CONTROL				Evaluación	Valor	Total	Justificación de la valoración
A.5 Politica de seguridad de la información						80,00%	
	A.5.1 Directrices de la dirección en seguridad de la información					80,00%	
		A.5.1.1	Conjunto de políticas para la seguridad de la información	4 - Gestionado	80%		Las políticas de seguridad de la información se han establecido y documentado. Pero se encuentra en proceso la propagación de la documentación.
		A.5.1.2	Revisión de las políticas para la seguridad de la información	4 - Gestionado	80%		Existe un procedimiento de Revisión de las políticas de seguridad por parte de la Dirección de forma periódica. Sin embargo, no hay registro de revisiones de las políticas hasta este momento.
A.6 Organización de la seguridad de la información						53,00%	
	A.6.1 Organización interna					56,00%	
		A.6.1.1	Asignación de responsabilidades para la segur. de la información	3 - Definido	60%		Se han definido, asignado y documentado los roles y las responsabilidades para la seguridad de la información. Pero los usuarios todavía no tienen claro el canal de notificación.
		A.6.1.2	Segregación de tareas	3 - Definido	60%		Hay unos procedimientos de gestión de autorizaciones a la información que facilitan que no se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización. Debe mejorarse porque hay solicitudes aprobadas por la misma persona y no por el director de área.
		A.6.1.3	Contacto con las autoridades	3 - Definido	60%		La dirección y el responsable de seguridad tienen los contactos apropiados sobre la autoridad pertinente en materia de seguridad con la que se debería contactar en caso de sufrir algún tipo de ataque. Hay documentación asociada al respecto.
		A.6.1.4	Contacto con grupo de especial interés	2 - Repetible	40%		El contacto con grupos de interés no se encuentra formalmente definido, aunque el responsable de seguridad está en contacto con grupos de interés u asociaciones profesionales especializados en seguridad.
		A.6.1.5	Seguridad de la información en la gestión de proyectos.	3 - Definido	60%		Existe un proceso formal de gestión de proyectos en el cual se contemplan los requisitos de seguridad de la información.
	A.6.2 Dispositivos móviles y teletrabajo					50,00%	
		A.6.2.1	Políticas de dispositivos móviles	3 - Definido	60%		Las medidas de seguridad para la protección contra los riesgos de la utilización de dispositivos móviles están documentada, se cuenta con una política formalmente definida.
		A.6.2.2	Teletrabajo	2 - Repetible	40%		Los usuarios conocen el uso que deben realizar sobre la información a la que se accede, trata o almacenada en emplazamientos de teletrabajo. Falta mejorarse estableciendo procedimientos y manuales al respecto.
A.7 Seguridad de recursos humanos						80,00%	
	A.7.1 Antes de empleo					80,00%	
		A.7.1.1	Investigación de antecedentes	4 - Gestionado	80%		Existe un procedimiento formalmente definido para la selección del personal donde se contemplan los aspectos de seguridad de la información. La responsabilidad es de la dirección y de recursos humanos.
		A.7.1.2	Términos y condiciones de empleo	4 - Gestionado	80%		En los términos y condiciones del contrato de trabajo se reflejan las políticas de seguridad de la organización en forma de documento de confidencialidad. Al empleado se le procura informar sobre el tratamiento que deben dar a la información en materia de seguridad.
	A.7.2 Durante el empleo					80,00%	
		A.7.2.1	Responsabilidades de gestión	4 - Gestionado	80%		Los empleados y contratistas conocen las normas en la gestión del trabajo. Se ha establecido la responsabilidad de la alta dirección en relación con el liderazgo en la gestión de seguridad de la información. Se efectúan reuniones de seguimiento y sensibilización por parte de la alta dirección.

		A.7.2.2	Conciencia de seguridad de la información y entrenamiento	4 - Gestionado	80%		Se cuenta con un programa de capacitación y sensibilización para todos los empleados, sobre la importancia de la seguridad de la información en la organización.
		A.7.2.3	Procedimiento disciplinario	4 - Gestionado	80%		Existe un procedimiento disciplinario documentado y acorde a los requisitos legales, en el cual se contemplan los incidentes relacionados con la protección de la información.
	A.7.3 Finalización del empleo o cambio en el puesto de trabajo					80,00%	
		A.7.3.1	Responsabilidades ante la finalización o cambio	4 - Gestionado	80%		Existe un procedimiento publicado y aprobado para el cambio de responsabilidades o terminación de empleo. Recursos humanos contempla las medidas de seguridad para la terminación o cambio de empleo. Pero no se efectúa medición o mejora.
