El campo es de todos Minagricultura	**FORMATO**	VERSION 12
	MAPA DE RIESGOS	**F01-PR-SIG-05**
		FECHA EDICIÓN 28/04/2021

PROCESO: **Gestión de Apoyo Logístico e Infraestructura**

SECCION B: RIESGOS DE SEGURIDAD DE LA INFORMACION

Identificación del riesgo						Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles								
		EVALUACION DE LA CRITICIDAD DEL ACTIVO							NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red		
								Conexiones a red pública desprotegidas	2								13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								Eliminación o reutilización de soportes sin borrar	3								8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios		
								Gestión del control de acceso ineficiente	2								9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad		
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2								9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo		
								No existen procedimientos formales para alta y baja de usuarios	2								9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación 9.4.3 Sistema de gestión de contraseña 8.1.1 Inventario de activos		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles						
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Inventario individual	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo			Uso soportes removibles no controlado	3	24	24	12	16	16	8	Aceptar	8.1.2 Propiedad de los activos	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Almacén
																	8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios fisicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.1 Controles de red		
																	13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.2 Controles de acceso fisico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
								No existen registros de auditoria	3								12.4.1 Registro de eventos		
																	12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
						Revelación de contraseñas	2	No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		
								No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
								No existen procedimientos de autorización para información pública	3								8.3.1 Gestión de medios removibles		
								No existen procedimientos para el etiquetado y manejo de la información	3								14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad física		
								Eliminación o reutilización de	3								11.2.7 Seguridad en el desecho o reutilización de equipos		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles			
		EVALUACION DE LA CRITICIDAD DEL ACTIVO							NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL							
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
						Robo de información	1	soportes sin borrar	3								8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3										
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación 9.4.3 Sistema de gestión de contraseña 8.1.1 Inventario de activos		
								Conexiones a red pública desprotegidas	2										
								Eliminación o reutilización de soportes sin borrar	3										
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Actas	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo			Uso soportes removibles no controlado	3	27	24	36	18	16	24	Tratar	8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 8.3.3 Tránsito de medios fisicos	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.2 Controles de acceso fisico 11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
								No existen registros de auditoria	3								12.4.1 Registro de eventos 12.4.2 Protección de la información del registro de eventos 12.4.3 Registro de administrador y operador 12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso 12.3.1 Copia de seguridad de la información		
						Revelación de contraseñas	2	No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		
								No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		

Identificación del riesgo						Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
																	8.3.1 Gestión de medios removibles		
								No existen procedimientos de autorización para información pública	3								14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	3	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad física		
																	11.2.7 Seguridad en el desecho o reutilización de equipos		

