, Este riesgo se Mitiga. |
| AJ | Falta de personal de apoyo, No hay suficiente personal en el área de sistemas, esto implica una exceso en carga laboral de la persona del área, | NO | | 10 | 10 | 100 | Solicitar un mayor número de personal para el área de sistemas, Este riesgo se Mitiga. |
| AK | Manejo de información descentralizada | NO | | 10 | 10 | 100 | Verificar la aplicabilidad de la norma de usabilidad e igualdad tecnológica contemplada en GEL |
| AL | Aplicativo del Centro médico, sin una persona a cargo que tenga los conocimientos tanto de sistemas de información como manejo de aplicativos de salud y atención a pacientes | NO | | 10 | 10 | 100 | Es necesario aplicar la normatividad vigente en cuento a la implementación de GEL en la entidad |
| AM | No existe una diferenciación en cuanto administración manejos, operatividad y funcionalidad de los aplicativos | NO | | 10 | 10 | 100 | Es necesario establecer el nivel de jerarquías y responsabilidades en los aplicativos, se recomienda el cumplimiento de la NTC/ISO 27000 y sus subsidies |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AN | Centralización sobre el área de sistemas de los procedimientos, referentes en los aplicativos de la entidad | NO | | 10 | 10 | 100 | No existe un documento que defina los roles administrativos, operativos, funcionales, auditoria ni manejo de la información, la centralización sobre una única persona va en contra de las normas vigentes en la actualidad, de igual manera es un alto riesgo mantener en una sola persona todo el control de los aplicativos |

Como resultado de los análisis y actividades adelantadas se tiene:

1. Es necesario desagregar las actividades de seguridad, manejo de información, soporte, infraestructura, administración de software y avances TIC´s en varias designaciones.

2. Se requiere entrara a reconfigurar en la sede Colegio de la CGR la red y las políticas con el fin de asegurar una mejor operación de los equipos.

3. Fortalecer el uso de la gestión electrónica de documentos

4. Fortalecer el almacenamiento, gestión de información y manejo de las copias de seguridad de los archivos contenidos en los discos duros de los equipos de la entidad.

5. Fomentar el conocimiento del manejo responsable de la información por parte de los usuarios finales, esto con el fin de mitigar la pérdida de datos o la modificación de los mismos.

Al realizar el análisis de la información de los informes presentados por el área de sistemas se tiene como resultados:

TRANSPARENCIA

(Busca facilitar el acceso a la información pública de manera permanente y permitir su aprovechamiento por parte de los usuarios ciudadanos y grupos de interés)

80

Se han abierto canales de comunicación a través del portal institucional y la información se ha publicado conforme se ha generado en cada área y dependiendo del impacto ya sea a la ciudadanía o las beneficiarias de los programas.se puede verificar en la información publicada en noticias de las tres sedes, normatividad y participación ciudadana en los subsitios del portal

COLABORACION

(Busca facilitar el acceso a la información pública de manera permanente y permitir su aprovechamiento por parte de los usuarios)

90

Se han abierto canales de comunicación a través del portal institucional y la información se ha publicado conforme se ha generado en cada área y dependiendo del impacto ya sea a la ciudadanía o las beneficiarias de los programas.se puede verificar en la información publicada en noticias de las tres sedes, normatividad y participación ciudadana en los subsitios del portal. La información se masifica mediante el uso del correo institucional tanto para la CGR como para el FBS,

PARTICIPACION

(promover la participación, conocer e involucrar a los usuarios en el que hacer público)

75

Se realizan convocatorias para la participación ciudadana y se ha habilitado el correo rendicióndecuentas@fbscgr.gov.co, el correo fondobienestar@fbscgr.gov.co con el fin de darle tramite a la solicitud de información y con el fin de brindar respuesta se realiza el proceso de radicación del correo con el fin de registrarlo en el sistema de gestión documental para adelantar el seguimiento de respuestas en el informe de PQRD´S

SERVICIOS CENTRADOS EN EL USUARIO

(Los usuarios cuentan con una oferta de trámites, servicios y espacios de comunicación a través de canales electrónicos usables y accesibles que responden a sus necesidades y expectativas)

80

Se han habilitado accesos a los aplicativos mediante enlaces web desde el portal institucional, los sistemas de información como lo son el sistema de crédito y cartera, ALFANET, Gestión Médica el mismo portal permiten la interacción de los beneficiarios de los programas con la entidad con el fin de interactuar y presentar la información con la disponibilidad que requiere el beneficiario final.

Links:

www.fbscgr.gov.co

https://alfanet.fbscgr.gov.co/alfanet

https://tao.fbscgr.gov.co/ords/f?p=102:LOGIN_DESKTOP::::::

https://salud.fbscgr.gov.co/patients/

en el link

https://www.fbscgr.gov.co/nuestros_servicios

https://www.fbscgr.gov.co/salud/nuestros_servicios

Se encuentran los servicios disponibles para los beneficiarios de los programas del FBS.

SISTEMA INTEGRADO PETICIONES, QUEJAS, RECLAMOS Y DENUNCIAS (PQRD) (Los usuarios cuentan con múltiples canales que operan de forma integrada, para la atención de peticiones, quejas, reclamos y denuncias)

90

El sistema de PQRD¨S se encuentra en los link´s:

https://www.fbscgr.gov.co/tools/marco.php?idcategoria=2062

https://www.fbscgr.gov.co/tools/marco.php?idcategoria=3941

El cual es revisado mediante las alarmas por la persona encargada en atención al usuario con el fin de redirigir las solicitudes presentadas de manera electrónica. Se realiza un seguimiento a estas solicitudes desde el informe de PQRD´S, también se ejerce un control desde la misma área de atención al usuario con el fin agilizar las respuestas a las solicitudes.

TRAMITES Y SERVICIOS EN LINEA

(Los usuarios cuentan con múltiples canales que operan de forma integrada, para la atención de peticiones, quejas, reclamos y denuncias)

100

Se han implementado accesos web a las aplicaciones mediante los links

www.fbscgr.gov.co

https://alfanet.fbscgr.gov.co/alfanet

https://tao.fbscgr.gov.co/ords/f?p=102:LOGIN_DESKTOP::::::

https://salud.fbscgr.gov.co/patients/

ESTRATEGIA DE TI

(Busca aportar valor al desarrollo sectorial e institucional de las entidades a través de una estrategia de TI)

50

El avance de la estrategia se tenía vinculado a un proyecto de inversión el cual no cuenta con recursos en la vigencia 2017 ni 2018, más se adelantaron actividades de ajustes de aplicaciones, apertura de aplicaciones y servicios con el apoyo de las áreas involucradas en los trámites de crédito, cartera, gestión documental y gestión médica. Se capacito a los funcionarios en el uso de hermanitas del correo corporativo, se realizó ajuste de infraestructura con el fin de asegurar la información almacenada y procesada por el FBS.