A.8 Gestión de activos						63,00%	
	A.8.1 Responsabilidad de los activos					75,00%	
		A.8.1.1	Inventario de activos	4 - Gestionado	80%		Existe un inventario de los activos asociados a la información y a los recursos para el tratamiento de la información. Cuneta con un procedimiento que evidencia la actualización del inventario.
		A.8.1.2	Propiedad de los activos	4 - Gestionado	80%		La propiedad de los activos de información del inventario está documentada, y se dispone de evidencia con respecto al conocimiento de los propietarios y su responsabilidad.
		A.8.1.3	Uso aceptable de los activos	3 - Definido	60%		Los usuarios son conscientes del uso responsable de la información y de los activos de la organización. Se cuenta con una política de uso aceptable de activos, divulgada a todo el personal de la empresa.
		A.8.1.4	Retorno de los activos	4 - Gestionado	80%		Existe control por parte de la organización y compromiso por parte de los empleados, una vez finaliza el empleo o acuerdo para devolver los activos de la organización. Existe un documento o procedimiento de desvinculación estipulado en el contrato y que es un requisito legal para la empresa.
	A.8.2 Clasificación de la información					66,67%	
		A.8.2.1	Clasificación de la información	4 - Gestionado	80%		La dirección ha aprobado una política y un procedimiento de clasificación de la información. Hay evidencia de la medición del control y de mejora a través del tiempo.
		A.8.2.2	Etiquetado de la información	3 - Definido	60%		La información es etiqueta por la persona responsable de informática pero faltan procedimientos para efectuar dicha etiquetación.
		A.8.2.3	Manipulado de la información	3 - Definido	60%		Existe un conjunto adecuado de procedimientos para la manipulación de la información. No hay evidencia de su medición.
	A.8.3 Manejo de los soportes					47,33%	
		A.8.3.1	Gestión de soportes extraíbles	1 - Inicial	22%		No existen procedimientos para la gestión de soportes extraíbles. No se pide autorización para extraer soportes de la organización, no se almacenan en lugar seguro y no se utilizan técnicas criptográficas para proteger los datos.
		A.8.3.2	Eliminación de soportes	3 - Definido	60%		Eliminación de forma segura de los soportes cuando ya no son necesarios, especialmente en el caso de contener información sensible, que pueda ser confidencial.La eliminación de los medios sigue prácticas documentas y aunque se eliminan de forma segura los soportes cuando ya no son necesarios, depende del personal a cargo que lo efectue.
		A.8.3.3	Soportes físicos en tránsito	3 - Definido	60%		Se utiliza siempre el mismo servicio de mensajería y se lleva a cabo un registro de las transferencias. Los empleados conocen los protocolos seguros para la transferencia. Pero no se efectúan mediciones.
A.9 Control de acceso						69,33%	
	A.9.1 Requisitos empresariales de control de acceso					60,00%	

	A.9.1.1	Política de control de acceso	3 - Definido	60%		Existe una política de control de acceso lógico y físico documentada que ha sido divulgada a todo el personal de la empresa, de lo cual se tiene evidencia.
	A.9.1.2	Acceso a las redes y servicios de red	3 - Definido	60%		Los usuarios solamente tienen acceso a las redes y a los servicios en red para los que están autorizados. Se cuenta con un procedimiento para el control de acceso a la red y el acceso a los servicios.
A.9.2 Gestión de acceso de usuario					73,33%	
	A.9.2.1	Registro y baja de usuario	4 - Gestionado	80%		Los usuarios disponen de un identificador que les proporciona derechos de acceso y les hace responsables de sus acciones. Se tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.
	A.9.2.2	Provisión de acceso de usuario	4 - Gestionado	80%		Existe un procedimiento formal para asignar o revocar los derechos de acceso a los usuarios en todos los sistemas y servicios. Se registran todos los cambios de acceso.
	A.9.2.3	Gestión de privilegiados de acceso	4 - Gestionado	80%		La política de control de acceso controla la asignación de derechos de acceso privilegiados. Están establecidos los procedimientos para registrar y cancelar usuarios cuando corresponda. Se tiene registro de los cambios de acceso.
	A.9.2.4	Gestión de la información secreta de autentificación de los usuarios	3 - Definido	60%		Se ha requerido a los usuarios el compromiso de mantener su información de autenticación de forma secreta. Se han generado directrices para su gestión.
	A.9.2.5	Revisión de los derechos de acceso de usuario	3 - Definido	60%		Existe la revisión a intervalos regulares del acceso de los usuarios y el cambio de rol al reasignarse funciones. Se tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.