Identificación del riesgo						Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	2	Eliminación o reutilización de soportes sin borrar	3								8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios físicos		
								No existe control para copia de información	3										
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								Conexiones a red pública desprotegidas	2								8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación 9.4.3 Sistema de gestión de contraseña		
								Eliminación o reutilización de soportes sin borrar	3										
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Capacitaciones en Gestión Documental	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo			Uso soportes removibles no controlado	3	24	24	24	16	16	16	Aceptar	8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 8.3.3 Tránsito de medios físicos	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.2 Controles de acceso físico 11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información 12.4.1 Registro de eventos 12.4.2 Protección de la información del registro de eventos 12.4.3 Registro de administrador y operador 12.4.4 Sincronización de reloj		
								No existen registros de auditoria	3										
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso 12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
																	8.3.1 Gestión de medios removibles		
								No existen procedimientos de autorización para información pública	3								14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso fisico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles				
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	2	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios		
								No existe control para copia de información	3								12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								Conexiones a red pública desprotegidas	2								8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo		
								Eliminación o reutilización de soportes sin borrar	3								9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles						
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Consecutivo de Comunicaciones Oficiales	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	24	16	16	16	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
																	8.1.3 Uso aceptable de los activos		
								Uso soportes removibles no controlado	3								8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
																	13.1.1 Controles de red		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	11.1.2 Controles de acceso físico		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3									7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2									8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3									13.2.1 Políticas y procedimientos para el intercambio de información		
																		13.2.2 Acuerdos de intercambio de información		
																		13.2.3 Mensajería electrónica		
																		14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																		14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2									12.1.4 Separación de entornos de desarrollo, prueba y operación		
																		12.3.1 Copia de seguridad de la información		
																		8.3.1 Gestión de medios removibles		
								No existen procedimientos de autorización para información pública	3									14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3									8.2.1 Clasificación de la información		
																		8.2.2 Etiquetado de la información		
																		8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3									11.1.2 Controles de acceso fisico		
																		11.1.3 Seguridad de oficinas, salas e instalaciones		
																		11.1.5 Trabajo en áreas seguras		
																		11.1.6 Áreas de entrega y carga		
																		11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2									11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles				
		EVALUACION DE LA CRITICIDAD DEL ACTIVO								NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL							
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
						Robo de información	2	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3										
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Conexiones a red pública desprotegidas	2										
								Eliminación o reutilización de soportes sin borrar	3										
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Derechos de petición	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	12	16	16	8	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
								Uso soportes removibles no controlado	3								8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.1 Controles de red		
																	13.1.2 Seguridad de servicios de red		
								No existe protección contra código malicioso	2								13.1.3 Segregación de redes		
																	12.2.1 Controles contra código malicioso		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.2 Controles de acceso físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3									7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2									8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3									13.2.1 Políticas y procedimientos para el intercambio de información		
																		13.2.2 Acuerdos de intercambio de información		
																		13.2.3 Mensajería electrónica		
																		14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																		14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2									12.1.4 Separación de entornos de desarrollo, prueba y operación		
																		12.3.1 Copia de seguridad de la información		
																		8.3.1 Gestión de medios removibles		
								No existen procedimientos de autorización para información pública	3									14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3									8.2.1 Clasificación de la información		
																		8.2.2 Etiquetado de la información		
																		8.2.3 Manejo de activos		
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3									11.1.2 Controles de acceso fisico		
																		11.1.3 Seguridad de oficinas, salas e instalaciones		
																		11.1.5 Trabajo en áreas seguras		
																		11.1.6 Áreas de entrega y carga		
																		11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2									11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	1	Eliminación o reutilización de soportes sin borrar	3									11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios		
								No existe control para copia de información	3									12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
						Acceso no autorizado	1	Acceso remoto no seguro	2									9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								Conexiones a red pública desprotegidas	2									8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo		
								Eliminación o reutilización de soportes sin borrar	3									9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Gestión del control de acceso ineficiente	2											
								No existen mecanismos de autenticación y validación del usuario	2											
								No existen procedimientos formales de revisión de accesos	2											
								No existen procedimientos formales para alta y baja de usuarios	2											