GOBIERNO DE TI

(Busca aportar valor al desarrollo institucional y/o sectorial a través de la implementación de esquemas de gobernabilidad de TI, alineados a los procesos y procedimientos de la entidad.)

30

Se ha iniciado con el proceso de estudio de las directrices de gobierno digital, a la fecha se adelanta el análisis de información para presentar las opciones de implementación a la alta gerencia.

INFORMACION

(Busca aportar valor estratégico a la toma de decisiones a partir de la gestión de la información como un producto y servicio de calidad)

80

La información generada por las áreas como por los servicios misionales son fuente para la toma de decisiones en la entidad, el análisis del área de crédito asegura la correcta asignación de recursos, la asignación de recursos en los programas misionales permite el mejor aprovechamiento de los mismos ya que se realiza un estudio a través de las realimentaciones presentadas por los beneficiarios con el fin de mejorar los servicios.

SISTEMAS DE INFORMACION

(Busca potenciar los procesos y servicios que presta la entidad a través de la gestión de los sistemas de información)

70

Los sistemas de información de crédito y cartera, el sistema de gestión documental y el sistema de gestión médica permiten un análisis de información y de interacción entre los beneficiarios de los servicios y el FBS, mediante el uso de TIC´s para ampliar la cobertura y realizar un seguimiento de los procesos adelantados en los aplicativos.

SERVICIOS TECNOLOGICOS

(Busca gestionar la infraestructura tecnológica que soporta los sistemas, los servicios de información y la operación de la entidad.)

90

Las plataformas tecnológicas se encuentran en constante actualización ya sea de infraestructura o de software, este último mediante el uso de consolas de gestión para adelantar un análisis de recursos y hacer los ajustes pertinentes para beneficiar las actividades de los procesos misionales de la entidad.

USO Y APROPIACION

(Busca realizar actividades orientadas al desarrollo de competencias TI y vincular los diversos grupos de interés en las iniciativas TI)

80

Se adelantaron capacitaciones en el uso del correo institucional y las herramientas Enterprise de la nueva versión, con el personal de atención al usuario y correspondencia, personal de archivo se adelantó el ajuste del aplicativo ALFANET para permitir una interacción más amigable con los usuarios finales. Para el aplicativo de crédito y cartera se adelantó una capacitación en el uso de la herramienta de auditoría para el personal de control interno, con el fin de verificar las acciones realizadas en el aplicativo por los usuarios funcionales.

CAPACIDADES INSTITUCIONALES

(Busca desarrollar capacidades institucionales para la prestación de servicios a través de la automatización de procesos y procedimientos y la aplicación de buenas prácticas de TI)

20

Se inició con el proceso de estudio de una nueva aplicación para los servicios misionales que permitan la comunicación con los beneficiarios de programas y reduzcan los tiempos de procesamiento de información.

DEFINICION DEL MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Y DE LOS SISTEMAS DE INFORMACION

(Busca definir el estado actual del nivel de seguridad y privacidad y define las acciones a implementar)

65

Se realizó el diagnóstico de la entidad con el cual se establecen los controles para mitigar los riesgos y las acciones encaminadas para su implementación.

IMPLEMENTACION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Y DE LOS SISTEMAS DE INFORMACION

(Busca desarrollar las acciones definidas en el plan de seguridad y privacidad.)

50

Se realizó el diagnóstico de la entidad con el cual se establecen los controles para mitigar los riesgos y las acciones encaminadas para su implementación.

MONITOREO Y MEJORAMIENTO CONTINUO

(Busca desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información.)

50

Se realizó el diagnóstico de la entidad con el cual se establecen los controles para mitigar los riesgos y las acciones encaminadas para su implementación.

Cuadro avance plan tecnológico:

| EJES | | Descripción avance | Proyectado | Avance |
|---|---|---|---|---|
| HARDWARE | Adquirir equipos, renovación tecnológica | Se realizó el cambio de equipos de dos sedes | 150 equipos | 87 Equipos |
| | Mantenimiento y ajuste de equipos | Se ajustó el cuarto de equipos del colegio y toda la infraestructura que existía | Una Infraestructura ajustad | Una Infraestructura ajustad |
| SOFTWARE | Ajuste de aplicativos | Se han ajustado 4 aplicativos | Mediante ajustes de rutinas, seguridad mejorada, certificado SSL comunicaciones y contingencia modificada | Se ajustarón los aplicativos instalados en el DATACENTER |
| | Adquisición de aplicativos | Se ha adelantado es estudio para la adquisición de un aplicativo para los | Dos aplicaciones | Una aplicación en estudio |

| | | | | |
|---|---|---|---|---|
| | | servicios misionales. | | |
| PERSONAS | Capacitaciones | Se adelantaron capacitaciones a los funcionarios de la sede administrativa | Un ciclo de capacitación | Capacitación en seguridad<br><br>Capacitación de ALFANET<br><br>Capacitación de herramientas correo electrónico |

## INFORME DE SEGURIDAD

a) Realización Mantenimiento: se realizó el mantenimiento de primer nivel de los equipos y software.

Sede administrativa: Debido a las amenazas mundiales fue necesario implementar un plan de choque general y restrictivo, se eliminaron las carpetas compartidas de los servidores ya que exponían a la red y la información contenida en los equipos a una amenaza crítica, asociada con la vulnerabilidad de intercambio de información a nivel de protocolo SMB.

| Sede | Número de infecciones | Mitigadas | Impacto | Resultado | Fallas de políticas | Fallas debidas a usuarios |
|---|---|---|---|---|---|---|
| Administrativa | 10 | 10 | 0 | 0 | NO | SI |
| Centro médico | 0 | 0 | 0 | 0 | NO | NO |
| Colegio CGR | 20 | 20 | 0 | 0 | NO | SI |

b) Realización de BACKUP´S: Para generar los BACKUP´S del DATACENTER externo se detiene el ambiente de producción y se clonan las máquinas virtuales existentes una vez al mes, semanalmente se realizan BACKUP´S de las bases de datos de los aplicativos con el fin de mitigar el impacto en caso de presentarse una amenaza sobre los servidores del FBS

Es necesario aclarar que el BACKUP´S se debe generar en la sede externa ya que a la fecha se está centralizando los recursos de DATACENTER en esta sede con el fin de lograr una administración centralizada de los recursos web y de aplicaciones. Las copias de seguridad de los usuarios deben programarse, más se han encontrado las siguientes fallas provocadas por los usuarios finales.