	A.9.2.6	Retirada o reasignación de los derechos de acceso	4 - Gestionado	80%		Los derechos de acceso de los empleados a la información y los recursos de tratamiento de la información son retirados a la finalización del empleo o ajustados. Se tienen definidas directrices para registrar y cancelar usuarios cuando corresponda.
A.9.3 Responsabilidades del usuario					60,00%	
	A.9.3.1	Uso de información secreta de autenticación	3 - Definido	60%		Existe una política por la cual los usuarios son responsables del uso de la información secreta. Este procedimiento está documentado y obliga.
A.9.4 Control de sistemas y acceso a las aplicaciones					84,00%	
	A.9.4.1	Restricción del acceso a la información	3 - Definido	60%		Se controla y restringe el acceso a la información y a las funciones de las aplicaciones de forma informal, el responsable de seguridad lo decide. La dirección cuenta con procedimientos de control de acceso para ejecutarlas. No se lleva registro.
	A.9.4.2	Procedimiento de inicio de sesión seguro	5 - Optimizado	100%		El procedimiento de inicio de sesión que controla el acceso a los sistemas y a las aplicaciones es seguro. Se han añadido técnicas más robustas, medios criptográficos, tarjetas inteligentes, doble autenticación, etc.
	A.9.4.3	Sistema de gestión de contraseñas	5 - Optimizado	100%		El sistema de gestión de contraseñas es implementado para conseguir la seguridad de las aplicaciones. Existen directrices para la gestión del control para manejar autenticación secreta en varias de sus aplicaciones.
	A.9.4.4	Uso de programas de servicios públicos privilegiados	3 - Definido	60%		Control establecido para manejar autenticación secreta en varias de sus aplicaciones por lo que ha generado directrices para su gestión. Se implementa un sistema que restringe y controla el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de las aplicaciones.
	A.9.4.5	Control de acceso al código fuente del programa	5 - Optimizado	100%		El código fuente del software propio que utiliza la organización tiene restringido su acceso. Existen políticas de restricción de acceso a los códigos fuente de los programas. Están planificadas las intervenciones que se desarrollan.
A.10 Criptografía					60,00%	
A.10.1 Controles criptográficos					60,00%	

		A.10.1.1	Políticas sobre el uso de controles criptográficos	3 - Definido	60%		Existe el establecimiento y comunicación de la política de uso de controles criptográficos. Se están desarrollando controles técnicos robustos para dar seguimiento a la gestión de estos controles.
		A.10.1.2	Gestión de claves.	3 - Definido	60%		Se han desarrollado e implementado políticas de uso. Se efectúa gestión de las claves criptográficas en todo el ciclo de vida.
A.11 Seguridad física y del entorno						66,83%	
	A.11.1 Áreas seguras					53,67%	
		A.11.1.1	Perímetro de seguridad física	3 - Definido	60%		El edificio cuenta con medidas de control del perímetro de seguridad, barrera física, cámaras de seguridad, sistema de alarma, etc. Existe evidencia de documentación de los planos y la definición de las áreas seguras.
		A.11.1.2	Controles de entrada físicas	3 - Definido	60%		Existe un control de seguridad para acceder al edificio. Se evidencia el uso de controles de acceso físico y la documentación de los visitantes a las instalaciones y las áreas seguras. Para acceder al CPD es necesario el uso de tarjeta esta protegido mediante controles de entrada adecuados, para asegurar el acceso a personal autorizado.
		A.11.1.3	Seguridad de oficina, despachos y recursos	3 - Definido	60%		Existen deficiencias que podrían ser mejoradas con respecto al control de acceso a las oficinas y despachos. Debería realizarse un modelo de diseño y aplicación.Existe un modelo de diseño y aplicación. Aunque todavía existen deficiencias que podrían ser mejoradas con respecto al control de acceso a las oficinas y despachos.
		A.11.1.4	Protección contra amenazas externas y ambientales	4 - Gestionado	80%		El edificio dispone de algunas medidas de protección física contra desastres naturales, ataques provocados por el hombre o accidentes. Generador eléctrico para caídas de corriente eléctrica o pararrayos.
		A.11.1.5	El trabajo en áreas seguras	1 - Inicial	22%		No se evidencian prácticas o procedimientos para el trabajo en las zonas que se han identificado como de alta seguridad. No se evidencia que estas zonas sean protegidas de forma especial con respecto al resto de las instalaciones.
		A.11.1.6	Zonas de entrega y carga	2 - Repetible	40%		Existen puntos de acceso tales como áreas de carga y descarga u otros puntos debidamente señalizados pero se desconoce si la empresa de seguridad los controla de forma correcta. No hay evidencia de documentación.