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles						
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Documentos de ORFEO	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	24	16	16	16	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
								Uso soportes removibles no controlado	3								8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
																	13.1.1 Controles de red		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	11.1.2 Controles de acceso físico		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3									7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2									8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3									13.2.1 Políticas y procedimientos para el intercambio de información		
																		13.2.2 Acuerdos de intercambio de información		
																		13.2.3 Mensajería electrónica		
																		14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																		14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2									12.1.4 Separación de entornos de desarrollo, prueba y operación		
																		12.3.1 Copia de seguridad de la información		
								No existen procedimientos de autorización para información pública	3									8.3.1 Gestión de medios removibles		
																		14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3									8.2.1 Clasificación de la información		
																		8.2.2 Etiquetado de la información		
																		8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3									11.1.2 Controles de acceso fisico		
																		11.1.3 Seguridad de oficinas, salas e instalaciones		
																		11.1.5 Trabajo en áreas seguras		
																		11.1.6 Áreas de entrega y carga		
																		11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2									11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	2	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3										
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Conexiones a red pública desprotegidas	2										
								Eliminación o reutilización de soportes sin borrar	3										
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Instrumentos Archivísticos	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	24	16	16	16	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
								Uso soportes removibles no controlado	3								8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
																	13.1.1 Controles de red		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	11.1.2 Controles de acceso físico		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3									7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2									8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3									13.2.1 Políticas y procedimientos para el intercambio de información		
																		13.2.2 Acuerdos de intercambio de información		
																		13.2.3 Mensajería electrónica		
																		14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																		14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2									12.1.4 Separación de entornos de desarrollo, prueba y operación		
																		12.3.1 Copia de seguridad de la información		
																		8.3.1 Gestión de medios removibles		
								No existen procedimientos de autorización para información pública	3									14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3									8.2.1 Clasificación de la información		
																		8.2.2 Etiquetado de la información		
																		8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3									11.1.2 Controles de acceso fisico		
																		11.1.3 Seguridad de oficinas, salas e instalaciones		
																		11.1.5 Trabajo en áreas seguras		
																		11.1.6 Áreas de entrega y carga		
																		11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2									11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	2	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios		
								No existe control para copia de información	3								12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								Conexiones a red pública desprotegidas	2								8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo		
								Eliminación o reutilización de soportes sin borrar	3								9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles			
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Instrumentos de Control y Seguimiento	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	24	16	16	16	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
								Uso soportes removibles no controlado	3								8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
																	13.1.1 Controles de red		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	11.1.2 Controles de acceso físico		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
								No existen procedimientos de autorización para información pública	3								8.3.1 Gestión de medios removibles		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso fisico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	2	Eliminación o reutilización de soportes sin borrar	3									11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3											
						Acceso no autorizado	1	Acceso remoto no seguro	2									9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Conexiones a red pública desprotegidas	2											
								Eliminación o reutilización de soportes sin borrar	3											
								Gestión del control de acceso ineficiente	2											
								No existen mecanismos de autenticación y validación del usuario	2											
								No existen procedimientos formales de revisión de accesos	2											
								No existen procedimientos formales para alta y baja de usuarios	2											

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles			
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Rollos de Microfilmación	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	32	12	16	16	8	Tratar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
								Uso soportes removibles no controlado	3								8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
																	13.1.1 Controles de red		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	11.1.2 Controles de acceso físico		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	4								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
																	8.3.1 Gestión de medios removibles		
								No existen procedimientos de autorización para información pública	3								14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso fisico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles			
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	1	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3										
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Conexiones a red pública desprotegidas	2										
								Eliminación o reutilización de soportes sin borrar	3										
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles						
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Documento PIGA	Información	2	4	3	Perdida de integridad del activo					12	24	18	8	16	12	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
								Uso soportes removibles no controlado	3								8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
																	8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.1 Controles de red		
																	13.1.2 Seguridad de servicios de red		
								No existe protección contra código malicioso	2								13.1.3 Segregación de redes		
								No existen procedimientos de monitorización de las instalaciones	3								12.2.1 Controles contra código malicioso		
																	11.1.2 Controles de acceso físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
								No existen procedimientos de autorización para información pública	3								8.3.1 Gestión de medios removibles		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso fisico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	2	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3										
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Conexiones a red pública desprotegidas	2										
								Eliminación o reutilización de soportes sin borrar	3										
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles			
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Repositorio de documentos del proceso	Información	4	4	3	Perdida de confidencialidad y integridad del activo					24	24	18	16	16	12	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
																	8.1.3 Uso aceptable de los activos		
								Uso soportes removibles no controlado	3								8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
																	13.1.1 Controles de red		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	11.1.2 Controles de acceso físico		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
																	8.3.1 Gestión de medios removibles		
								No existen procedimientos de autorización para información pública	3								14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso fisico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles				
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	1	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3										
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Conexiones a red pública desprotegidas	2										
								Eliminación o reutilización de soportes sin borrar	3										
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles						
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Solicitud de anticipos	Información	4	4	2	Perdida de confidencialidad y integridad del activo					24	24	12	16	16	8	Aceptar	9.4.3 Sistema de gestión de contraseña 8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 8.3.3 Tránsito de medios físicos 11.2.3 Seguridad del cableado 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 12.2.1 Controles contra código malicioso 11.1.2 Controles de acceso físico 11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga 12.7.1 Controles de la auditoría de sistemas de información 12.4.1 Registro de eventos 12.4.2 Protección de la información del registro de eventos 12.4.3 Registro de administrador y operador 12.4.4 Sincronización de reloj 12.2.1 Controles contra código malicioso 12.3.1 Copia de seguridad de la información 7.2.2 Concienciación, educación y capacitación de la seguridad de la información	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
								Uso soportes removibles no controlado	3											
						Escuchas no autorizadas	1	Cableado desprotegido	3											
								Comunicaciones a través de redes públicas o desprotegidas	2											
								No existe protección contra código malicioso	2											
								No existen procedimientos de monitorización de las instalaciones	3											
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3											
								No existen registros de auditoria	3											
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2											
								No existe concienciación y formación en seguridad	3											

