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

PROCESO: **Control Interno Disciplinario**

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
Conocimiento Apoyo a la gestión	Procesos	3		3	Perdida de confidencialidad y disponibilidad del activo	Gestión ineficiente de la seguridad de la información	2	Gestión de las políticas de seguridad de la información insuficiente	3	24		24	12		12	Aceptar	18.2.2 Cumplimiento de políticas y normas de seguridad 5.1.1 Políticas para la seguridad de la información 5.1.2 Revisión de las políticas para la seguridad de la información 6.1.5 Seguridad de la información en la gestión de proyectos	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.	Control Interno Disciplinario
								No existe contacto con otras organizaciones y grupos de interés	3								6.1.3 Contacto con las autoridades 6.1.4 Contacto con grupos de interés especial		
								No existe documentacion	2								12.1.1 Procedimientos operativos documentados		
								No existe plan de continuidad	4								17.1.1 Planificacion de la continuidad de la seguridad de la información 17.1.2 Implementación de la continuidad de la seguridad de la información 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información 17.2.1 Disponibilidad de las instalaciones de procesamiento de información		
								No existe procedimiento para la gestión de incidencias de seguridad	3								16.1.1 Responsabilidades y procedimientos 16.1.2 Reporte de eventos sobre la seguridad de la información 16.1.3 Reporte de debilidades en la seguridad de la información 16.1.4 Valoración y decisión sobre los eventos de seguridad de la información 16.1.5 Respuesta a los incidentes de seguridad de la información 16.1.6 Aprendizaje de los incidentes de seguridad de la información 16.1.7 Recolección de evidencias		
								Gestión inadecuada de terceras partes	3								15.1.2 Seguridad en el acuerdo con proveedores 18.2.1 Revisión independiente de la seguridad de la información		
								No existen auditorías regulares	4								18.2.1 Revisión independiente de la seguridad de la información 18.2.2 Cumplimiento de políticas y normas de seguridad		

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				
						Incumplimiento legal, reglamentario o contractual	2											18.2.2 Cumplimiento de politicas y normas de seguridad		
																		18.2.3 Revisión de cumplimiento técnico		
																		18.2.3 Revisión de cumplimiento técnico		
								No existen procedimientos para cumplimiento de la propiedad intelectual	2									18.1.2 Derechos de propiedad intelectual		
								No existen requisitos de seguridad en contratos de empleados	3									6.1.1 Roles y responsabilidades de la seguridad de la información		
																		7.1.2 Términos y condiciones del puesto de trabajo		
																		7.2.1 Responsabilidades de la dirección		
								Violación de la legislación aplicable	4									18.1.1 Identificación de legislación aplicable y requisitos contractuales		
																		18.1.1 Identificación de legislación aplicable y requisitos contractuales		
																		18.1.2 Derechos de propiedad intelectual		
																		18.1.3 Protección de registros		
																		18.1.4 Privacidad y protección de información de identificación personal		
																		18.1.4 Privacidad y protección de información de identificación personal		
																		18.1.5 Regulación de controles de criptografía		
																		18.1.5 Regulación de controles de criptografía		
																		18.2.2 Cumplimiento de politicas y normas de seguridad		
																		18.2.3 Revisión de cumplimiento técnico		
						Acceso no autorizado	1	Acceso remoto no seguro	2									9.1.2 Acceso a redes y servicios de red		
								Conexiones a red pública desprotegidas	2									13.1.1 Controles de red		
																		13.1.2 Seguridad de servicios de red		
																		13.1.3 Segregación de redes		
								Eliminación o reutilización de soportes sin borrar	3									8.3.1 Gestión de medios removibles		
																		8.3.2 Desecho de medios		
								Gestión del control de acceso ineficiente	2									9.4.1 Restricción del acceso a la información		
																		9.2.1 Alta y baja de usuario		
								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		
								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		

Identificación del riesgo						Análisis del riesgo inherente										Evaluación del nivel de riesgos y definición de controles					
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Documentos excel de relacion de expedientes	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	24	16	16	16	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.	Control Interno Disciplinario
																	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		
						Revelación de información	1	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		

