



FORMATO
MAPA DE RIESGOS

VERSION
12
F01-PR-SIG-05
FECHA EDICIÓN
28/04/2021

PROCESO:

SECCIÓN B: RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN DE LA CRITICIDAD DEL ACTIVO			RIESGO	AMENAZA	VALORACIÓN DE LA AMENAZA	VULNERABILIDAD	VALORACIÓN DE VULNERABILIDAD	NIVEL DE RIESGO INHERENTE			NIVEL DE RIESGO RESIDUAL			OPCIÓN DE TRATAMIENTO	CONTROL	Soporte	Responsable
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
						Aceso no autorizado	1	Acceso remoto no seguro	2							9.1.2 Acceso a redes y servicios de red			
								Conexiones a red pública desprotegidas	2							13.1.1 Controles de red			
								Eliminación o reutilización de soportes sin borrar	3							13.1.2 Seguridad de servicios de red			
								Gestión del control de acceso ineficiente	2							13.1.3 Segregación de redes			
								No existen mecanismos de autenticación y validación del usuario	2							8.3.1 Gestión de medios removibles			
								No existen procedimientos formales de revisión de accesos	2							8.3.2 Desecho de medios			
								No existen procedimientos formales para alta y baja de usuarios	2							9.4.1 Restricción del acceso a la información			
								Uso soportes removibles no controlado	3							9.2.1 Alta y baja de usuario			
								Cableado desprotegido	3							9.4.2 Procesos de inicio seguro de sesión			
								Comunicaciones a través de redes públicas o desprotegidas	2							9.4.3 Sistema de gestión de contraseña			
								No existe protección contra código malicioso	2							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			

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
Esquema bases de datos de los sistemas de información Operativos.	Información	4	4	4	Pérdida de confidencialidad, integridad y disponibilidad del activo		No existen procedimientos de monitorización de las instalaciones	2							Aceptar	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 implementación de controles se realiza directamente en la plataforma dispuesta para tal fin.	Jefe Oficina TIC	
							No existe control sobre el uso de utilidades de sistema	3											11.1.5 Trabajo en áreas seguras
							No existen registros de auditoría	3	24	24	24	16	16	16		11.1.6 Áreas de entrega y carga			
							No existe protección contra código malicioso	2								12.7.1 Controles de la auditoría de sistemas de información			
							No existe concienciación y formación en seguridad	3								12.4.1 Registro de eventos			
							No existen procesos disciplinarios claros para incidentes de seguridad de la información	3								12.4.2 Protección de la información del registro de eventos			
							Uso no aceptable de activos	2								12.4.3 Registro de administrador y operador			
							Comunicaciones a través de redes públicas o desprotegidas	3								12.4.4 Sincronización de reloj			
							No existe control para copia de información	2								12.2.1 Controles contra código malicioso			
							No existen procedimientos de autorización para información pública	3								12.3.1 Copia de seguridad de la información			
							No existen procedimientos para el etiquetado y manejo de la información	3								7.2.2 Concienciación, educación y capacitación de la seguridad de la información			
							Control de acceso al edificio y a las salas ineficiente	3								7.2.3 Proceso disciplinario			
							No existen procedimientos de monitorización de las instalaciones	2								8.1.3 Uso aceptable de los activos			
	Eliminación o reutilización de soportes sin borrar	3							13.2.1 Políticas y procedimientos para el intercambio de información										
									13.2.2 Acuerdos de intercambio de información										
									13.2.3 Mensajería electrónica										
									14.1.2 Seguridad del servicio de aplicación en redes públicas										
									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 aplicación en redes públicas										
									8.2.1 Clasificación de la información										
									8.2.2 Etiquetado de la información										
									8.2.3 Manejo de activos										
									11.1.2 Controles de acceso físico										
									11.1.3 Seguridad de oficinas, salas e instalaciones										
									11.1.5 Trabajo en áreas seguras										
									11.1.6 Áreas de entrega y carga										
									11.2.1 Ubicación y protección de equipos										
									11.1.1 Perímetro de seguridad física										
									11.2.7 Seguridad en el desecho o reutilización de equipos										
									8.1.4 Devolución de los activos										

Identificación del riesgo			Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles										
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
Información Institucional cargada en los sistemas de información operativos	Información	4	4	4	Pérdida de confidencialidad, integridad y disponibilidad del activo	1	Cableado desprotegido	3	24	24	24	16	16	16	Aceptar	13.1.3 Segregación de redes	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 TIC	
							Eliminación o reutilización de soportes sin borrar	3								8.3.1 Gestión de medios removibles			
							Gestión del control de acceso ineficiente	2								8.3.2 Desecho de medios			
							No existen mecanismos de autenticación y validación del usuario	2								9.4.1 Restricción del acceso a la información			
							No existen procedimientos formales de revisión de accesos	2								9.2.1 Alta y baja de usuario			
							No existen procedimientos formales para alta y baja de usuarios	2								9.4.2 Procesos de inicio seguro de sesión			
							Uso soportes removibles no controlado	3								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																	
		12.2.1 Controles contra código malicioso																	
		12.3.1 Copia de seguridad de la información																	
		7.2.2 Concienciación, educación y capacitación de la seguridad de la información																	