	A.11.2 Seguridad de los equipos					80,00%	
		A.11.2.1	Emplazamiento y protección del equipo	5 - Optimizado	100%		Está establecida la protección de los equipos según lo estableció en la política de seguridad. Hay evidencia de la implementación de controles orientados a garantizar la seguridad de estos equipos.
		A.11.2.2	Instalación de suministro	5 - Optimizado	100%		El edificio dispone de sistemas contra fallos en el suministro eléctrico. El área de mantenimiento del edificio se ocupa de su mantenimiento y gestión.
		A.11.2.3	Seguridad del cableado	5 - Optimizado	100%		El edificio dispone de eficientes sistemas de cableado y telecomunicaciones. El área de mantenimiento se ocupa de su gestión y mantenimiento.
		A.11.2.4	Mantenimiento de los equipos	5 - Optimizado	100%		Los equipos de sobremesa y portátiles de los usuarios reciben un mantenimiento anual para asegurar su disponibilidad e integridad. Se lleva un registro del mantenimiento preventivo y correctivo que se efectúa, así como tampoco de los fallos, reparaciones e incidencias. Se lleva un registro de todo ello.
		A.11.2.5	Retirada de materiales propiedad de la empresa	3 - Definido	60%		Están identificados los usuarios pueden sacar de las instalaciones activos. Se lleva a cabo registro de salida de equipos fuera de los locales de la organización, así como de su retorno

		A.11.2.6	Seguridad de los equipos fuera de las instalaciones	3 - Definido	60%		Los usuarios que sacan equipos o cualquier otro tipo de información fuera de las oficinas tienen conocimiento del riesgo de seguridad que conlleva, en caso de daño, robo o escucha. Conectan utilizando conexiones seguras VPN. Pero no se mantiene un registro que defina la cadena de custodia de los equipos y no se realizan controles. Se han realizado cursos básicos de concienciación.
		A.11.2.7	Reutilización o eliminación segura de equipos	2 - Repetible	40%		Se comprueba que los soportes de almacenamiento no guardan información sensible o software bajo licencia de la organización cuando van a ser destruidos o dados de baja. Los soportes con información sensible o con derechos de autor son destruidos físicamente o por medio de formateo que impida la recuperación de la información original. En el procedimiento existen deficiencias, ya que no se documenta la forma de actuar y tampoco los soporte sobre los que se ha intervenido.
		A.11.2.8	Equipos de usuario desatendidos	4 - Gestionado	80%		Los usuarios mediante el código de conducta informático son conscientes de los requisitos y procedimientos que se deben seguir para proteger el equipo desatendido. Se han implantado los procedimientos de seguridad y se les ha asesorado.
		A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	4 - Gestionado	80%		Existe política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables. Así como políticas de pantalla limpia. A los usuarios se les ha concienciado.
A.12 Operaciones de seguridad						67,76%	
	A.12.1 Procedimientos y responsabilidades en las operaciones					73,33%	
		A.12.1.1	Procedimientos operativos documentales	5 - Optimizado	100%		El personal conoce los procedimientos operativos para las actividades del sistema asociadas a los recursos de tratamiento y comunicación de la información, tal como encendido y apagado ordenadores, copias de respaldo, etc. Se han documentado los procedimientos de operación y los usuarios lo tienen a su disposición para consulta.
		A.12.1.2	Gestión de cambios	2 - Repetible	40%		Un técnico informático se encarga de efectuar el control sobre la seguridad de la información en cambios que se producen en la organización, procesos de negocio, instalaciones o tratamiento de la información y los sistemas. Pero no está definido un protocolo a seguir.Un técnico informático se encarga de efectuar el control sobre la seguridad de la información en cambios que se producen en la organización, procesos de negocio, instalaciones o tratamiento de la información y los sistemas. Pero no está definido un protocolo a seguir.
		A.12.1.3	Gestión de la capacidad	2 - Repetible	40%		Se aplica un sistema de control y de ajuste básico para asegurar donde es necesario la mejora de la disponibilidad y de la eficiencia de los sistemas. Los controles para la detección de problemas son rudimentarios. Debería elaborarse un plan documentado de gestión de la capacidad para los sistemas de misión crítica.
		A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	2 - Repetible	40%		Existe pero con deficiencias la separación entre entornos de operación, de prueba y de desarrollo con respecto al software a medida que necesita la organización para el desarrollo de su actividad.