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3									7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2									8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3									13.2.1 Políticas y procedimientos para el intercambio de información		
																		13.2.2 Acuerdos de intercambio de información		
																		13.2.3 Mensajería electrónica		
																		14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																		14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2									12.1.4 Separación de entornos de desarrollo, prueba y operación		
																		12.3.1 Copia de seguridad de la información		
																		8.3.1 Gestión de medios removibles		
								No existen procedimientos de autorización para información pública	3									14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3									8.2.1 Clasificación de la información		
																		8.2.2 Etiquetado de la información		
																		8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3									11.1.2 Controles de acceso fisico		
																		11.1.3 Seguridad de oficinas, salas e instalaciones		
																		11.1.5 Trabajo en áreas seguras		
																		11.1.6 Áreas de entrega y carga		
																		11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2									11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	1	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3										
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Conexiones a red pública desprotegidas	2										
								Eliminación o reutilización de soportes sin borrar	3										
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles						
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Solicitud de servicios parque automotor	Información	4	4	2	Perdida de confidencialidad y integridad del activo					24	24	12	16	16	8	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
								Uso soportes removibles no controlado	3								8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
																	13.1.1 Controles de red		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	11.1.2 Controles de acceso físico		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
								No existen procedimientos de autorización para información pública	3								8.3.1 Gestión de medios removibles		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso fisico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL		Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD								
						Robo de información	1	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios			
								No existe control para copia de información	3								12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos			
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes			
								Conexiones a red pública desprotegidas	2								8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios			
								Eliminación o reutilización de soportes sin borrar	3								9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad			
								Gestión del control de acceso ineficiente	2								9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo			
								No existen mecanismos de autenticación y validación del usuario	2								9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación			
								No existen procedimientos formales de revisión de accesos	2											
								No existen procedimientos formales para alta y baja de usuarios	2											

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles			
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Solicitud de servicios planta física	Información	4	4	2	Perdida de confidencialidad y integridad del activo					24	24	12	16	16	8	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
								Uso soportes removibles no controlado	3								8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
																	13.1.1 Controles de red		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	11.1.2 Controles de acceso físico		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
								No existen procedimientos de autorización para información pública	3								8.3.1 Gestión de medios removibles		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso fisico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Robo de información	1	Eliminación o reutilización de soportes sin borrar	3									11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3											
						Acceso no autorizado	1	Acceso remoto no seguro	2									9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Conexiones a red pública desprotegidas	2											
								Eliminación o reutilización de soportes sin borrar	3											
								Gestión del control de acceso ineficiente	2											
								No existen mecanismos de autenticación y validación del usuario	2											
								No existen procedimientos formales de revisión de accesos	2											
								No existen procedimientos formales para alta y baja de usuarios	2											