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
					Revelación de contraseñas	2	No existen procesos disciplinarios claros para incidentes de seguridad de la información Uso no aceptable de activos	3 2							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 aplicación 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 aplicación en redes públicas 8.2.1 Clasificación de la información 8.2.2 Etiquetado de la información 8.2.3 Manejo de activos 11.1.2 Controles de acceso físico 11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.5 Trabajo en áreas seguras 11.1.6 Áreas de entrega y carga 11.2.1 Ubicación y protección de equipos 11.1.1 Perímetro de seguridad física 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				
					Revelación de información	2	Comunicaciones a través de redes públicas o desprotegidas No existe control para copia de información No existen procedimientos de autorización para información pública No existen procedimientos para el etiquetado y manejo de la información	3 2 3 3											
					Robo de documentación	2	Control de acceso al edificio y a las salas ineficiente No existen procedimientos de monitorización de las instalaciones	3 2											
					Robo de información	1	Eliminación o reutilización de soportes sin borrar No existe control para copia de información	3 3											
							Fallos conocidos en inversiones Gestión de actualizaciones de seguridad ineficiente	3 2							12.6.1 Gestión de vulnerabilidades técnicas 12.6.2 Restricciones en la instalación de programas 14.2.4 Restricciones en cambios a paquetes de aplicaciones 12.5.1 Instalación de programas en sistemas en producción 14.2.2 Procedimiento de control de cambio en sistemas de información				

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles																
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD												
Sistema ORFEO	Software	1	1	4	Pérdida de disponibilidad del activo	Elevación de privilegios	2								Aceptar	14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación	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 TIC									
						Gestión ineficiente de contraseñas	2													9.2.3 Gestión de derechos de acceso privilegiado							
						No existen registros de auditoría	3													9.2.4 Gestión de información secreta de autenticación							
						Fallo de sistemas	1	Configuración de parámetros errónea	3													12.4.1 Registro de eventos					
								Especificaciones para desarrolladores incompletas o confusas	3													12.4.2 Protección de la información del registro de eventos					
								Fallos conocidos en inversiones	3	0	0	24	0	0		16						12.4.3 Registro de administrador y operador					
								Gestión de actualizaciones de seguridad ineficiente	3	No existen registros de auditoría	3													12.4.4 Sincronización de reloj			
												Pruebas de software insuficientes	3													14.1.1 Análisis y especificaciones de requisitos de seguridad de la información	
																											14.2.1 Política de desarrollo seguro
																											14.2.5 Principios para la ingeniería de sistemas seguros
						Incumplimiento legal, reglamentario o contractual	2	Validación de la legislación aplicable	3												14.2.6 Entorno seguro de desarrollo						
						Uso de sistemas con usuarios no																		14.2.7 Desarrollo externalizado			
																								Acesso remoto no seguro			3
																								12.6.1 Gestión de vulnerabilidades técnicas			
																								14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación			
															14.2.4 Restricciones en cambios a paquetes de aplicaciones												
															12.5.1 Instalación de programas en sistemas en producción												
															12.6.1 Gestión de vulnerabilidades técnicas												
															12.6.2 Restricciones en la instalación de programas												
															14.2.2 Procedimiento de control de cambio en sistemas de información												
															14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación												
															14.2.4 Restricciones en cambios a paquetes de aplicaciones												
															12.4.1 Registro de eventos												
															14.2.8 Pruebas de seguridad del sistema												
															14.2.9 Pruebas de aceptación del sistema												
															14.3.1 Protección de la información de prueba												
															10.1.1 Política en el uso de controles criptográficos												
															18.1.2 Derechos de propiedad intelectual												
															10.1.1 Política en el uso de controles criptográficos												
															10.1.2 Gestión de claves de criptografía												
															9.1.2 Acceso a redes y servicios de red												
															9.4.2 Procesos de inicio seguro de sesión												
															9.4.3 Sistema de gestión de contraseña												