	A.12.2 Protección contra malware					100,00%	
		A.12.2.1	Controles contra el malware	5 - Optimizado	100%		Los equipos llevan protección contra código malicioso, software de detección de código malicioso y de reparación. Los usuarios asumen su responsabilidad al respecto a la seguridad. Hay implementadas políticas y controles de detección para la prevención y recuperación, también hay procedimientos de concienciación del usuario.
	A.12.3 Copias de seguridad					100,00%	

	A.12.3.1	Copia de seguridad de la información	5 - Optimizado	100%		Se realizan copias de seguridad de la información, del software y de los sistemas de acuerdo a una planificación periódica acordada. Están documentadas las políticas de respaldo y definidos los requisitos de conservación y protección.
A.12.4 Registro y seguimiento					50,00%	
	A.12.4.1	Registro de eventos	2 - Repetible	40%		Existe registro de eventos para la protección y revisión de las actividades de los usuarios pero no es controlado por ningún responsable de la organización
	A.12.4.2	Protección de la información de los registros	2 - Repetible	40%		El responsable de informática de la organización lleva el control contra manipulaciones indebidas y accesos no autorizados. Se deberían mejorar los mecanismos para proteger contra cambios no autorizados y problemas operacionales relativos a los dispositivos e información de registro.
	A.12.4.3	Registros de administración y operación	2 - Repetible	40%		El administrador del sistema tiene privilegios para manipular los registros en las instalaciones de la organización. Supervisa las actividades del sistema y el cumplimento de las actividades de administración de la red.
	A.12.4.4	Sincronización del reloj	4 - Gestionado	80%		Los relojes de todos los sistemas de tratamiento de la información dentro del dominio están sincronizados con una fuente única de tiempo.
A.12.5 Control de software en explotación					60,00%	
	A.12.5.1	Instalación de software en explotación	3 - Definido	60%		En el procedimiento de despliegue de sistemas se han definido políticas y actividades específicas para la instalación de software, se dispone de una lista de software permitido y un inventario de licenciamiento adquirido.
A.12.6 Técnico de gestión de vulnerabilidades					41,00%	
	A.12.6.1	Gestión de vulnerabilidades técnicas	1 - Inicial	22%		Se realiza de manera básica la gestión de las vulnerabilidades técnicas de los sistemas de información utilizados. Se deberían evaluar la exposición de la organización a dichas vulnerabilidades, así como adoptar las medidas adecuadas para afrontar el riesgo asociado.
	A.12.6.2	Restricciones de instalación de software	3 - Definido	60%		El personal tiene claro el tipo de software que está permitido instalar y conoce las reglas con respecto a ese tema. La organización tiene definidas unas normas para decidir el tipo de software pueden instalar los usuarios y los privilegios. Existe documentación al respecto.
A.12.7 Consideraciones sobre la auditoria de sistemas de información					100,00%	
	A.12.7.1	Controles de auditoría de sistemas de información	5 - Optimizado	100%		Se cumplen los requisitos de auditoría exigidos para las auditorias de gestión y las auditorías internas a sistema de gestión.
A.13 Seguridad de las comunicaciones					55,33%	
A.13.1 Gestión de la seguridad de la red					40,67%	
	A.13.1.1	Controles de red	2 - Repetible	40%		Las redes son controladas de forma básica para proteger la información en los sistemas y aplicaciones. Deberían establecerse las responsabilidades y procedimientos para la gestión de equipos de red, así como controles para salvaguardar la confidencialidad e integridad de los datos.
	A.13.1.2	Seguridad de los servicios de red	3 - Definido	60%		Están implementados mecanismos de seguridad, niveles y gestión de los servicios de red que solamente el responsable de seguridad de la organización conoce. Existen deficiencias en cuanto a los procedimientos.
	A.13.1.3	Segregación en redes	1 - Inicial	22%		No existe segregación de redes, solamente hay una única red en la que se conectan todos los equipos y no hay ninguna política para impedir que equipos externos se conecten a dicha red. La red inalámbrica es meramente de cortesía y no accede a la red de trabajo.
A.13.2 Intercambio de información					70,00%	

		A.13.2.1	Políticas y procedimientos de intercambio de información	3 - Definido	60%		Se conoce por parte del personal los procedimientos para el intercambio de información de forma básica. Se han documentado los controles sobre el uso de técnicas criptográficas, directrices para la retención, eliminación de la correspondencia e información sensible.
		A.13.2.2	Acuerdos de intercambio de información	3 - Definido	60%		El intercambio de información de negocio y de software entre la organización y terceros se realiza de forma segura. Se cuida especialmente el tratamiento de datos personales. Pero no existen políticas, procedimientos o normas aprobadas por la dirección.
