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

PROCESO: **Capacidades Productivas y Generación de Ingresos**

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 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación 9.4.3 Sistema de gestión de contraseña 8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.3.1 Gestión de medios removibles		
								Conexiones a red pública desprotegidas	2												
								Eliminación o reutilización de soportes sin borrar	3												
								Gestión del control de acceso ineficiente	2												
								No existen mecanismos de autenticación y validación del usuario	2												
								No existen procedimientos formales de revisión de accesos	2												
								No existen procedimientos formales para alta y baja de usuarios	2												
								Uso soportes removibles no controlado	3												

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
Contratos y convenios alianzas productivas	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	12	16	16	8	Aceptar	8.3.2 Desecho de medios	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 Capacidades Productivas y Generación de Ingresos
																	8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.1 Controles de red		
																	13.1.2 Seguridad de servicios de red		
								No existe protección contra código malicioso	2								13.1.3 Segregación de redes		
																	12.2.1 Controles contra código malicioso		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.2 Controles de acceso físico		
																	11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
						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		

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 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 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 existe control para copia de información	2								14.1.2 Seguridad del servicio de aplicacion en redes públicas 8.2.1 Clasificación de la información 8.2.2 Etiquetado de la información 8.2.3 Manejo de activos		
								No existen procedimientos de autorización para información pública	3								11.1.2 Controles de acceso físico 11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga 11.2.1 Ubicación y protección de equipos 11.1.1 Perímetro de seguridad física		
								No existen procedimientos para el etiquetado y manejo de la 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		
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	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		
								No existen procedimientos de monitorización de las instalaciones	2								9.1.2 Acceso a redes y servicios de red		
						Robo de información	1	Eliminación o reutilización de soportes sin borrar	3										
								No existe control para copia de información	3										
								Acceso remoto no seguro	2										

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	Conexiones a red pública desprotegidas	2								13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								Eliminación o reutilización de soportes sin borrar	3								8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios		
								Gestión del control de acceso ineficiente	2								9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario		
								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		
								No existen procedimientos formales para alta y baja de usuarios	2								6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación 9.4.3 Sistema de gestión de contraseña		
								Uso soportes removibles no controlado	3								8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 8.3.3 Tránsito de medios físicos		
						Escuchas no autorizadas	1	Cableado desprotegido	3								11.2.3 Seguridad del cableado		
								Comunicaciones a través de redes públicas o desprotegidas	2								13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 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		

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
Contratos y convenios capacidades productivas	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	12	16	16	8	Aceptar	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 7.2.3 Proceso disciplinario 8.1.3 Uso aceptable de los activos 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 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 14.1.2 Seguridad del servicio de aplicacion en redes públicas 8.2.1 Clasificación de la información 8.2.2 Etiquetado de la información 8.2.3 Manejo de activos 11.1.2 Controles de acceso físico 11.1.3 Seguridad de oficinas, salas e instalaciones	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 Capacidades Productivas y Generación de Ingresos
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3										
								No existen registros de auditoria	3										
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2										
						Revelación de contraseñas	2	No existe concienciación y formación en seguridad	3										
								No existen procesos disciplinarios claros para incidentes de seguridad de la información	3										
								Uso no aceptable de activos	2										
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3										
								No existe control para copia de información	2										
								No existen procedimientos de autorización para información pública	3										
								No existen procedimientos para el etiquetado y manejo de la información	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				
						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 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		
								No existen procedimientos de monitorización de las instalaciones	2										
						Robo de información	1	Eliminación o reutilización de soportes sin borrar	3										
								No existe control para copia de información	3										
						Acceso no autorizado	1	Acceso remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes 8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios 9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación		
								Conexiones a red pública desprotegidas	2										
								Eliminación o reutilización de soportes sin borrar	3										
								Gestión del control de acceso ineficiente	2										
								No existen mecanismos de autenticación y validación del usuario	2										
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles							
		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
Documentos de calidad	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	24	16	16	16	Aceptar	9.4.3 Sistema de gestión de contraseña 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 7.2.3 Proceso disciplinario 8.1.3 Uso aceptable de los activos 13.2.1 Políticas y procedimientos para el intercambio de información 13.2.2 Acuerdos de intercambio de información 13.2.3 Mensajería electrónica	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 Capacidades Productivas y Generación de Ingresos
								Uso soportes removibles no controlado	3										
						Escuchas no autorizadas	1	Cableado desprotegido	3										
								Comunicaciones a través de redes públicas o desprotegidas	2										
								No existe protección contra código malicioso	2										
								No existen procedimientos de monitorización de las instalaciones	3										
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3										
								No existen registros de auditoria	3										
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2										
						Revelación de contraseñas	2	No existe concienciación y formación en seguridad	3										
								No existen procesos disciplinarios claros para incidentes de seguridad de la información	3										
								Uso no aceptable de activos	2										
								Comunicaciones a través de	3										

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
						Revelación de información	2	redes públicas o desprotegidas									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 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 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		
								Eliminación o reutilización de soportes sin borrar	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				
								Soportes sin borrar									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		
						Acceso no autorizado	1										6.2.2 Teletrabajo		
								No existen procedimientos formales para alta y baja de usuarios	2								9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación 9.4.3 Sistema de gestión de contraseña		
								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		
								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		
						Escuchas no autorizadas	1	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		
								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	De conformidad con la	