- No se atienden la recomendación básica de no crear carpetas, subarpetas y nombres largos en los archivos, esto hace vulnerables los archivos e imposibilita la realización de copias de respaldo.

- Desorden, no hacen un correcto uso de las TRD, es conocido por el manejo documental de los documentos físicos que se requiere un manejo en espejo de los archivos digitales, los funcionarios no hacen caso de la recomendación del AGN.

- Existen archivos de carácter personal en los discos duros de la entidad, los funcionarios hacen copias de respaldo de sus archivos personales en los equipos del FBS.

Con el fin de mitigar los riesgos el área de sistemas se encuentra en proceso de montar una herramienta automatizada de copias de respaldo, esto se realiza con software GNU, con lo cual no se infringen derechos de autor, más para adelantar estas actividades es necesario; en este trimestre se planteó el ajuste mediante GOOGLESYNC y drive para automatizar las copias en todas las sedes con su almacenamiento en la nube. Se ha realizado las pruebas con la herramienta de sincronización del sistema operativo Windows 10 para la generación automática de backup

- Es necesario actualizar las TRD de las áreas, por parte de sistemas se ha enviado correos al comité de archivo realizando recomendaciones y solicitando las actualizaciones debidas, a la fecha este comité no se ha reunido ni se ha tenido respuesta.

- Es necesario crear las carpetas de manejo documental digital en los equipos e computo, pero previo a esta actividad el comité de archivo debe socializar la política de manejo electrónico de documentos solicitada por el AGN y el MINTIC, se ha creado un almacenamiento centralizado para los archivos digitales con ayuda del área de archivo para optimizar los recursos a la hora de verificar la información.

- Es necesario modificar la infraestructura de la red del FBS a nivel administrativo, esto con el fin de asegurar la programación de copias, respaldo de las mismas y almacenaje de los medios de grabación. En la actualidad no se cuenta con un espacio de archivo digital, este archivo debe cumplir con las condiciones técnicas específicas. En la sede actual no se puede llevar a cabo estas modificaciones. Para adelantar estos ajustes es necesario activar una unidad de almacenamiento con sistema Linux para mitigar riesgos de propagación de virus y amenazas al momento de realizar estas copias.

- No se ha realizado una capacitación en manejo electrónico de documentos a los funcionarios del FBS. Esto es necesario ya que no se podría unificar el criterio de manejo si no se han impartido las bases de conocimiento a los funcionarios. Para formalizar el proceso es necesario adelantar un estudio de ajuste sobre las políticas de manejo de archivo electrónico

- Es necesario validar los controles de cada área a sus archivos digitales,

c) Actualización de aplicativos, mediante las consolas de sistema operativo, antivirus y aplicativos base se envían diariamente las diversas actualizaciones de seguridad a todos los equipos de la sede centro, en el colegio y centro médico la descarga es

directa ya que no se puede realizar administración de la red, de igual forma al momento de realizar el mantenimiento de hardware se complementa con la actualización de los aplicativos si los equipos cuentan con conexión a internet. Se adelantó esta actualización en las tres sedes de manera independiente ya que la instalación de los canales de internet modifico el direccionamiento de las sedes y saco de servicio las políticas de intercambio entre las sedes, se encuentra en proceso de ajuste para integrar las sedes nuevamente.

d) Impacto por violación de políticas de seguridad,

| Sede | Políticas antivirus | Políticas seguridad navegación | Políticas de red | Políticas de actualización | Fallas de políticas |
|---|---|---|---|---|---|
| Administrativa | 10 | 8 | 5 | 10 | 2 % |
| Centro médico | 0 | 4 | 5 | 10 | 1 % |
| Colegio CGR | 20 | 10 | 5 | 10 | 20 % |

Sede administrativa; Se tiene un porcentaje de fallas en políticas de un 2%, esto debido en su mayoría a fallas en la seguridad debido al uso de software portable almacenado en USB, fallas de actualización de la aplicación java. Se procede con el fortalecimiento de políticas de actualizaciones desde los servidores y de forma presencial, por este motivo en cuanto se envían nuevos boletines del fabricante del software se procede con la revisión y aplicación de actualizaciones, es necesario aclarar que se está sacrificando la disponibilidad de los equipos porque los procesos de instalación de actualizaciones en algunos casos exceden las dos horas.

Centro médico, 1% Las fallas presentadas se deben a los permisos especiales de navegación que existen para las conexiones remotas, hay que recordar que abrir puertos de software de videoconferencias acarrea un riesgo el cual se mitiga más no puede llevarse a cero debido al intercambio de información que se requiere. Se procede con el fortalecimiento de políticas de actualizaciones desde los servidores y de forma presencial, por este motivo en cuanto se envían nuevos boletines del fabricante del software se procede con la revisión y aplicación de actualizaciones, es necesario aclarar que se está sacrificando la disponibilidad de los equipos porque los procesos de instalación de actualizaciones en algunos casos exceden las dos horas.

Colegio de la CGR, 20% Debido a la propia naturaleza educativa, el nivel de violaciones de políticas de seguridad es alto, se maneja una mitigación sobre la red administrativa para evitar propagaciones de virus en la red o pérdida de información. Se procede con el fortalecimiento de políticas de actualizaciones desde los servidores y de forma presencial,

por este motivo en cuanto se envían nuevos boletines del fabricante del software se procede con la revisión y aplicación de actualizaciones, es necesario aclarar que se está sacrificando la disponibilidad de los equipos porque los procesos de instalación de actualizaciones en algunos casos exceden las dos horas.

e) Con base en los establecido en la ley 1273 de 2009, la NTC 5254 y la NTC-ISO 2700 las cuales determinan el manejo de la información de medios digitales, niveles de acceso a la información en equipos de usuarios finales, servidores y manejo de riesgos informáticos, se presenta la necesidad de establecer los roles y alcances de cada administrador, en la actualidad la oficina de sistemas cumple estas funciones sobre los siguientes aplicativos:

- ✓ WINDOWS SERVER instalados en la sede administrativa.
- ✓ Portal institucional cuyo hosting se encuentra en un servidor externo a la entidad.
- ✓ Cuentas de correo electrónico. Servidor externo
- ✓ Software Oracle 10 G – 11G motor de base de datos del sistema financiero y Nómina.