		A.13.2.3	Mensajería electrónica	3 - Definido	60%		Solamente se utiliza como tipo de mensajería el correo electrónico y están implementados mecanismos de fiabilidad y disponibilidad del servicio. Así como de protección frente a accesos no autorizados.
		A.13.2.4	Acuerdos de confidencialidad o de no revelación	5 - Optimizado	100%		Existen acuerdos de confidencialidad y de no revelación en la organización con respecto a negocios con otras organizaciones. Están identificados, documentados y revisados regularmente dichos acuerdos.
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información						57,85%	
	A.14.1 Requisitos de seguridad en los sistemas de información					53,33%	
		A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	3 - Definido	60%		Existen procedimientos para el análisis de seguridad del software a adquirir, así como con un listado de requerimientos generales para cualquier caso que se evalúa y se toma en cuenta al momento de seleccionar un proveedor.
		A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	3 - Definido	60%		Se utilizan métodos de control en las aplicaciones utilizadas que pasan información a través de redes públicas. Hacen uso de autenticación seguro basado en certificado electrónico y firmas digitales. Se encuentra protegida ante actividades fraudulentas o no autorizadas.
		A.14.1.3	Protección de las transacciones de servicios de aplicaciones	2 - Repetible	40%		Se tiene en cuenta una serie de consideraciones sobre la seguridad de la información en las transacciones de servicios de aplicaciones para prevenir las transmisiones incompletas, alteración del mensaje, etc. Pero debería mejorarse mediante protocolos seguros, rutas de comunicación cifrada.
	A.14.2 Seguridad en el desarrollo y en los procesos de soporte					60,22%	
		A.14.2.1	Políticas de desarrollo seguro	3 - Definido	60%		Se han establecido reglas con respecto al desarrollo de aplicaciones y sistemas. Su implementación está en curso dentro de los planes.
		A.14.2.2	Procedimientos de control de cambio del sistema	3 - Definido	60%		La incorporación de nuevos sistemas y los cambios importantes en los existentes se han realizado mediante un proceso formal de documentación, especificaciones y pruebas. Se han documentado los procedimientos formales de control de cambios.
		A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	3 - Definido	60%		La aplicación interna de negocio que se utiliza en el servicio de llamadas telefónicas es revisada y aprobadas sus modificaciones antes del cambio del sistema operativo. Hay políticas para garantizar que no existen efectos adversos en las funcionalidades o en la seguridad de la organización.
		A.14.2.4	Restricciones a los cambios en los paquetes de software	2 - Repetible	40%		Se controlan los paquetes de software suministrados por proveedores. No se ha dado el caso de ser necesaria la modificación del software original, se instalan los parches y actualizaciones aprobadas por éste.
		A.14.2.5	Principios de ingeniería de sistemas seguros	1 - Inicial	22%		Para la actividad de la organización no es necesario aplicar los principios de ingeniería seguros.
		A.14.2.6	Entorno de desarrollo seguro	3 - Definido	60%		Se efectúan controles de seguridad en la organización, diferenciación de entornos, control de accesos, etc. Está documentado convenientemente.
		A.14.2.7	Externalización del desarrollo de software	4 - Gestionado	80%		El desarrollo del software propio que utiliza la organización es supervisado y controlado por personal interno. Se formalizan acuerdos con referencia a las licencias, código, derechos de propiedad intelectual, etc. Es consensuado con el proveedor en acuerdos firmados y consensuados. Están regulados y revisados los acuerdos.

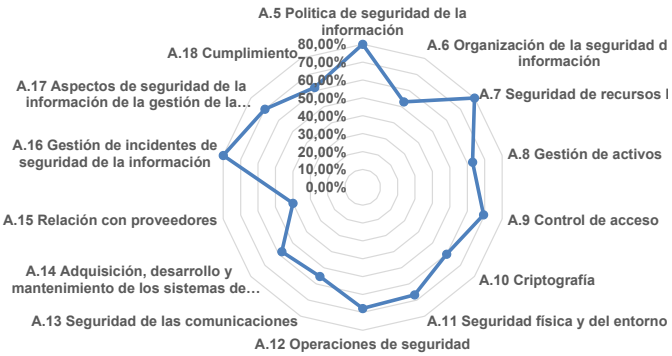
		A.14.2.8	Pruebas funcionales de seguridad del sistema	4 - Gestionado	80%		El personal informático de la organización dispone de un plan de pruebas funcionales de seguridad y se prueba y revisa periódicamente.
