

FORMATO
MAPA DE RIESGOS

PROCESO: Gestión de Financiamiento y Riesgos Agropecuarios

SECCION B: RIESGOS DE SEGURIDAD DE LA INFORMACION

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				
					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				
							Eliminación o reutilización de soportes sin borrar	3							13.1.2 Seguridad de servicios de red				
							Gestión del control de acceso ineficiente	2							13.1.3 Segregación de redes				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							8.3.2 Desecho de medios				
							No existen procedimientos formales para alta y baja de usuarios	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 contraseñas				
															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 contraseñas				
															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									
Administración de herramienta para proyectos de inversión	Información	4	4	4	Pérdida de confidencialidad, integridad y disponibilidad del activo	Uso soportes removibles no controlado		3	24	24	24	16	16	16	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.	Dirección de Financiamiento y Riesgos Agropecuarios						
																								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
					Escuchas no autorizadas	1	Cableado desprotegido	3							13.1.2 Seguridad de servicios de red									
							Comunicaciones a través de redes públicas o desprotegidas	2							13.1.3 Segregación de redes									
							No existe protección contra código malicioso	2							13.1.3.1 Controles contra código malicioso									
							No existen procedimientos de monitorización de las instalaciones	3							11.1.2 Controles de acceso físico									
							No existe control sobre el uso de utilidades de sistema	3							11.1.3 Seguridad de oficinas, salas e instalaciones									
							Manipulación de los registros	2							11.1.5 Trabajo en áreas seguras									
							No existen registros de auditoría	3							11.1.6 Áreas de entrega y carga									
							Pérdida o corrupción de la información	1							12.7.1 Controles de la auditoría de sistemas de información									
							No existe protección contra código malicioso	2							12.4.1 Registro de eventos									
							No existe concienciación y formación en seguridad	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									
															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									

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 aplicación en redes públicas		
								No existe control para copia de información	2							14.1.3 Protección de transacciones en servicio de aplicación			
								No existen procedimientos de autorización para información pública	3							12.1.4 Separación de entornos de desarrollo, prueba y operación			
								No existen procedimientos para el etiquetado y manejo de la información	3							12.3.1 Copia de seguridad de la información			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							8.3.1 Gestión de medios removibles			
										No existen procedimientos de monitorización de las instalaciones	2						14.1.2 Seguridad del servicio de aplicación en redes públicas		
																8.2.1 Clasificación de la información			
																8.2.2 Etiquetado de la información			
																8.2.3 Manejo de activos			
																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			
																11.1.1 Perímetro de seguridad física			

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				
							No existe control para copia de información	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				
					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				
							Eliminación o reutilización de soportes sin borrar	3							13.1.2 Seguridad de servicios de red				
							Gestión del control de acceso ineficiente	2							13.1.3 Segregación de redes				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							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				

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			
						Revelación de información	2	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			
						Revelación de información	2	No existe control para copia de información	2							13.2.2 Acuerdos de intercambio de información			
						Revelación de información	2	No existen procedimientos de autorización para información pública	3							13.2.3 Mensajería electrónica			
						Revelación de información	2	No existen procedimientos para el etiquetado y manejo de la información	3							14.1.2 Seguridad del servicio de aplicación en redes públicas			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							14.1.3 Protección de transacciones en servicio de aplicación			
						Robo de documentación	2	No existen procedimientos de monitorización de las instalaciones	2							12.1.4 Separación de entornos de desarrollo, prueba y operación			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							12.3.1 Copia de seguridad de la información			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							8.3.1 Gestión de medios removibles			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							14.1.2 Seguridad del servicio de aplicación en redes públicas			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							8.2.1 Clasificación de la información			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							8.2.2 Etiquetado de la información			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							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 físico			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							11.1.3 Seguridad de oficinas, salas e instalaciones			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							11.1.5 Trabajo en áreas seguras			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							11.1.6 Áreas de entrega y carga			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							11.2.1 Ubicación y protección de equipos			
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	3							11.1.1 Perímetro de seguridad física			

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				
							No existe control para copia de información	3							8.1.4 Devolución de los activos				
							Acceso remoto no seguro	2							8.3.2 Desecho de medios				
							Conexiones a red pública desprotegidas	2							12.3.1 Copia de seguridad de la información				
							Eliminación o reutilización de soportes sin borrar	3							12.4.1 Registro de eventos				
							Gestión del control de acceso ineficiente	2							6.2.2 Teletrabajo				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							8.3.3 Tránsito de medios físicos				
					Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	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				