En estos aplicativos y software se cumplen con las actividades de creación de usuarios, revisión de conectividad, definición de políticas de acceso. Sistema Financiero se verifica la conexión y el funcionamiento del software Oracle, a Nivel operativo cada módulo como lo es el de contabilidad, cartera, crédito, tesorería asociados y global corresponde a cada responsable de área según el módulo tiene la potestad de solicitar modificaciones sobre los usuarios toda vez sean aprobadas la Gerencia del Fondo de Bienestar Social de la CGR.

- ✓ Portal institucional se hace la administración de usuarios en cuanto a bloqueos, el ingreso de información se realiza cumpliendo los requisitos establecidos en el SICME. Y con la aprobación de los editores de la entidad y diligenciamiento del formato de publicaciones. Se contrató el hosting del portal institucional de la entidad y la habilitación de los niveles de restricciones con el contrato de mantenimiento del portal institucional. Se realizó el cambio de portal, en este momento se encuentra en proceso de estabilización.

- ✓ Actividades GEL; No se ha reunido el comité de GEL de la entidad.

  Es necesario realizar el PESI y el PETI de la entidad, más este documento debe ser generado por el comité GEL y su líder de implementación.

Los aplicativos de gestión médica, ALFANET, de gestión académica DIAMANTE y SIGEP local son administrados por los responsables de cada sede y el profesional de talento Humano, debido al tipo de información que se maneja en cada uno de ellos. Ya que en la actualidad no hay ninguna designación en el área de sistemas que soporte dicha asignación en cumplimiento con la normatividad vigente en el País. Es necesario definir el funcionario de nivel directivo el cual le sean asignadas las funciones de encargado de seguridad y manejo de la información.

| APLICATIVO | ADMINISTRACIÓN |
|---|---|
| SIGEP (LOCAL) | Profesional ESP G14, Talento Humano |
| ALFANET | Atención al usuario |
| GESTIÓN MÉDICA | Directora de desarrollo y Bienestar |
| PORTAL INSTITUCIONAL | Directora de desarrollo y Bienestar |
| TAO | Directora administrativa y Financiera |
| DIRECTORIOS ACTIVOS | Profesional Esp G.14 sistemas |
| CORREO ELECTRÓNICO | Profesional Esp G.14 sistemas |
| ANTIVIRUS | Profesional Esp G.14 sistemas |
| SISTEMAS CHECKPOINT | Profesional Esp G.14 sistemas |
| DIAMANTE | Rectora Colegio CGR |

En la entidad dentro de la planta no se cuenta con un Director de Tecnologías y Sistemas de Información, el cual se encuentra establecido en el decreto 415 del 7 de marzo de 2016. Se recomienda realizar la revisión de las funciones del líder GEL con el fin de asignar las funciones establecidas por este decreto en el líder GEL.

## ACTIVIDADES DE MITIGACIÓN AMENAZAS

En la actualidad se ha desatado una tormenta de amenazas que aprovechan las vulnerabilidades propias de los sistemas MICROSOFT, por lo cual en las tres sedes se ha debido implementar nuevos servidores y migrar a versiones 2012 la arquitectura que soporta las redes del FBS, en la actualidad cada instalación requiere de al menos una semana por servidor virtual, más tres entre estabilización entrada en producción sincronización y afinación para las necesidades de cada sede. En el DATACENTER externo debido a la imposibilidad de atender 7/24 estos equipos es necesario realizar BACKUP´S

de aplicaciones de manera más recurrente, pero esto repercute en la disponibilidad de aplicativos, los tiempos de BACKUP´S exceden las dos (2) Horas, tiempo en el cual los aplicativos no son accesibles. Estos BACKUP´S deben ser ejecutados en horas de oficina ya que se debe coordinar con los proveedores de aplicaciones, proveedor del DATACENTER y asegurar el acceso desde las sedes administrativa y centro médico, para asegurar la respuesta ante alguna falla es necesario destinar tres horas para generar las copias de respaldo, se está modificando el proceso de la siguiente manera:

1. Mensualmente generar un EXPORT de máquinas, tres (3) horas de indisponibilidad
2. Semanalmente generar EXPORT de las bases de datos, se realiza por aplicación por lo cual el tiempo requerido no es fácilmente determinable.

No es posible salvaguardar los archivos de los funcionarios en este momento, se sigue utilizando el procedimiento establecido, pero los tiempos exceden un mes para generar las copias de los equipos de la sede administrativa sin contar las copias del centro médico ni del Colegio. Se iniciará un proceso de generación de una carpeta de BACKUP´S en cada equipo con el fin de arrastrar los archivos de trabajo de las áreas, esta actividad requiere de una SAN en cada sede, más se procederá con una implementación temporal con los elementos disponibles en la entidad.