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
					Uso de sistemas por usuarios no autorizados	1	Asignación errónea de derechos de acceso	2							9.2.2 Provisión de acceso a usuarios 9.2.3 Gestión de derechos de acceso privilegiado 9.2.5 Revisión de los derechos de acceso de usuarios 9.2.6 Retirada o ajuste de los derechos de acceso				
					Acceso a soportes no autorizado	2	Instalación desprotegida Uso no aceptable de activos	3 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 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				
					Daños 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 No existe concienciación y formación en seguridad No existe supervisión de terceros dentro de la organización Proceso de contratación ineficiente	3 3 3 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 comunicación en la cadena de suministro 7.2.1 Responsabilidades de la dirección 7.2.2 Concienciación, educación y capacitación de la seguridad de la información				
					Destrucción	2	Exposición a temperaturas extremas No existe sistema estabilizador de tensión Uso incorrecto de equipos	3 3 3							11.1.3 Seguridad de oficinas, salas e instalaciones 15.2.2 Gestión de cambios en la provisión de servicios 7.1.2 Términos y condiciones del puesto de trabajo 11.1.4 Protección contra amenazas externas y ambientales 11.2.2 Servicios de suministro 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				
					Deterioro de los soportes	1	Mantenimiento insuficiente	2							11.2.4 Mantenimiento de equipos 8.1.1 Inventario de activos				
					Falta de mantenimiento de equipos	1	Gestión de cambios ineficiente Mantenimiento insuficiente No existe gestión de activos	2 2 2							8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos				

De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del

Identificación del riesgo					Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles							
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
Servidores Físicos	Físico	1	1	4	Pérdida de disponibilidad del activo		Planificación y monitorización de capacidad inadecuada	2	0	0	24	0	0	16	Aceptar	12.1.3 Gestión de la capacidad	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 TIC	
						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 a 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
								No existe gestión de activos								2			11.2.5 Retirada de activos
								No existe procedimiento para el control de cambios								2			11.2.6 Seguridad de equipos y activos fuera de las instalaciones
								No existen políticas para el uso de dispositivos portátiles								2			8.1.1 Inventario de activos
								Uso no aceptable de activos								2			8.1.2 Propiedad de los activos
						Polvo, humedad, corrosión	2	Exposición a humedad, polvo, suciedad								3			8.1.3 Uso aceptable de los activos
																			12.1.2 Gestión del cambio
						Recuperación de medios reciclados o descartados	1	No existe gestión de activos								2			6.2.1 Política de dispositivos móviles
								No existe procedimiento para devolución de activos								2			8.1.3 Uso aceptable de los activos
Robo de equipamiento	1	Instalación desprotegida	3	11.1.4 Protección contra amenazas externas y ambientales															
				No existe gestión de activos	2	11.2.1 Ubicación y protección de equipos													
				No existen políticas para el uso de dispositivos portátiles	3	11.2.2 Mantenimiento de equipos													
				No existen procedimiento para devolución de activos	2	8.1.1 Inventario de activos													
															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				
															11.2.1 Ubicación y protección de equipos				
															8.1.1 Inventario de activos				
															8.1.2 Propiedad de los activos				
															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				
															8.1.4 Devolución de los activos				
															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						Evaluación del nivel de riesgos y definición de controles											
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD							
Equipos de Aire Acondicionado	Físico	1	1	4	Pérdida de disponibilidad del activo	Acceso a soportes no autorizado	2									11.2.3 Seguridad del cableado	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 controles se realiza directamente en la plataforma dispuesta para tal fin	Jefe Oficina TIC				
						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	
																						11.1.4 Protección contra amenazas externas y ambientales
																						11.2.1 Ubicación y protección de equipos
																						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 comunicación en la cadena de suministro
																						7.2.1 Responsabilidades de la dirección
																						7.2.2 Concienciación, educación y capacitación de la seguridad de la información
																						11.1.3 Seguridad de oficinas, salas e instalaciones
																						15.2.2 Gestión de cambios en la provisión de servicios
																						7.1.2 Términos y condiciones del puesto de trabajo
														11.1.4 Protección contra amenazas externas y ambientales								
														11.2.2 Servicios de suministro								
														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								
														12.1.2 Gestión del cambio								
														11.2.4 Mantenimiento de equipos								
														8.1.1 Inventario de activos								
														8.1.2 Propiedad de los activos								
														8.1.3 Uso aceptable de los activos								
									0	0	24	0	0	16	12.1.3 Gestión de la capacidad							
															11.1.3 Seguridad de oficinas, salas e instalaciones							
															11.1.4 Protección contra amenazas externas y ambientales							
															11.1.3 Seguridad de oficinas, salas e instalaciones							
															11.1.4 Protección contra amenazas externas y ambientales							
															11.2.1 Ubicación y protección de equipos							