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				
							No existe control para copia de información	3							8.1.4 Devolución de los activos				
							Acceso remoto no seguro	2							8.3.2 Desecho de medios				
							Conexiones a red pública desprotegidas	2							12.3.1 Copia de seguridad de la información				
							Eliminación o reutilización de soportes sin borrar	3							12.4.1 Registro de eventos				
							Gestión del control de acceso ineficiente	2							6.2.2 Teletrabajo				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							8.3.3 Tránsito de medios físicos				
					Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	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				

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	DISPONSIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSIBILIDAD						
					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 aplicación en redes públicas			
							No existe control para copia de información	2							14.1.3 Protección de transacciones en servicio de aplicación						
							No existen procedimientos de autorización para información pública	3							12.1.4 Separación de entornos de desarrollo, prueba y operación						
							No existen procedimientos para el etiquetado y manejo de la información	3							12.3.1 Copia de seguridad de la información						
					Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3							8.3.1 Gestión de medios removibles						
																		14.1.2 Seguridad del servicio de aplicación en redes públicas			
							No existen procedimientos de monitorización de las instalaciones	2							8.2.1 Clasificación de la información						
															8.2.2 Etiquetado de la información						
															8.2.3 Manejo de activos						
															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						
															11.1.1 Perímetro de seguridad física						

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				
							No existe control para copia de información	3							8.1.4 Devolución de los activos				
							Acceso remoto no seguro	2							8.3.2 Desecho de medios				
							Conexiones a red pública desprotegidas	2							12.3.1 Copia de seguridad de la información				
							Eliminación o reutilización de soportes sin borrar	3							12.4.1 Registro de eventos				
							Gestión del control de acceso ineficiente	2							6.2.2 Teletrabajo				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							8.3.3 Tránsito de medios físicos				
					Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	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				

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				
Credenciales de ingresos a herramienta tecnológica SUJF	Información	2	4	4	Pérdida de integridad y disponibilidad del activo	1	Uso soportes removibles no controlado	3	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.	Dirección de Financiamiento y Riesgos Agropecuarios	
							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 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 auditoría	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		
						Usó 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 aplicación en redes públicas
								No existe control para copia de información	2										14.1.3 Protección de transacciones en servicio de aplicación	
								No existen procedimientos de autorización para información pública	3										12.1.4 Separación de entornos de desarrollo, prueba y operación	
								No existen procedimientos para el etiquetado y manejo de la información	3										12.3.1 Copia de seguridad de la información	
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3										8.3.1 Gestión de medios removibles	
										No existen procedimientos de monitorización de las instalaciones	2									
																			8.2.1 Clasificación de la información	
																			8.2.2 Etiquetado de la información	
																			8.2.3 Manejo de activos	
																			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	
																			11.1.1 Perímetro de seguridad física	

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				
							No existe control para copia de información	3							8.1.4 Devolución de los activos				
							Acceso remoto no seguro	2							8.3.2 Desecho de medios				
							Conexiones a red pública desprotegidas	2							12.3.1 Copia de seguridad de la información				
							Eliminación o reutilización de soportes sin borrar	3							12.4.1 Registro de eventos				
							Gestión del control de acceso ineficiente	2							6.2.2 Teletrabajo				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							8.3.3 Tránsito de medios físicos				
					Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	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				

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 aplicación en redes públicas		
								No existe control para copia de información	2							14.1.3 Protección de transacciones en servicio de aplicación			
								No existen procedimientos de autorización para información pública	3							12.1.4 Separación de entornos de desarrollo, prueba y operación			
								No existen procedimientos para el etiquetado y manejo de la información	3							12.3.1 Copia de seguridad de la información			
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3							8.3.1 Gestión de medios removibles			
										No existen procedimientos de monitorización de las instalaciones	2						14.1.2 Seguridad del servicio de aplicación en redes públicas		
															8.2.1 Clasificación de la información				
															8.2.2 Etiquetado de la información				
															8.2.3 Manejo de activos				
															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				
															11.1.1 Perímetro de seguridad física				

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				
							No existe control para copia de información	3							8.1.4 Devolución de los activos				
							Acceso remoto no seguro	2							8.3.2 Desecho de medios				
							Conexiones a red pública desprotegidas	2							12.3.1 Copia de seguridad de la información				
							Eliminación o reutilización de soportes sin borrar	3							12.4.1 Registro de eventos				
							Gestión del control de acceso ineficiente	2							6.2.2 Teletrabajo				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							8.3.3 Tránsito de medios físicos				
					Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	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				