FONDO DE BIENESTAR SOCIAL
CONTRALORÍA GENERAL DE LA REPÚBLICA
NIT. 800.252.683-3

# INVENTARIO DE INFORMACIÓN FONDO DE BIENESTAR SOCIAL DE LA CGR

| Nombre de la información | Descripción | Área responsable de la información | Tipología de información | Ámbito geográfico | Idioma | Fuente primaria | Evidencia de solicitud | Tipo de información / origen | Frecuencia de generación de la información | Formato | Frecuencia de actualización |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Portal Institucional - PORTAL | El portal de Internet del Fondo de Bienestar Social de la Contraloría General de la Republica de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados con la Entidad. Incluye: enlaces a las aplicaciones que se administran | Oficina de Comunicaciones | Servicios y Beneficios | Nacional e Internacional | Español / Ingles | Fuente primaria | Estado - Contraloría - Ciudadanía | Digital | Diaria | pdf, doc,xls,csv,wms,zip,Html, css,Java scrip | Quincenal |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | dentro del Fondo, foros, documentos información misional y demás ; está dirigido resolver necesidades de información especifica | | | | | | | | | | |
| INTRANET | La intranet del Fondo de Bienestar Social de La Contraloría General de la Republica es el sitio web que ofrece a los funcionarios de la Entidad, información de manera fácil e íntegra, permitiendo el acceso a una serie de recursos y de servicios relacionados con la Entidad. Temas de interés a los funcionarios | Oficina de Comunicaciones | Institucional y de Interés para los funcionarios | Nacional | Español | Fuente primaria | Funcionarios de la Entidad | Digital | Diaria | pdf, doc,xls,csv,wms,zip,Html, css,Java scrip | Diaria |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Correo electrónico | Servicio de red que permite a los usuarios enviar y recibir correos electrónicos | Oficina de Sistemas e Informática | Oficial | Nacional e Internacional | Español | Fuente primaria | Servicio | Digital | Permanente | Texto | Permanente |
| Plan Estratégico | Almacena el avance de las acciones asociadas al Plan de Acción del FBS | Oficina de Planeación | Gestión | Nacional | Español | Fuente primaria | Administrativa | Manual - Documento Físico | Trimestral | XLS | Trimestral |
| PMI | Plan de Mejoramiento Institucional PMI - Almacena el avance de las actividades que buscar mitigar los hallazgos encontrados por los diferentes entes que nos realizan auditoria y que se plasman en un plan de mejoramiento | Oficina de Planeación | Gestión | Nacional | Español | Fuente primaria | Entidad Pública | Documento Físico / Manual | Mensual | XLS | Mensual |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Plan de Manejo de riesgos | Almacena el avance de las actividades que buscan mitigar los riesgos encontrados y que hacen parte del manejo de riesgo institucional | Oficina de Control Interno: Realiza el seguimiento; el registro lo realizan cada dependencias responsables de la actividad | Gestión | Nacional | Español | Fuente primaria | Administrativa | Documento Físico / Manual | Mensual | XLS | Mensual |
| Alfanet | Sistema de Gestión Documental: Es un sistema lógico que permite radicar documentos recibidos, registrar documentos enviados, realizar trámites, gestión, archivo y consulta de los documentos | Atención Al Usuario | Documental | Nacional | Español | Fuente primaria | Interna / Externa | Físico / Digital | Diaria | TIF, pdf, excel, word | Automático |
| Nomograma | Almacena la información sobre la normatividad que rige a la Entidad | Oficina de Planeación | Gestión | Nacional | Español | Fuente primaria | Interna / Externa | Documento Físico / Manual | Mensual | doc/txt | Mensual |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SICME | Sistema Integrado de Control de Calidad - Control de Documentos Internos del Sistema de Control de Calidad | Oficina de Planeación | Gestión | Nacional | Español | Fuente primaria | Interna / Externa | Documento Físico / Manual | Mensual | doc/txt | Mensual |
| Boletín Ingresos y Egresos | Sistema de apoyo al FBS para el control de los ingresos y egresos diarios. Apoyo al proceso contable | Dirección Administrativa y Financiera | Gestión | Nacional | Español | Fuente primaria | Entidad Pública | Documento Físico / Manual | Cada Hora | Bases de Datos | Diaria |
| Portal - Sitio WEB | Es el aplicativo donde muestra los servicios y beneficios ofrecidos por el FBS a los funcionarios | Sistemas | Gestión | Nacional | Español | Fuente primaria | Entidad Pública | Audiovisual | Semanal | HTML | Semanal |
| SIGEP | Aplicativo para la administración del sistema de talento Humano de la planta de personal del FBS | Talento Humano | Talento Humano | Nacional | Español | Fuente primaria | Interna / Administrativa | Documento Físico / Digital | Diaria | pdf, papel, archivos planos | Diaria |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PQR | Sistema de Información que permite registrar las solicitudes de quejas, derechos de petición, denuncias, etc | Atención Al Usuario | Gestión | Nacional | Español | Fuente primaria | PQR | Digital / Físico | Diaria | Bases de Datos | Diaria |
| TAO | Aplicativo para la gestión de créditos y cartera | Dirección Administrativa y Financiera | Gestión | Nacional | Español | Fuente primaria | Interna / Administrativa | Digital | Diaria | Bases de Datos | Diaria |

ANÁLISIS GAP

## Estado actual controles

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

## Estado actual requisitos

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

| Anexo A de referencia | Título de control | Descripción del control | Función | Status | Hallazgos |
|---|---|---|---|---|---|
| A.5 | Políticas de seguridad de la información | | | | |
| 5.1 | Directrices de la Dirección en seguridad de la información. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 5.1.1 | Conjunto de políticas para la seguridad de la información | Existe un documento. Más se requiere su actualización a la nueva plataforma | | MD | Está documentado, se pone en práctica pero falta la formalización |
| 5.1.2 | Revisión de las políticas para la seguridad de la información | No se ha realizado la revisión por parte de la alta gerencia | | MD | Está documentado, se pone en práctica pero falta la formalización |
| A.6 | Aspectos Organizativos De La Seguridad De La Información | | | | |
| 6.1 | Organización interna. | | | | |
| 6.1.1 | Asignación de responsabilidades para la segur. de la información | No existe una | | RD | El control está diseñado pero no se ajusta a la norma |

| | | | | | |
|---|---|---|---|---|---|
| | | designación formal de estas responsabilidades | | | |
| 6.1.2 | Segregación de tareas | | | RD | No se realiza mediante medios convencionales |
| 6.1.3 | Contacto con las autoridades | | | RD | No está establecido |
| 6.1.4 | Contacto con grupos de interés especial | | | MD | |
| 6.1.5 | Seguridad de la información en la gestión de proyectos. | No existe | | MD | |
| 6.2 | Dispositivos para movilidad y teletrabajo. | | | | |
| 6.2.1 | Política de uso de dispositivos para movilidad | | | RD | |
| 6.2.2 | Teletrabajo | En formulación | | RD | Aunque existe una política del estado Colombiano, en la entidad no se ha establecido el proceso, ni mucho menos los controles |
| A.7 | SEGURIDAD LIGADA A LOS RECURSOS HUMANOS | | | | |
| 7.1 | Antes de la contratación. | | | | |
| 7.1.1 | Investigación de antecedentes | | | MD | Depende de recursos humanos y no se tiene claridad si se hace o no |
| 7.1.2 | Términos y condiciones de contratación. | | | MD | Depende de recursos humanos y no se tiene claridad si se hace o no |
| 7.2 | Durante la contratación | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 7.2.1 | Responsables de gestión | | | D | |
| 7.2.2 | Concienciación, educación y capacitación en seguridad de la información. | | | RD | No está establecido |
| 7.2.3 | Proceso disciplinario | | | RD | Depende dejuridica y no se tiene claridad si se hace o no |
| 7.3 | Cese o cambio de puesto de trabajo. | | | | |
| 7.3.1 | Cese o cambio de puesto de trabajo. | | | RD | No se hace |
| A.8 | Gestión de activos | | | | |
| 8.1 | Responsabilidad sobre los activos | | | | |
| 8.1.1 | Inventario de activos. | | | MD | |
| 8.1.2 | Propiedad de los activos | | | MD | |
| 8.1.3 | Uso aceptable de los activos. | | | MD | El control se diseñó, se aplica pero no se alinea con la norma |
| 8.1.4 | Devolución de activos. | | | MD | no se utiliza |
| 8.2 | Clasificación de la información | | | | |
| 8.2.1 | Directrices de clasificación. | | | RD | El control se diseñó y aplica, pero no está ajustado del todo con la norma |
| 8.2.2 | Etiquetado y manipulado de la información | | | RD | El control se diseñó y aplica, pero no está ajustado del todo con la norma |
| 8.2.3 | Manipulación de activos | | | RD | El control se diseñó y aplica, pero no está ajustado del todo con la norma |
| 8.3 | Manejo de los soportes de almacenamiento | | | | |
| 8.3.1 | Gestión de soportes extraibles | | | RD | |