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
Documentos de política	Información	4	4	3	Perdida de confidencialidad y integridad del activo	Manipulación de los registros	2	No existen registros de auditoria	3	24	24	18	16	16	12	Aceptar	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 7.2.3 Proceso disciplinario 8.1.3 Uso aceptable de los activos 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 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 14.1.2 Seguridad del servicio de aplicacion en redes públicas 8.2.1 Clasificación de la información 8.2.2 Etiquetado de la información 8.2.3 Manejo de activos 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	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 Capacidades Productivas y Generación de Ingresos
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2										
						Revelación de contraseñas	2	No existe concienciación y formación en seguridad	3										
								No existen procesos disciplinarios claros para incidentes de seguridad de la información	3										
								Uso no aceptable de activos	2										
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3										
								No existe control para copia de información	2										
								No existen procedimientos de autorización para información pública	3										
								No existen procedimientos para el etiquetado y manejo de la información	3										
						Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente	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				
								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 remoto no seguro	2								9.1.2 Acceso a redes y servicios de red 13.1.1 Controles de red 13.1.2 Seguridad de servicios de red 13.1.3 Segregación de redes		
								Conexiones a red pública desprotegidas	2								8.3.1 Gestión de medios removibles 8.3.2 Desecho de medios		
								Eliminación o reutilización de soportes sin borrar	3								9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad		
								Gestión del control de acceso ineficiente	2								9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo		
								No existen mecanismos de autenticación y validación del usuario	2								9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación 9.4.3 Sistema de gestión de contraseña		
								No existen procedimientos formales de revisión de accesos	2								8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos		
						Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	2										
								Uso soportes removibles no											

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 de bases de datos de contratos y convenios	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo			Uso soportes removibles no controlado	3	24	24	12	16	16	8	Aceptar	8.3.1 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 7.2.3 Proceso disciplinario 8.1.3 Uso aceptable de los activos 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	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 Capacidades Productivas y Generación de Ingresos
						Escuchas no autorizadas	1	Cableado desprotegido	3											
								Comunicaciones a través de redes públicas o desprotegidas	2											
								No existe protección contra código malicioso	2											
								No existen procedimientos de monitorización de las instalaciones	3											
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3											
								No existen registros de auditoria	3											
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2											
						Revelación de contraseñas	2	No existe concienciación y formación en seguridad	3											
								No existen procesos disciplinarios claros para incidentes de seguridad de la información	3											
								Uso no aceptable de activos	2											
								Comunicaciones a través de redes públicas o desprotegidas	3											

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
						Revelación de información	2	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 8.2.1 Clasificación de la información		
								No existen procedimientos para el etiquetado y manejo de la información	3								8.2.2 Etiquetado de la información 8.2.3 Manejo de activos		
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3								11.1.2 Controles de acceso físico 11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga 11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad física		
						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 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 9.4.2 Procesos de inicio seguro de sesión		
								No existen mecanismos de											

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Informes Dirección de Capacidades y Generación de Ingresos.	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo	Acceso no autorizado	1	autenticación y validación del usuario	2	24	24	12	16	16	8	Aceptar	9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad 9.2.5 Revisión de los derechos de acceso de usuarios 6.2.2 Teletrabajo 9.1.1 Política de control de acceso 9.2.1 Alta y baja de usuario 9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación 9.3.1 Uso de información secreta de autenticación 9.4.3 Sistema de gestión de contraseña 8.1.1 Inventario de activos 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	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	Dirección de Capacidades Productivas y Generación de Ingresos
								No existen procedimientos formales de revisión de accesos	2										
								No existen procedimientos formales para alta y baja de usuarios	2										
								Uso soportes removibles no controlado	3										
						Escuchas no autorizadas	1	Cableado desprotegido	3										
								Comunicaciones a través de redes públicas o desprotegidas	2										
								No existe protección contra código malicioso	2										
								No existen procedimientos de monitorización de las instalaciones	3										
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3										
								No existen registros de auditoria	3										

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 12.3.1 Copia de seguridad de la información	implementación de controles se realiza directamente en la plataforma dispuesta para tal 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 11.1.6 Áreas de entrega y carga 11.2.1 Ubicación y protección de equipos		
								No existen procedimientos de monitorización de las instalaciones	2								11.1.1 Perímetro de seguridad física		
								Eliminación o reutilización de	3								11.2.7 Seguridad en el desecho o reutilización de equipos		

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

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
Otros contratos y convenios	Información	4	4	3	Perdida de confidencialidad y integridad del activo	Escuchas no autorizadas	1	Comunicaciones a través de redes públicas o desprotegidas	2	24	24	9	16	16	6	Aceptar	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 7.2.3 Proceso disciplinario 8.1.3 Uso aceptable de los activos 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 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	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 Capacidades Productivas y Generación de Ingresos
								No existe protección contra código malicioso	2												
								No existen procedimientos de monitorización de las instalaciones	3												
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3												
								No existen registros de auditoria	3												
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2												
						Revelación de contraseñas	2	No existe concienciación y formación en seguridad	3												
								No existen procesos disciplinarios claros para incidentes de seguridad de la información	3												
								Uso no aceptable de activos	2												
						Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas	3												
								No existe control para copia de información	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				
								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 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		

	REVISO	APROBO
Firma		
Nombre	**Sergio Enrique Rámirez Payares**	**Sergio Enrique Rámirez Payares**
Cargo	Director de Capacidades Productivas y Generación de Ingresos	Director de Capacidades Productivas y Generación de Ingresos
Fecha	5 de mayo de 2021	5 de mayo de 2021