Identificación del riesgo						Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Planes de Transferencias Documentales	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	12	16	16	8	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Grupo de Gestión Documental y Biblioteca
																	8.1.1 Inventario de activos		
								Uso soportes removibles no controlado	3								8.1.2 Propiedad de los activos		
																	8.1.3 Uso aceptable de los activos		
																	8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.1 Controles de red		
																	13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.2 Controles de acceso físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
								No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		

Identificación del riesgo						Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
																	8.3.1 Gestión de medios removibles		
								No existen procedimientos de autorización para información pública	3								14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso fisico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad fisica		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles				
		EVALUACION DE LA CRITICIDAD DEL ACTIVO								NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL							
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
						Robo de información	1	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios 12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
								No existe control para copia de información	3										
						Elevación de privilegios	2	Fallos conocidos en inversiones	3								12.6.1 Gestión de vulnerabilidades técnicas 12.6.2 Restricciones en la instalación de programas 14.2.4 Restricciones en cambios a paquetes de aplicaciones 12.5.1 Instalación de programas en sistemas en producción 14.2.2 Procedimiento de control de cambio en sistemas de información 14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 12.4.1 Registro de eventos 12.4.2 Protección de la información del registro de eventos 12.4.3 Registro de administrador y operador 12.4.4 Sincronización de reloj 14.1.1 Análisis y especificaciones de requisitos de seguridad de la información 14.2.1 Política de desarrollo seguro		
								Gestión de actualizaciones de seguridad ineficiente	2										
								Gestión ineficiente de contraseñas	2										
								No existen registros de auditoria	3										
								Configuración de parámetros errónea	3										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles			
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Sistema de Información Gestión de Activos e Inventarios	Software	1	1	4	Perdida de disponibilidad del activo	Fallo de sistemas	1	Especificaciones para desarrolladores incompletas o confisas	3	0	0	24	0	0	16	Aceptar	14.2.5 Principios para la ingeniería de sistemas seguros 14.2.6 Entorno seguro de desarrollo 14.2.7 Desarrollo externalizado 9.4.5 Control de acceso a código fuente de programa	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin	Grupo de Almacén
								Fallos conocidos en inversiones	3								12.6.1 Gestión de vulnerabilidades técnicas 14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación 14.2.4 Restricciones en cambios a paquetes de aplicaciones		
								Gestión de actualizaciones de seguridad ineficiente	3								12.5.1 Instalación de programas en sistemas en producción 12.6.1 Gestión de vulnerabilidades técnicas 12.6.2 Restricciones en la instalación de programas 14.2.2 Procedimiento de control de cambio en sistemas de información 14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación 14.2.4 Restricciones en cambios a paquetes de aplicaciones		
								No exiten registros de auditoría	3								12.4.1 Registro de eventos		
								Prubas de software insuficientes	3								14.2.8 Pruebas de seguridad del sistema 14.2.9 Pruebas de aceptación del sistema 14.3.1 Protección de la información de prueba		
						Incumplimiento legal, reglamentario o contractual	2	Validación de la legislación aplicable	3								10.1.1 Política en el uso de controles criptográficos 18.1.2 Derechos de propiedad intelectual		
																	10.1.1 Política en el uso de controles criptográficos		