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 generados por proyectos de inversión	Información	3	4	2	Pérdida de integridad del activo	1	Uso soportes removibles no controlado	3	18	24	12	12	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 Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Dirección de Financiamiento y Riesgos Agropecuarios																				
							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 Conciliación, educación y capacitación de la seguridad de la información
							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	No existe control sobre el uso de utilidades de sistema	3	No existen registros de auditoría	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	DISPONSIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSIBILIDAD				
						Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información	3							7.2.3 Proceso disciplinario			
						Revelación de información	1	Uso no aceptable de activos	2							8.1.3 Uso aceptable de los activos			
						Revelación de información	1	Comunicaciones a través de redes públicas o desprotegidas	3							13.2.1 Políticas y procedimientos para el intercambio de información			
						Revelación de información	1	No existe control para copia de información	2							13.2.2 Acuerdos de intercambio de información			
						Revelación de información	1	No existen procedimientos de autorización para información pública	3							13.2.3 Mensajería electrónica			
						Revelación de información	1	No existen procedimientos para el etiquetado y manejo de la información	3							14.1.2 Seguridad del servicio de aplicación en redes públicas			
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3							14.1.3 Protección de transacciones en servicio de aplicación			
						Robo de documentación	1	No existen procedimientos de monitorización de las instalaciones	2							12.1.4 Separación de entornos de desarrollo, prueba y operación			
						Robo de documentación	1									12.3.1 Copia de seguridad de la información			
						Robo de documentación	1									8.3.1 Gestión de medios removibles			
						Robo de documentación	1									14.1.2 Seguridad del servicio de aplicación en redes públicas			
						Robo de documentación	1									8.2.1 Clasificación de la información			
						Robo de documentación	1									8.2.2 Etiquetado de la información			
						Robo de documentación	1									8.2.3 Manejo de activos			
						Robo de documentación	1									11.1.2 Controles de acceso físico			
						Robo de documentación	1									11.1.3 Seguridad de oficinas, salas e instalaciones			
						Robo de documentación	1									11.1.5 Trabajo en áreas seguras			
						Robo de documentación	1									11.1.6 Áreas de entrega y carga			
						Robo de documentación	1									11.2.1 Ubicación y protección de equipos			
						Robo de documentación	1									11.1.1 Perímetro de seguridad física			

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				
							No existe control para copia de información	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				
					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				
							Eliminación o reutilización de soportes sin borrar	3							13.1.2 Seguridad de servicios de red				
							Gestión del control de acceso ineficiente	2							13.1.3 Segregación de redes				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							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				

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				
							No existe control para copia de información	3							8.1.4 Devolución de los activos				
							Acceso remoto no seguro	2							8.3.2 Desecho de medios				
							Conexiones a red pública desprotegidas	2							12.3.1 Copia de seguridad de la información				
							Eliminación o reutilización de soportes sin borrar	3							12.4.1 Registro de eventos				
							Gestión del control de acceso ineficiente	2							6.2.2 Teletrabajo				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							8.3.3 Tránsito de medios físicos				
					Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	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				

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																							
Información generada por la herramienta tecnológica SUJFP	Información	2	4	4	Pérdida de integridad y disponibilidad del activo	1	Uso soportes removibles no controlado	3	12	24	12	8	16	8	Aceptar	9.4.3 Sistema de gestión de contraseñas	De conformidad con la Política de Seguridad y Privacidad de la Información, Dirección de Financiamiento y Riesgos Agropecuarios																					
							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 Conciliación, educación y capacitación de la seguridad de la información
							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	No existe control sobre el uso de utilidades de sistema	3	No existen registros de auditoría	3	No existe protección contra código malicioso	2	No existe concienciación y formación en seguridad	3							
							Escuchas no autorizadas	1								Manipulación de los registros			2	Pérdida o corrupción de la información	1	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	DISPONSIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSIBILIDAD						
						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 aplicación en redes públicas
								No existe control para copia de información	2									14.1.3 Protección de transacciones en servicio de aplicación			
								No existen procedimientos de autorización para información pública	3									12.1.4 Separación de entornos de desarrollo, prueba y operación			
								No existen procedimientos para el etiquetado y manejo de la información	3									12.3.1 Copia de seguridad de la información			
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3									8.3.1 Gestión de medios removibles			
																					14.1.2 Seguridad del servicio de aplicación en redes públicas
								No existen procedimientos de monitorización de las instalaciones	2									8.2.1 Clasificación de la información			
																		8.2.2 Etiquetado de la información			
																		8.2.3 Manejo de activos			
																		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			
																		11.1.1 Perímetro de seguridad física			

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				
							No existe control para copia de información	3							8.1.4 Devolución de los activos				
							Acceso remoto no seguro	2							8.3.2 Desecho de medios				
							Conexiones a red pública desprotegidas	2							12.3.1 Copia de seguridad de la información				
							Eliminación o reutilización de soportes sin borrar	3							12.4.1 Registro de eventos				
							Gestión del control de acceso ineficiente	2							6.2.2 Teletrabajo				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							8.3.3 Tránsito de medios físicos				
					Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	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				