| | | | | | |
|---|---|---|---|---|---|
| 8.3.2 | Eliminación de soporte | | | PNP | no se hace |
| 8.3.3 | Soportes físicos en transito | | | RD | no se hace seguimiento |
| A.9 | Control de accesos | | | | |
| 9.1 | Requisitos de negocio para el control de accesos. | | | | |
| 9.1.1 | Política de control de accesos | | | MD | |
| 9.1.2 | Control de acceso a las redes y servicios asociados. | | | MD | |
| 9.2 | Gestión de acceso de usuario. | | | | |
| 9.2.1 | Gestión de altas/bajas en el registro de usuarios. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 9.2.2 | Gestión de los derechos de acceso asignados a usuarios. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 9.2.3 | Gestión de los derechos de acceso con privilegios especiales. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 9.2.4 | Gestión de información confidencial de autenticación de usuarios. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 9.2.5 | Revisión de los derechos de acceso de los usuarios. | | | RD | |
| 9.2.6 | Retirada o adaptación de los derechos de acceso | | | MD | Falta formalizar la política |
| 9.3 | Responsabilidades del usuario | | | | |
| 9.3.1 | Uso de información confidencial para la autenticación | | | MD | |

| | | | | | |
|---|---|---|---|---|---|
| 9.4 | Control de acceso a sistemas y aplicaciones. | | | | |
| 9.4.1 | Restricción del acceso a la información. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 9.4.2 | Procedimientos seguros de inicio de sesión. | | | MD | |
| 9.4.3 | Gestión de contraseñas de usuario. | | | MD | |
| 9.4.4 | Uso de herramientas de administración de sistemas. | | | MD | |
| 9.4.5 | Control de acceso al código fuente de los programas. | | | NA (Not Applicable) | |
| A.10 | Cifrados | | | | |
| 10.1 | Controles criptográficos | | | | |
| 10.1.1 | Política de uso de los controles criptográficos | | | RD | No se trabaja controles criptográficos |
| 10.1.2 | Gestión de claves | | | RD | No se trabaja controles criptográficos |
| A.11 | Seguridad física y ambiental | | | | |
| 11.1 | Areas seguras | | | | |
| 11.1.1 | Perímetro de seguridad física. | | | MD | |
| 11.1.2 | Controles físicos de entrada. | | | MD | |

| | | | | | |
|---|---|---|---|---|---|
| 11.1.3 | Seguridad de oficinas, despachos y recursos. | | | MD | Hasta ahora estan conformando el equipo que maneja la seguridad de oficinas |
| 11.1.4 | Protección contra las amenazas externas y ambientales. | | | MD | |
| 11.1.5 | El trabajo en áreas seguras. | | | MD | |
| 11.1.6 | Áreas de acceso público, carga y descarga | | | MD | |
| 11.2 | Seguridad de los equipos | | | | |
| 11.2.1 | Emplazamiento y protección de equipos. | | | RD | |
| 11.2.2 | Instalaciones de suministro. | | | RD | |
| 11.2.3 | Seguridad del cableado. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 11.2.4 | Mantenimiento de los equipos. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 11.2.5 | Salida de activos fuera de las dependencias de la empresa. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 11.2.6 | Seguridad de los equipos y activos fuera de las instalaciones. | | | RD | |
| 11.2.7 | Reutilización o retirada segura de dispositivos de almacenamiento. | | | RD | no hay un proceso establecido para esto |
| 11.2.8 | Equipo informático de usuario desatendido. | | | RD | |

| | | | | | |
|---|---|---|---|---|---|
| 11.2.9 | Política de puesto de trabajo despejado y bloqueo de pantalla | | | MD | |
| A.12 | SEGURIDAD EN LA OPERATIVA | | | | |
| 12.1 | Responsabilidades y procedimientos de operación | | | | |
| 12.1.1 | Documentación de procedimientos de operación. | | | PNP | No existe |
| 12.1.2 | Gestión de cambios. | | | RD | |
| 12.1.3 | Gestión de capacidades. | | | RD | |
| 12.1.4 | Separación de entornos de desarrollo, prueba y producció | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 12.2 | Protección contra código malicioso | | | | |
| 12.2.1 | Controles contra el código malicioso | | | RD | |
| 12.3 | Copias de seguridad | | | | |
| 12.3.1 | Copias de seguridad de la información | | | MD | |
| 12.4 | Registro de actividad y supervisión | | | | |
| 12.4.1 | Registro y gestión de eventos de actividad. | | | MD | |
| 12.4.2 | Protección de los registros de información. | | | RD | no se ha establecido |

| | | | | | |
|---|---|---|---|---|---|
| 12.4.3 | Registros de actividad del administrador y operador del sistema. | | | RD | no hay seguimiento ni control ni procedimiento |
| 12.4.4 | Sincronización de relojes | | | MD | No se realiza formalmente |
| 12.5 | Control de software en explotación | | | | |
| 12.5.1 | Instalación del software en sistemas en producción | | | MD | |
| 12.6 | Gestión de la vulnerabilidad técnica | | | | |
| 12.6.1 | Gestión de las vulnerabilidades técnicas. | | | MD | |
| 12.6.2 | Restricciones en la instalación de software | | | MD | |
| 12.7 | Consideraciones de las auditorías de los sistemas de información | | | | |
| 12.7.1 | controles de auditoría de los sistemas de información | | | MD | |
| A.13 | Seguridad en las telecomunicaciones | | | | |
| 13.1 | Gestión de la seguridad en las redes | | | | |
| 13.1.1 | Controles de red. | | | MD | Hasta ahora van a comenzar su formulación |
| 13.1.2 | Mecanismos de seguridad asociados a servicios en red. | | | MD | |
| 13.1.3 | Segregación de redes | | | MD | |