Identificación del riesgo						Análisis del riesgo inherente																
		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
								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 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		
								Conexiones a red pública desprotegidas	2								9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad		
								Eliminación o reutilización de soportes sin borrar	3								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		
								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										
						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 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		
								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								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	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de	Control Interno
								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
Expedientes	Información	4	4	4	Pérdida de confidencialidad, integridad y disponibilidad del activo			No existen registros de auditoría	3	24	24	24	16	16	16	Aceptar	12.4.3 Registro de administrador y operador 12.4.4 Sincronización de reloj	Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Disciplinario
						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	1	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 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		
								No existen procedimientos de monitorización de las instalaciones	2								11.2.1 Ubicación y protección de equipos 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 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 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		
								Gestión del control de acceso ineficiente	2								9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión		
								No existen mecanismos de autenticación y											

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 de gestión	Información	2	4	4	Perdida de integridad y disponibilidad del activo	Acceso no autorizado	1	No existen mecanismos de autenticación y validación del usuario	2	12	24	12	8	16	8	Aceptar	9.4.3 Sistema de gestión de contraseña	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Control Interno Disciplinario
																	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		
																	11.1.2 Controles de acceso físico		
								No existen procedimientos de monitorización de las instalaciones	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
																	12.4.1 Registro de eventos		
								No existen registros de auditoria	3								12.4.2 Protección de la información del registro de eventos		
																	12.4.3 Registro de administrador y operador		
																	12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso		
																	12.3.1 Copia de seguridad de la información		
						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		
																	13.2.1 Políticas y procedimientos para el intercambio de información		
								Comunicaciones a través de redes públicas o desprotegidas	3								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		

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 8.2.2 Etiquetado de la información 8.2.3 Manejo de activos		
								No existen procedimientos para el etiquetado y manejo de la información	3								11.1.2 Controles de acceso físico		
						Robo de documentación	1	Control de acceso al edificio y a las salas ineficiente	3								11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga 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		
								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 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		

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				
Inhibitorios	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo					24	24	24	16	16	16	Aceptar	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 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 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	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.	Control Interno Disciplinario
						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											
						Revelación de información	1	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	1	Control de acceso al edificio y a las salas ineficiente	3											
								No existen procedimientos de monitorización de las instalaciones	2											
								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				
						Robo de información	2	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		
Remisiones por competencia	Información	3	4	3	Perdida de integridad del activo	Acceso no autorizado	1	Acceso remoto no seguro	2	18	24	18	12	16	12	Aceptar	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	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.	Control Interno Disciplinario
								Conexiones a red pública desprotegidas	2								9.4.1 Restricción del acceso a la información 9.2.1 Alta y baja de usuario 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseña 9.4.4 Uso de programas privilegiados de utilidad		
								Eliminación o reutilización de soportes sin borrar	3								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		
								Gestión del control de acceso ineficiente	2								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		
								No existen mecanismos de autenticación y validación del usuario	2								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		
								No existen procedimientos formales de revisión de accesos	2								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		
								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										
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	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
						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	1	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		
						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		
								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		

Identificación del riesgo						Análisis del riesgo inherente								Evaluación del nivel de riesgos y definición de controles							
ACTIVOS DE INFORMACION	TIPO DE ACTIVO	EVALUACION DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACION DE LA AMENAZA	VULNERABILIDAD	VALORACION DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCION DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONSABILIDAD				
Repositorio de documentos	Información	4	4	4	Perdida de confidencialidad, integridad y disponibilidad del activo	Acceso no autorizado	1	No existen procedimientos formales para alta y baja de usuarios	2	12	24	18	8	16	12	Aceptar	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	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 Disciplinario
								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 fisico 11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga		
						Manipulación de los registros	2	No existe control sobre el uso de utilidades de sistema	3								12.7.1 Controles de la auditoría de sistemas de información		
								No existen registros de auditoria	3								12.4.1 Registro de eventos 12.4.2 Protección de la información del registro de eventos 12.4.3 Registro de administrador y operador 12.4.4 Sincronización de reloj		
						Pérdida o corrupción de la información	1	No existe protección contra código malicioso	2								12.2.1 Controles contra código malicioso 12.3.1 Copia de seguridad de la información		
						Revelación de contraseñas	2	No existe concienciación y formación en seguridad	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		
								No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								7.2.3 Proceso disciplinario		
								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		