Identificación del riesgo						Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles							
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
						Uso de sistemas por usuarios no autorizados	1	Acceso remoto no seguro	3								10.1.2 Gestión de claves de criptografía 9.1.2 Acceso a redes y servicios de red 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.5 Revisión de los derechos de acceso de usuarios 9.2.6 Retirada o ajuste de los derechos de acceso		
								Asgnación errónea de derechos de acceso	2										
Sistema ORFEO	Servicios	1	1	4	Perdida de disponibilidad del activo	Fallo en la provisión	2	No existe procedimiento para el control de cambios	2			24			16		15.2.2 Gestión de cambios en la provisión de servicios 15.1.1 Política de seguridad en la relación con proveedores 15.1.2 Seguridad en el acuerdo con proveedores 15.1.3 Tecnología de la información y comunicacion en la cadena de suminitro 15.2.1 Monitorización y revisión de la provisión de servicios	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin	Jefe Oficina TIC
								No existen acuerdos de calidad del servicio (SLA)	3										
						Elevación de privilegios	2	Fallos conocidos en inversiones	3								12.6.1 Gestión de vulnerabilidades técnicas 12.6.2 Restricciones en la instalación de programas 14.2.4 Restricciones en cambios a paquetes de aplicaciones 12.5.1 Instalación de programas en sistemas en producción 14.2.2 Procedimiento de control de cambio en sistemas de información 14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación 9.2.3 Gestión de derechos de acceso privilegiado		
								Gestión de actualizaciones de seguridad ineficiente	2										
								Gestión ineficiente de											

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Sistema Catalogación Bibliográfica KOHA	Software	1	1	4	Perdida de disponibilidad del activo			Gestión ineficiente de contraseñas	2	0	0	24	0	0	16	Aceptar	9.2.4 Gestión de información secreta de autenticación	Grupo de Gestión Documental	Grupo de Almacén
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Fallo de sistemas	1	Configuración de parámetros errónea	3								14.1.1 Análisis y especificaciones de requisitos de seguridad de la información		
																	14.2.1 Política de desarrollo seguro		
								Especificaciones para desarrolladores incompletas o confisas	3								14.2.5 Principios para la ingeniería de sistemas seguros		
																	14.2.6 Entorno seguro de desarrollo		
																	14.2.7 Desarrollo externalizado		
																	9.4.5 Control de acceso a código fuente de programa		
								Fallos conocidos en inversiones	3								12.6.1 Gestión de vulnerabilidades técnicas		
																	14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación		
																	14.2.4 Restricciones en cambios a paquetes de aplicaciones		
								Gestión de actualizaciones de seguridad ineficiente	3								12.5.1 Instalación de programas en sistemas en producción		
																	12.6.1 Gestión de vulnerabilidades técnicas		
																	12.6.2 Restricciones en la instalación de programas		
																	14.2.2 Procedimiento de control de cambio en sistemas de información		
																	14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación		

Identificación del riesgo						Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
																	14.2.4 Restricciones en cambios a paquetes de aplicaciones		
								No exiten registros de auditoría	3								12.4.1 Registro de eventos		
								Prubas de software insuficientes	3								14.2.8 Pruebas de seguridad del sistema		
																	14.2.9 Pruebas de aceptación del sistema		
																	14.3.1 Protección de la información de prueba		
						Incumplimiento legal, reglamentario o contractual	2	Validación de la legislación aplicable	3								10.1.1 Política en el uso de controles criptográficos		
																	18.1.2 Derechos de propiedad intelectual		
																	10.1.1 Política en el uso de controles criptográficos		
																	10.1.2 Gestión de claves de criptografía		
						Uso de sistemas por usuarios no autorizados	1	Acceso remoto no seguro	3								9.1.2 Acceso a redes y servicios de red		
																	9.4.2 Procesos de inicio seguro de sesión		
																	9.4.3 Sistema de gestión de contraseña		
																	9.2.2 Provisión de acceso a usuarios		
								Asgnación errónea de derechos de acceso	2								9.2.3 Gestión de derechos de acceso privilegiado		
																	9.2.5 Revisión de los derechos de acceso de usuarios		
																	9.2.6 Retirada o ajuste de los derechos de acceso		

	REVISO	APROBO
Firma		
Nombre	**Yudy Estella Pulgarín Marín**	**Yudy Estella Pulgarín Marín**
Cargo	Subdirectora Administrativa	Subdirectora Administrativa
Fecha	7 de junio de 2021	7 de junio de 2021