| | | | | | |
|---|---|---|---|---|---|
| 13.2 | Intercambio de información con partes externas | | | | |
| 13.2.1 | Políticas y procedimientos de intercambio de información. | | | RD | |
| 13.2.2 | Acuerdos de intercambio. | | | RD | |
| 13.2.3 | Mensajería electrónica. | | | RD | |
| 13.2.4 | Acuerdos de confidencialidad y secreto. | | | RD | No están formalizados a pesar de que existe un documento. Solo en contadas ocasiones los trabajan |
| A.14 | Adquisición, desarrollo y mantenimiento de sistemas | | | | |
| 14.1 | Requisitos de seguridad de los sistemas de información | | | | |
| 14.1.1 | Análisis y especificación de los requisitos de seguridad. | | | MD | |
| 14.1.2 | Seguridad de las comunicaciones en servicios accesibles por redes públicas | | | MD | |
| 14.2 | Seguridad en los procesos de desarrollo y soporte | | | | |
| 14.2.1 | Política de desarrollo seguro de software. | | | RD | No existe |
| 14.2.2 | Procedimientos de control de cambios en los sistemas. | | | RD | No existe |
| 14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | | | RD | No existe |

| | | | | | |
|---|---|---|---|---|---|
| 14.2.4 | Restricciones a los cambios en los paquetes de software. | | | MD | |
| 14.2.5 | Uso de principios de ingeniería en protección de sistemas. | | | MD | |
| 14.2.6 | Seguridad en entornos de desarrollo. | | | RD | No existe |
| 14.2.7 | Externalización del desarrollo de software. | | | MD | No existe |
| 14.2.8 | Pruebas de funcionalidad durante el desarrollo de los sistemas. | | | RD | |
| 14.2.9 | Pruebas de aceptación. | | | RD | |
| 14.3 | Daños de prueba | | | | |
| 14.3.1 | Protección de los datos utilizados en pruebas | | | MD | |
| A.15 | RELACIONES CON SUMINISTRADORES | | | | |
| 15.1 | Seguridad de la información en las relaciones con suministradores | | | | |
| 15.1.1. | Política de seguridad de la información para suministradores. | | | RD | |
| 15.1.2 | Tratamiento del riesgo dentro de acuerdos con suministradores | | | RD | |
| 15.1.3 | Cadena de suministro en tecnologías de la información y comunicaciones | | | RD | |
| 15.2 | Gestión de la prestación del servicio por suministradores | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 15.2.1 | Supervisión y revisión de los servicios prestados por terceros. | | | RD | |
| 15.2.2 | Gestión de cambios en los servicios prestados por terceros | | | RD | |
| A.16 | Gestión de incidentes de seguridad de la información | | | | |
| 16.1 | Gestión de incidentes de seguridad de la información y mejoras | | | | |
| 16.1.1 | Responsabilidades y procedimientos. | | | MD | |
| 16.1.2 | Notificación de los eventos de seguridad de la información. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 16.1.3 | Notificación de puntos débiles de la seguridad. | | | MD | |
| 16.1.4 | Valoración de eventos de seguridad de la información y toma de decisiones | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 16.1.5 | Respuesta a los incidentes de seguridad. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 16.1.6 | Aprendizaje de los incidentes de seguridad de la información. | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 16.1.7 | Recopilación de evidencias | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| A.17 | Aspectos de seguridad de la información dentro de la continuidad del negocio | | | | |
| 17.1 | Continuidad de la seguridad de la información | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 17.1.1 | Planificación de la continuidad de la seguridad de la información | | | MD | El control se realiza pero falta su documentación formal. Está alineado con la norma |
| 17.1.2 | implantación de la continuidad de la seguridad de la información. | | | RD | |
| 17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | | | RD | |
| 17.2 | Redundancias | | | | |
| 17.2.1 | Disponibilidad de instalaciones para el procesamiento de la información | | | RD | |
| A.18 | Cumplimiento | | | | |
| 18.1 | Cumplimento de los requisitos legales y contractuales | | | | |
| 18.1.1 | Identificación de la legislación aplicable. | | | MD | |
| 18.1.2 | Derechos de propiedad intelectual (DPI). | | | MD | Hay un control que no cumple con las normas. Debe ser rediseñado |
| 18.1.3 | Protección de los registros de la organización. | | | MD | |
| 18.1.4 | Protección de datos y privacidad de la información personal. | | | MD | El control se realiza, pero falta su documentación formal. Está alineado con la norma y las leyes y políticas existentes en el país |
| 18.1.5 | Regulación de los controles criptográficos | | | RD | no existe |
| 18.2 | Revisiones de la seguridad de la información | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 18.2.1 | Revisión independiente de la seguridad de la información. | | | RD | no existe |
| 18.2.2 | Cumplimiento de las políticas y normas de seguridad. | | | RD | no existe |
| 18.2.3 | Comprobación del cumplimiento | | | RD | no existe |