		A.14.2.9	Pruebas de aceptación del sistema	4 - Gestionado	80%		El personal informático de la organización ha establecido un programa de pruebas de aceptación relacionados con nuevos sistemas de información, actualizaciones y nuevas versiones. Hay una política aprobada por la dirección al respecto.
	A.14.3 Datos de prueba					60,00%	
		A.14.3.1	Protección de datos de prueba	3 - Definido	60%		En el desarrollo del software propio de la organización se utilizan datos no reales con los que se realizan las pruebas posteriores de los sistemas. Se encuentra ambientes por separado para desarrollo, test y producción. Está documentado convenientemente.
A.15 Relación con proveedores						40,00%	
	A.15.1 Seguridad en las relaciones con proveedores					40,00%	
		A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	2 - Repetible	40%		Existen acuerdos entre la organización y los proveedores sobre el acceso a los activos. Falta la divulgación de la política de seguridad en las relaciones con los proveedores.
		A.15.1.2	Requisitos de seguridad en contratos con terceros	2 - Repetible	40%		Las condiciones de seguridad de la información no se reflejan en los contratos de forma explícita. Se efectúa de manera informal. Se deberían establecer y documentar los acuerdos con los proveedores para asegurar no haya malentendidos y además, el proveedor respete las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información.
		A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	2 - Repetible	40%		El suministro de tecnología de la información y de las comunicaciones tiene lugar mediante la contratación de otras empresas.
	A.15.2 Gestión de la provisión de servicios del proveedor					40,00%	
		A.15.2.1	Control y revisión de la provisión de servicios del proveedor	2 - Repetible	40%		Se revisa y supervisa de forma básica los servicios de los proveedores en los términos y condiciones de seguridad de la información acordados. Pero no hay políticas ni procedimientos acordados por la dirección para ello.
		A.15.2.2	Gestión de cambios en la provisión del servicio de proveedor	2 - Repetible	40%		Los cambios en la provisión de un servicio no se documentan, ni se lleva control. Depende de la gestión del líder del proyecto área relacionada.
A.16 Gestión de incidentes de seguridad de la información						80,00%	
	A.16.1 Gestión de incidentes de seguridad de la información y mejoras					80,00%	
		A.16.1.1	Responsabilidades y procedimientos	5 - Optimizado	100%		Se han establecidos las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada ante incidentes de seguridad. Se evidencia la existencia y divulgación del procedimiento de gestión de incidentes, así como la medición de ellos.
		A.16.1.2	Informar eventos de seguridad de la información	5 - Optimizado	100%		El responsable informático conoce la forma de informar de eventos de seguridad además, están implementados los canales de comunicación adecuados para notificar los eventos de seguridad. Existe y es de conocimiento por parte de todos los implicados de los procedimientos para la gestión de incidentes.
		A.16.1.3	Informar las debilidades de seguridad de la información	4 - Gestionado	80%		Los empleados son conscientes de la importancia de notificar los puntos débiles que observen o sospechen en los sistemas. Saben los procedimientos para ponerlo en conocimiento de su responsable.
		A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	4 - Gestionado	80%		Se lleva un registro de los eventos que se producen, se evalúan y se decide si se clasifican como incidentes de seguridad de la información. Existe un procedimiento al respecto.
		A.16.1.5	Respuesta a incidentes de seguridad de la información	4 - Gestionado	80%		Existen procedimientos documentados para dar respuesta a incidentes de seguridad de la información. El personal ha sido formado sobre la forma de actuar ante este tipo de situaciones.

		A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	2 - Repetible	40%		Se evalúa la necesidad de mejorar o añadir controles que limiten incidentes. Pero no están implementados mecanismos para cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información.
		A.16.1.7	Recopilación de evidencias	4 - Gestionado	80%		La organización tiene definidos procedimientos para la recogida, adquisición y preservación de la información que puede servir de evidencia.
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio						70,00%	
	A.17.1 Continuidad de la seguridad de la información					80,00%	
		A.17.1.1	Planificación de la continuidad de la seguridad de la información	4 - Gestionado	80%		El plan de continuidad de negocio ante contratiempos y situaciones de parada de los distintos servicios (energía, comunicaciones, red, etc.) está desarrollado en profundidad para situaciones adversas.
		A.17.1.2	Implementación de la continuidad de la seguridad de la información	4 - Gestionado	80%		El responsable de informática tiene establecidas una serie de medidas para restablecer la disponibilidad de la información en caso de situaciones inesperadas. Además, está documentado todo el proceso.
		A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	4 - Gestionado	80%		Se efectúan por parte del responsable informático controles a intervalos regulares que verifiquen que los procesos, procedimientos y controles para la seguridad de la información son válidos y eficaces durante situaciones adversas. Hay procedimientos establecidos, ni documentación aprobada por la dirección al respecto.
