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

PROCESO: **Gestión de Desarrollo y Modernización de Mercados**

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		
																		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		
								No existen mecanismos de autenticación y validación del usuario	2									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 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	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		

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 y ayudas de memorias	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo			formatos para alta y baja de usuarios	2	36	24	36	24	16	24	Tratar	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 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.	Desarrollo y Modernización de Mercados
								Uso soportes removibles no controlado	3										
						Escuchas no autorizadas	1	Cableado desprotegido	3								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		
								Comunicaciones a través de redes públicas o desprotegidas	2										
								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 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		
								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	2								12.2.1 Controles contra código malicioso		

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				
						Pérdida o corrupción de la información	1	código malicioso	2								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		
								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		

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 documentación	3										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		
						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 físicos		
						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		
								Conexiones a red pública desprotegidas	2								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		
								No existen mecanismos de autenticación y validación del usuario	2								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 procedimientos formales de revisión de accesos	2								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		

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
Bases de datos	Información	3	4	4	Perdida de integridad y disponibilidad del activo			No existen procedimientos formales para alta y baja de usuarios	2	18	24	12	12	16	8	Aceptar	9.2.3 Gestión de derechos de acceso privilegiado	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	Desarrollo y Modernización de Mercados
																	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		
								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		
																	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		
								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	2								12.2.1 Controles contra código malicioso		

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				
						Pérdida o corrupción de la información	1	código malicioso	2								12.3.1 Copia de seguridad de la información	fin.	
						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		
								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 físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		

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 documentación	1										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		
						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 físicos		
						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		
								Conexiones a red pública desprotegidas	2								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		
								No existen mecanismos de autenticación y validación del usuario	2								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 procedimientos formales de revisión de accesos	2								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		

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				
Carpeta compartida	Información	4	4	3	Perdida de confidencialidad y integridad del activo			No existen procedimientos formales para alta y baja de usuarios	2	24	24	18	16	16	12	Aceptar	9.2.3 Gestión de derechos de acceso privilegiado	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	Desarrollo y Modernización de Mercados
																	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		
								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		
																	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		
								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	2								12.2.1 Controles contra código malicioso		

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
						Pérdida o corrupción de la información	1	código malicioso	2								12.3.1 Copia de seguridad de la información	fin.	
						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		
								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 físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		

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 documentación	2										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		
						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 físicos		
						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		
								Conexiones a red pública desprotegidas	2								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		
								No existen mecanismos de autenticación y validación del usuario	2								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 procedimientos formales de revisión de accesos	2								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		

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
Informes	Información	3	4	4	Perdida de integridad y disponibilidad del activo			No existen procedimientos formales para alta y baja de usuarios	2	18	24	12	12	16	8	Aceptar	9.2.3 Gestión de derechos de acceso privilegiado	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	Desarrollo y Modernización de Mercados
																	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		
								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		
																	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		
								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	2								12.2.1 Controles contra código malicioso		

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				
						Pérdida o corrupción de la información	1	código malicioso	2								12.3.1 Copia de seguridad de la información	fin.	
						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		
								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 físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		

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 documentación	1										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		
						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 físicos		
						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		
								Conexiones a red pública desprotegidas	2								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		
								No existen mecanismos de autenticación y validación del usuario	2								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 procedimientos formales de revisión de accesos	2								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		

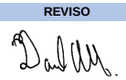
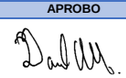
Identificación del riesgo						Análisis del riesgo inherente											Evaluación del nivel de riesgos y definición de controles			
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Memorandos de entendimiento, planes, programas y proyectos.	Información	3	4	4	Perdida de integridad y disponibilidad del activo			No existen procedimientos formales para alta y baja de usuarios	2	18	24	12	12	16	8	Aceptar	9.2.3 Gestión de derechos de acceso privilegiado	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	Desarrollo y Modernización de Mercados
																	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		
								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		
																	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		
								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	2								12.2.1 Controles contra código malicioso		

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
						Pérdida o corrupción de la información	1	código malicioso	2								12.3.1 Copia de seguridad de la información	fin.	
						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		
								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 físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		

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 documentación	1										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		
						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 físicos		
						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		
								Gestión de actualizaciones de seguridad ineficiente	2								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		
								Gestión ineficiente de contraseñas	2								9.2.3 Gestión de derechos de acceso privilegiado		
																	9.2.4 Gestión de información secreta de autenticación		
								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		

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
Sistema Agrocomercio	Software	1	1	3	Perdida de disponibilidad del activo	Fallo de sistemas	1	Configuración de parámetros errónea	3	0	0	24	0	0	16	Aceptar	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 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 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 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 12.4.1 Registro de eventos 14.2.8 Pruebas de seguridad del sistema 14.2.9 Pruebas de aceptación del sistema	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	Desarrollo y Modernización de Mercados
								Especificaciones para desarrolladores incompletas o confisas	3										
								Fallos conocidos en inversiones	3										
								Gestión de actualizaciones de seguridad ineficiente	3										
								No exiten registros de auditoría	3										
								Prubas de software insuficientes	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				
																	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		
						Uso de sistemas por usuarios no autorizados	1	Acceso remoto no seguro	3								10.1.1 Política en el uso de controles criptográficos		
																	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		
								Asgnación errónea de derechos de acceso	2								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		

	REVISO	APROBO
Firma		
Nombre	**Daniel Arboleda Cortes**	**Daniel Arboleda Cortes**
Cargo	**Jefe de Oficina de Asuntos Internacionales**	Jefe de Oficina de Asuntos Internacionales
Fecha	12 de mayo de 2021	12 de mayo de 2021