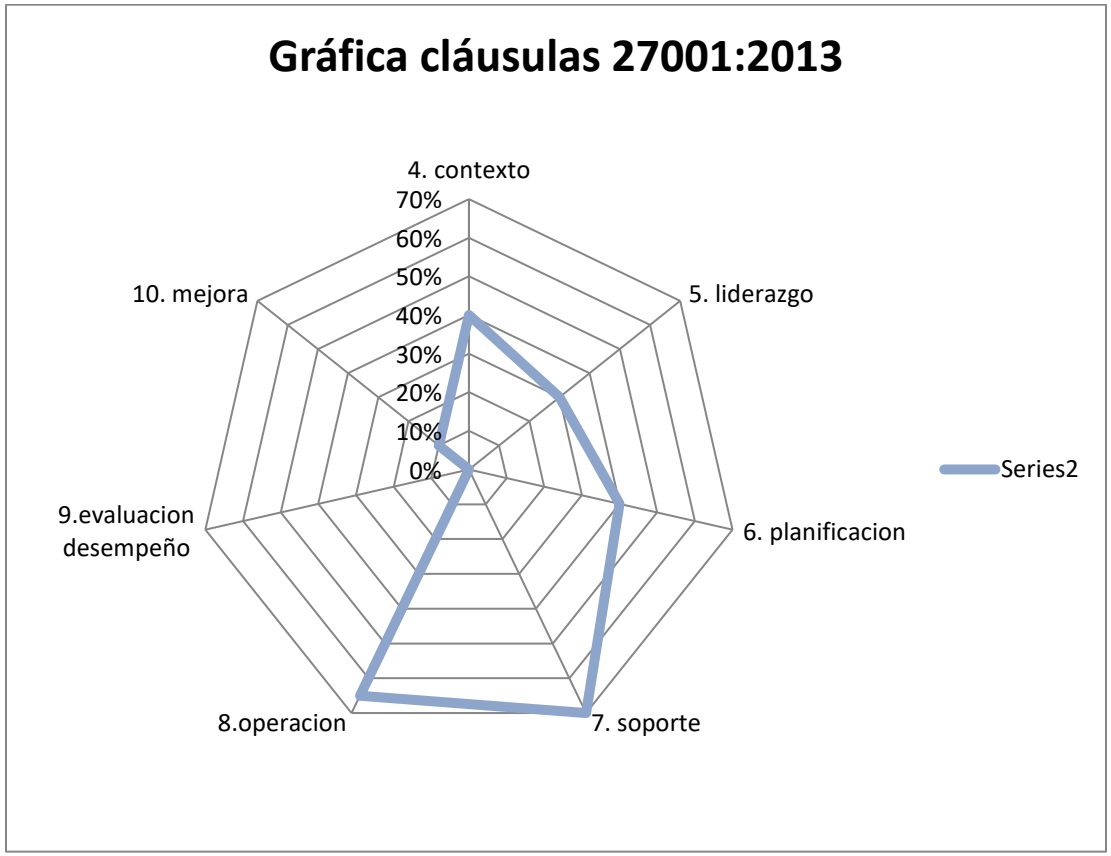
## Estado implementación 27001 contra clausulas (cláusulas en D)

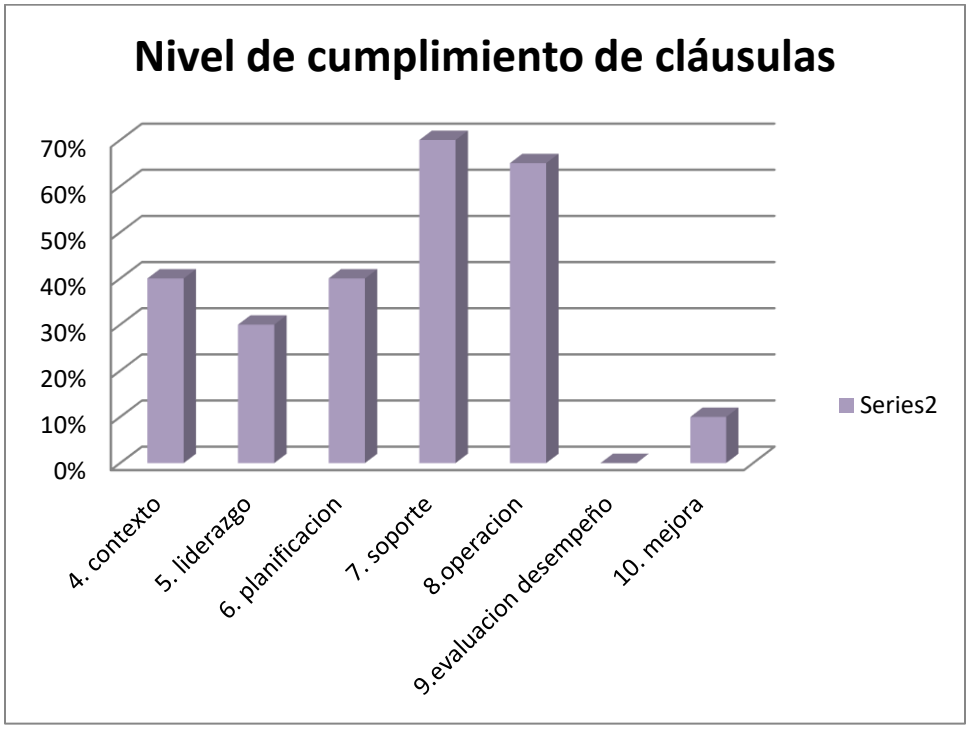
| Clausulas ISO | Cantidad | Conformidad % | Meta |
|---|---|---|---|
| 4.1.Conocimiento de la organización y de su contexto | 0 | 0 | 100% |
| 4.2. Comprensión de las necesidades y expectativas de las partes interesadas | 0 | 0 | 100% |
| 4.3. Determinación del alcance del SGSI | 0 | 0 | 100% |
| 5.2. Política | 0 | 0 | 100% |
| 6.1. Acciones para tratar riesgos y oportunidades | 0 | 0 | 100% |
| 6.2. Objetivos de seguridad de la información y planes para lograrlos | 0 | 0 | 100% |
| 7.1. Recursos: se debe determinar y proporcionar los recursos | 0 | 0 | 100% |
| 7.2. Competencia | 0 | 0 | 100% |
| 7.3. Toma de conciencia | 0 | 0 | 100% |
| 7.4. Comunicación | 0 | 0 | 100% |
| 7.5. Información documentada | 0 | 0,00 | 100% |
| 8.1. Planificación y control operacional | 0 | 0 | 100% |

| | | | |
|---|---|---|---|
| 8.2. Evaluacion de riesgos según los criterios establecidos en 6.1.2 (a) | 0 | 0 | 100% |
| 8.3. Tratamiento de riesgos de la seguridad de la información | 0 | 0 | 100% |

**Estado actual requisitos**

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


Gráfica cláusulas 27001:2013
4. contexto
70%
60%
50%
40%
30%
20%
10%
0%
5. liderazgo
6. planificacion
7. soporte
8.operacion
9.evaluacion desempeño
10. mejora
Series2


Nivel de cumplimiento de cláusulas
70%
60%
50%
40%
30%
20%
10%
0%
4. contexto
5. liderazgo
6. planificacion
7. soporte
8.operacion
9.evaluacion desempeño
10. mejora
Series2

**GRÁFICA RADIAL CONTROLES ANEXO A 27002:2013**

## GRÁFICO DE BARRAS PORCENTAJE CUMPLIMIENTO DOMINIOS ANEXO A