	A.17.2 Redundancias					60,00%	
		A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	3 - Definido	60%		Están implementados mecanismos de redundancia de la información. Se ha llegado a un acuerdo con otra empresa, en el uso como centro alternativo con estaciones de trabajo que proporcionen servicio aceptable para el negocio en caso de contingencia. Pero todavía no sido probado su funcionamiento.
A.18 Cumplimiento						62,00%	
	A.18.1 Cumplimiento de requisitos legales y contractuales					44,00%	
		A.18.1.1	Identificación de la legislación aplicable y los requisitos contractuales.	2 - Repetible	40%		El asesor jurídico y el responsable de informática conocen los requisitos pertinentes en cuanto a la legislación pero no se encuentran definidos y documentados los controles específicos y las responsabilidades individuales.
		A.18.1.2	Derechos de propiedad intelectual	2 - Repetible	40%		Se respetan los derechos de propiedad intelectual y de los productos de software patentado pero no hay implementados procedimientos adecuados para garantizar el cumplimiento de los requisitos legales.
		A.18.1.3	Protección de los registros de la organización	2 - Repetible	40%		Existe protección para los registros de la organización contra la pérdida, destrucción, falsificación o acceso no autorizados pero con muchas deficiencias. No se hace en relación con unos requisitos legales, regulatorios y de negocio documentados.
		A.18.1.4	Protección y privacidad de la información de carácter personal	2 - Repetible	40%		Debería mejorarse la garantía y privacidad de los datos, según se requiere en la legislación y la reglamentación aplicables. Es necesario contar con una buena política de privacidad y protección de la información de carácter personal.
		A.18.1.5	Regulación de controles criptográficos	3 - Definido	60%		Existe una política respecto a los controles criptográficos. Su implementación está en curso.
	A.18.2 Revisiones de seguridad de la información					80,00%	
		A.18.2.1	Revisión independiente de seguridad de la información	4 - Gestionado	80%		Se están realizando revisiones sobre la gestión de la seguridad de la información y su implantación en la organización. Se cuenta con un plan de auditoria y revisión interna de la operación de los controles y del SGSI.

		A.18.2.2	Cumplimiento de políticas y estándares de seguridad	4 - Gestionado	80%		La dirección y el responsable determinan cómo revisar los requisitos definidos en las políticas, normas y otra reglamentación. Se revisan periódicamente los indicadores con respecto al desempeño de los controles y el cumplimiento de las políticas por parte de la dirección.
		A.18.2.3	Revisión de cumplimiento técnico	4 - Gestionado	80%		El responsable de informática realiza revisiones de cumplimiento técnico de las normas de seguridad. Se efectúan pruebas de intrusión, evaluación de vulnerabilidades, planificadas, documentadas y repetidas.

CONTROL	Valor	CUMPLIMIENTO
A.5 Política de seguridad de la información	80,00%	CUMPLE
A.6 Organización de la seguridad de la información	53,00%	CUMPLE PARCIALMENTE
A.7 Seguridad de recursos humanos	80,00%	CUMPLE
A.8 Gestión de activos	63,00%	CUMPLE PARCIALMENTE
A.9 Control de acceso	69,33%	CUMPLE
A.10 Criptografía	60,00%	CUMPLE PARCIALMENTE
A.11 Seguridad física y del entorno	66,83%	CUMPLE
A.12 Operaciones de seguridad	67,76%	CUMPLE
A.13 Seguridad de las comunicaciones	55,33%	CUMPLE PARCIALMENTE
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	57,85%	CUMPLE PARCIALMENTE
A.15 Relación con proveedores	40,00%	CUMPLE PARCIALMENTE
A.16 Gestión de incidentes de seguridad de la información	80,00%	CUMPLE
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio	70,00%	CUMPLE
A.18 Cumplimiento	62,00%	CUMPLE

Situación


A.5 Politica de seguridad de la información
A.6 Organización de la seguridad d información
A.7 Seguridad de recursos h
A.8 Gestión de activos
A.9 Control de acceso
A.10 Criptografía
A.11 Seguridad física y del entorno
A.12 Operaciones de seguridad
A.13 Seguridad de las comunicaciones
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de…
A.15 Relación con proveedores
A.16 Gestión de incidentes de seguridad de la información
A.17 Aspectos de seguridad de la información de la gestión de la…
A.18 Cumplimiento
80,00%
70,00%
60,00%
50,00%
40,00%
30,00%
20,00%
10,00%
0,00%