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				
Informes de ejecución ICR, LEC, ISA - Incentivo al Seguro Agropecuario, FONSA	Información	3	4	3	Pérdida de integridad del activo		Uso soportes removibles no controlado	3	18	24	9	12	16	6	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, Dirección de Financiamiento y Riesgos Agropecuarios		
							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																			
					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				
							No existe protección contra código malicioso	2							13.1.2 Seguridad de servicios de red				
							No existen procedimientos de monitorización de las instalaciones	3							13.1.3 Segregación de redes				
							Manipulación de los registros	2							12.2.1 Controles contra código malicioso				
							No existe control sobre el uso de utilidades de sistema	3							11.1.2 Controles de acceso físico				
							No existen registros de auditoría	3							11.1.3 Seguridad de oficinas, salas e instalaciones				
							Pérdida o corrupción de la información	1							11.1.5 Trabajo en áreas seguras				
							No existe protección contra código malicioso	2							11.1.6 Áreas de entrega y carga				
							No existe concienciación y formación en seguridad	3							12.7.1 Controles de la auditoría de sistemas de 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			
						Usó 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 aplicación en redes públicas		
								No existe control para copia de información	2							14.1.3 Protección de transacciones en servicio de aplicación			
								No existen procedimientos de autorización para información pública	3							12.1.4 Separación de entornos de desarrollo, prueba y operación			
								No existen procedimientos para el etiquetado y manejo de la información	3							12.3.1 Copia de seguridad de la información			
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3							8.3.1 Gestión de medios removibles			
										No existen procedimientos de monitorización de las instalaciones	2						14.1.2 Seguridad del servicio de aplicación en redes públicas		
															8.2.1 Clasificación de la información				
															8.2.2 Etiquetado de la información				
															8.2.3 Manejo de activos				
															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				
															11.1.1 Perímetro de seguridad física				

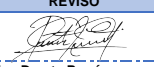
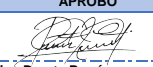
Identificación del riesgo					Análisis del riesgo inherente					Evaluación del nivel de riesgos y definición de controles									
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE 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				
							No existe control para copia de información	3							8.1.4 Devolución de los activos				
							Acceso remoto no seguro	2							8.3.2 Desecho de medios				
							Conexiones a red pública desprotegidas	2							12.3.1 Copia de seguridad de la información				
							Eliminación o reutilización de soportes sin borrar	3							12.4.1 Registro de eventos				
							Gestión del control de acceso ineficiente	2							6.2.2 Teletrabajo				
							No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles				
							No existen procedimientos formales de revisión de accesos	2							8.3.3 Tránsito de medios físicos				
					Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	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				

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																		
Informes de supervisión ICR, LEC, ISA - Incentivo al Seguro Agropecuario, FONSA	Información	3	4	3	Pérdida de integridad del activo	1	Uso soportes removibles no controlado	3	18	24	9	12	16	6	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, Dirección de Financiamiento y Riesgos Agropecuarios																
							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
							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	No existe control sobre el uso de utilidades de sistema	3	No existen registros de auditoría	3	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 Conciliación, educación y capacitación de la seguridad de la información	
							Escuchas no autorizadas	1								Manipulación de los registros			2	Pérdida o corrupción de la información	1	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 aplicación en redes públicas			
							No existe control para copia de información	2							14.1.3 Protección de transacciones en servicio de aplicación												
							No existen procedimientos de autorización para información pública	3							12.1.4 Separación de entornos de desarrollo, prueba y operación												
							No existen procedimientos para el etiquetado y manejo de la información	3							12.3.1 Copia de seguridad de la información												
					Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3							8.3.1 Gestión de medios removibles												
																								14.1.2 Seguridad del servicio de aplicación en redes públicas			
							No existen procedimientos de monitorización de las instalaciones	2							8.2.1 Clasificación de la información												
															8.2.2 Etiquetado de la información												
															8.2.3 Manejo de activos												
															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												
															11.1.1 Perímetro de seguridad física												

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				
						1	Robo de información	1	Eliminación o reutilización de soportes sin borrar	3									
						1	Robo de información	3	No existe control para copia de información	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 físicos

	REVISO	APROBO
Firma		
Nombre	Luis Felipe Duarte Ramirez	Luis Felipe Duarte Ramirez
Cargo	Director de Financiamiento y Riesgos Agropecuarios	Director de Financiamiento y Riesgos Agropecuarios
Fecha	13 de mayo de 2021	13 de mayo de 2021