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

PROCESO: **Control Interno a la Gestión**

SECCION B: RIESGOS DE SEGURIDAD DE LA INFORMACION

Identificación del riesgo						Análisis del riesgo inherente									Evaluación del nivel de riesgos y definición de controles								
		EVALUACION DE LA CRITICIDAD DEL ACTIVO							NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL										
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red		
								Conexiones a red pública desprotegidas	2								13.1.1 Controles de red		
																	13.1.2 Seguridad de servicios de red		
																	13.1.3 Segregación de redes		
								Eliminación o reutilización de soportes sin borrar	3								8.3.1 Gestión de medios removibles		
																	8.3.2 Desecho de medios		
								Gestión del control de acceso ineficiente	2								9.4.1 Restricción del acceso a la información		
								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		
																	9.1.1 Política de control de acceso		
																	9.2.1 Alta y baja de usuario		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles						
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Actas	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo			No existen procedimientos formales para alta y baja de usuarios	2	27	24	36	18	16	24	Tratar	9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación 9.4.3 Sistema de gestión de contraseña 8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 8.3.3 Tránsito de medios fisicos 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 fisico 11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga 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	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Jefe Oficina Control Interno a la Gestión
								Uso soportes removibles no controlado	3											
						Escuchas no autorizadas	1	Cableado desprotegido	3											
								Comunicaciones a través de redes públicas o desprotegidas	2											
								No existe protección contra código malicioso	2											
								No existen procedimientos de monitorización de las instalaciones	2											
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3											
								No existen registros de auditoria	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				
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
						Revelación de contraseñas	2	No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		
								No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3								13.2.1 Políticas y procedimientos para el intercambio de información		
																	13.2.2 Acuerdos de intercambio de información		
																	13.2.3 Mensajería electrónica		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
																	14.1.3 Protección de transacciones en servicio de aplicación		
								No existe control para copia de información	2								12.1.4 Separación de entornos de desarrollo, prueba y operación		
																	12.3.1 Copia de seguridad de la información		
								No existen procedimientos de autorización para información pública	3								8.3.1 Gestión de medios removibles		
																	14.1.2 Seguridad del servicio de aplicacion en redes públicas		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.1 Clasificación de la información		
																	8.2.2 Etiquetado de la información		
																	8.2.3 Manejo de activos		
								Control de acceso al edificio y a									11.1.2 Controles de acceso físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		

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	Control de acceso al edificio y a las salas ineficiente	3								11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad física		
						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		

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				
Auditorías de gestión	Información	2	4	4	Perdida de integridad y disponibilidad del activo			No existen procedimientos formales para alta y baja de usuarios	2	12	24	24	8	16	16	Aceptar	9.2.2 Provisión de acceso a usuarios	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	Jefe Oficina Control Interno a la Gestión
																	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		
								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	2	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		

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	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso	se realiza directamente en la plataforma dispuesta para tal fin.	
																	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		
																	11.1.2 Controles de acceso físico		
								Control de acceso al edificio y a									11.1.3 Seguridad de oficinas, salas e instalaciones		

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	Control de acceso al edificio y a las salas ineficiente	3								11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad física		
						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		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles						
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Planes de mejoramiento Contraloría General de la República.	Información	2	4	4	Perdida de integridad y disponibilidad del activo			No existen procedimientos formales para alta y baja de usuarios	2	12	24	12	8	16	8	Aceptar	9.2.2 Provisión de acceso a usuarios	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	Jefe Oficina Control Interno a la Gestión
																	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		
								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		

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	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso	se realiza directamente en la plataforma dispuesta para tal fin.	
																	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		
																	11.1.2 Controles de acceso físico		
								Control de acceso al edificio y a									11.1.3 Seguridad de oficinas, salas e instalaciones		

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	Control de acceso al edificio y a las salas ineficiente	3									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			
								No existen procedimientos de monitorización de las instalaciones	2											
						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 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes			
								Conexiones a red pública desprotegidas	2									8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios			
								Eliminación o reutilización de soportes sin borrar	3									9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad			
								Gestión del control de acceso ineficiente	2									9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario			
								No existen mecanismos de autenticación y validación del usuario	2											
								No existen procedimientos formales de revisión de accesos	2											

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles			
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Programa anual de auditoria	Información	2	4	4	Perdida de integridad y disponibilidad del activo			No existen procedimientos formales para alta y baja de usuarios	2	12	24	24	8	16	16	Aceptar	9.2.2 Provisión de acceso a usuarios	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	Jefe Oficina Control Interno a la Gestión
																	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		
								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	2	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		

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	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso	se realiza directamente en la plataforma dispuesta para tal fin.	
																	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		
								Control de acceso al edificio y a									11.1.2 Controles de acceso físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		

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	Control de acceso al edificio y a las salas ineficiente	3								11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga 11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad fisica		
						Robo de información	2	Eliminación o reutilización de soportes sin borrar	3								11.2.7 Seguridad en el desecho o reutilización de equipos 8.1.4 Devolución de los activos 8.3.2 Desecho de medios		
								No existe control para copia de información	3								12.3.1 Copia de seguridad de la información 12.4.1 Registro de eventos 6.2.2 Teletrabajo 8.3.1 Gestión de medios removibles 8.3.3 Tránsito de medios fisicos		
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								Conexiones a red pública desprotegidas	2								8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios		
								Eliminación o reutilización de soportes sin borrar	3								9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad		
								Gestión del control de acceso ineficiente	2								9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario		
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles						
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Requerimientos de la contraloría	Información	3	4	4	Perdida de integridad y disponibilidad del activo			No existen procedimientos formales para alta y baja de usuarios	2	18	24	24	12	16	16	Aceptar	9.2.2 Provisión de acceso a usuarios	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	Jefe Oficina Control Interno a la Gestión
																	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		
								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		

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	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso	se realiza directamente en la plataforma dispuesta para tal fin.	
																	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		
																	11.1.2 Controles de acceso físico		
								Control de acceso al edificio y a									11.1.3 Seguridad de oficinas, salas e instalaciones		

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	Control de acceso al edificio y a las salas ineficiente	3								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			
								No existen procedimientos de monitorización de las instalaciones	2										
						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			

	REVISO	APROBO
Firma		
Nombre	**Ana Marlene Huertas López**	**Ana Marlene Huertas López**
Cargo	Jefe Oficina de Control Interno	Jefe Oficina de Control Interno
Fecha	5 de mayo de 2021	5 de mayo de 2021