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 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		
								No existen procedimientos de monitorización de las instalaciones	2								11.2.1 Ubicación y protección de equipos		
																	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 a soportes no autorizado	2	Instalación desprotegida	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
																	11.1.5 Trabajo en áreas seguras		
																	11.1.6 Áreas de entrega y carga		
																	11.2.1 Ubicación y protección de equipos		
																	11.2.3 Seguridad del cableado		
								Uso no aceptable de activos	3								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		
						Daño por agua	2	Susceptibilidad a polvo, humedad	3								11.1.4 Protección contra amenazas externas y ambientales		
																	11.2.1 Ubicación y protección de equipos		
						Daño por tercera parte	2	Gestión inadecuada de terceras partes	3								15.1.1 Política de seguridad en la relación con proveedores		
																	15.1.2 Seguridad en el acuerdo con proveedores		
																	15.1.3 Tecnología de la información y comunicacion en la cadena de suminitro		
								No existe concienciación y formación en seguridad	3								7.2.1 Responsabilidades de la dirección		
																	7.2.2 Concienciación, educación y capacitación de la seguridad de la información		
								No existe supervisión de terceros dentro de la organización	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
								Proceso de contratación ineficiente	3								15.2.2 Gestión de cambios en la provisión de servicios		
																	7.1.2 Términos y condiciones del puesto de trabajo		
								Exposición a temperaturas extremas	3								11.1.4 Protección contra amenazas externas y ambientales		
								No existe sistema estabilizador de tensión	3								11.2.2 Servicios de suministro		

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				
Expedientes medio magnéticos	Físico			4	Perdida de disponibilidad del activo	Destrucción	2	Uso incorrecto de equipos	3			24			16	Aceptar	11.2.6 Seguridad de equipos y activos fuera de las instalaciones 7.2.2 Concienciación, educación y capacitación de la seguridad de la información 8.1.3 Uso aceptable de los activos 11.2.4 Mantenimiento 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.	Control Interno Disciplinario
						Deterioro de los soportes	1	Mantenimiento insuficiente	2										
						Falta de mantenimiento de equipos	1	Gestión de cambios innneficiente	2								12.1.2 Gestión del cambio		
								Mantenimiento insuficiente	2								11.2.4 Mantenimiento de equipos		
								No existe gestión de activos	2								8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos		
								Planificación y monitorización de capacidad inadecuada	2								12.1.3 Gestión de la capacidad		
						Fuego	2	No existen equipos de detección de incendios	3								11.1.3 Seguridad de oficinas, salas e instalaciones		
								No existen equipos de extinción de incendios	3								11.1.4 Protección contra amenazas externas y ambientales		
						Inundación	2	Ubicaciones susceptibles e inundación	3								11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.4 Protección contra amenazas externas y ambientales		
						Manipulación de los equipos	1	No existe control de los activos fuera de las instalaciones	3								11.2.1 Ubicación y protección de equipos 11.2.5 Retirada de activos 11.2.6 Seguridad de equipos y activos fuera de las instalaciones		
								No existe gestión de activos	2								8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.1.4 Devolución de los activos		
								No existe procedimientos para el control de cambios	2								12.1.2 Gestión del cambio		
								No existen políticas para el uso de dispositivos portátiles	2								6.2.1 Política de dispositivos móviles		
								Uso no aceptable de activos	2								8.1.3 Uso aceptable de los activos		
						Polvo, humedad, corrosión	2	Exposición a humedad, polvo, suciedad	3								11.1.4 Protección contra amenazas externas y ambientales 11.2.1 Ubicación y protección de equipos 11.2.4 Mantenimiento de equipos		
						Recuperación de medios reciclados o descartados	1	No existe gestión de activos	2								8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.1.4 Devolución de los activos		
								No existen procedimientos para devolución de activos	2								8.3.1 Gestión de medios removibles		
																	11.1.1 Perímetro de seguridad física 11.1.2 Controles de acceso físico 11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.6 Áreas de entrega y carga		
								Instalación desprotegida	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
						Robo de equipamento	1										11.2.1 Ubicación y protección de equipos		
								No existe gestión de activos	2								8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
								No existen políticas para el uso de dispoositivos portátiles	3								11.2.5 Retirada de activos		
																	11.2.6 Seguridad de equipos y activos fuera de las instalaciones		
																	6.2.1 Política de dispositivos móviles