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
					Manipulación de los equipos	1	No existe control de los activos fuera de las instalaciones	3							11.2.5 Retirada de activos				
							No existe gestión de activos	2							11.2.6 Seguridad de equipos y activos fuera de las instalaciones				
							No existe procedimiento para el control de cambios	2							8.1.1 Inventario de activos				
							No existen políticas para el uso de dispositivos portátiles	2							8.1.2 Propiedad de los activos				
							Uso no aceptable de activos	2							8.1.3 Uso aceptable de los activos				
					Polvo, humedad, corrosión	2	Exposición a humedad, polvo, suciedad	3							8.1.4 Devolución de los activos				
					Recuperación de medios reciclados o descartados	1	No existe gestión de activos	2							12.1.2 Gestión del cambio				
							No existe procedimiento para devolución de activos	2							6.2.1 Política de dispositivos móviles				
					Robo de equipamiento	1	Instalación desprotegida	3							8.1.3 Uso aceptable de los activos				
							No existe gestión de activos	2							11.1.4 Protección contra amenazas externas y ambientales				
							No existen políticas para el uso de dispositivos portátiles	3							11.2.1 Ubicación y protección de equipos				
							No existen procedimiento para devolución de activos	2							11.2.4 Mantenimiento de equipos				
															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				
															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				
															11.2.1 Ubicación y protección de equipos				
															8.1.1 Inventario de activos				
															8.1.2 Propiedad de los activos				
															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				
															8.1.4 Devolución de los activos				
					Acceso a soportes no autorizado	2	Instalación desprotegida	3							11.1.3 Seguridad de oficinas, salas e instalaciones				
							Uso no aceptable de activos	3							11.1.5 Trabajo en áreas seguras				
															11.1.6 Áreas de entrega y carga				
															11.2.1 Ubicación y protección de equipos				
															11.2.3 Seguridad del cableado				
															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				
					Daños 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				
															15.1.1 Política de seguridad en la relación con proveedores				
							Gestión inadecuada de terceras partes	3							15.1.2 Seguridad en el acuerdo con proveedores				

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
Equipos de Conectividad estándar	Físico	1	1	3	Pérdida de disponibilidad del activo	Daño por tercera parte	No existe concienciación y formación en seguridad	2	3	0	0	18	0	0	12	Aceptar	15.1.3 Tecnología de la información y comunicación en la cadena de suministro	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 TIC
							No existe supervisión de terceros dentro de la organización	3	7.2.1 Responsabilidades de la dirección										
							Proceso de contratación ineficiente	3	7.2.2 Concienciación, educación y capacitación de la seguridad de la información										
									11.1.3 Seguridad de oficinas, salas e instalaciones										
						Destrucción	Exposición a temperaturas extremas	2	3								15.2.2 Gestión de cambios en la provisión de servicios		
							No existe sistema estabilizador de tensión	3	3								7.1.2 Términos y condiciones del puesto de trabajo		
							Uso incorrecto de equipos	3	3								11.1.4 Protección contra amenazas externas y ambientales		
						Deterioro de los soportes	1	1	2								11.2.2 Servicios de suministro		
						Falta de mantenimiento de equipos	Gestión de cambios ineficiente	1	2								11.2.6 Seguridad de equipos y activos fuera de las instalaciones		
							Mantenimiento insuficiente	2	2								7.2.2 Concienciación, educación y capacitación de la seguridad de la información		
							No existe gestión de activos	2	2								8.1.3 Uso aceptable de los activos		
							Planificación y monitorización de capacidad inadecuada	2	2								11.2.4 Mantenimiento de equipos		
						Fuego	No existen equipos de detección de incendios	2	3								12.1.2 Gestión del cambio		
							No existen equipos de extinción de incendios	3	3								11.2.4 Mantenimiento de equipos		
						Inundación	Ubicaciones susceptibles a inundación	2	3								8.1.1 Inventario de activos		
																	8.1.2 Propiedad de los activos		
						Manipulación de los equipos	No existe control de los activos fuera de las instalaciones	1	3								8.1.3 Uso aceptable de los activos		
							No existe gestión de activos	2	2								12.1.3 Gestión de la capacidad		
							No existe procedimiento para el control de cambios	2	2								11.1.3 Seguridad de oficinas, salas e instalaciones		
							No existen políticas para el uso de dispositivos portátiles	2	2								11.1.4 Protección contra amenazas externas y ambientales		
Uso no aceptable de activos	2	2	11.1.3 Seguridad de oficinas, salas e instalaciones																
				11.1.4 Protección contra amenazas externas y ambientales															
				11.1.3 Seguridad de oficinas, salas e instalaciones															
				11.1.4 Protección contra amenazas externas y ambientales															
				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															
				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															
				12.1.2 Gestión del cambio															
				6.2.1 Política de dispositivos móviles															
				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 INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
					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 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				
					Recuperación de medios reciclados o descartados	1	No existe gestión de activos	2							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 11.2.1 Ubicación y protección de equipos				
					Robo de equipamiento	1	Instalación desprotegida	3							8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 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				
							No existe gestión de activos	2								8.1.4 Devolución de los activos			
							No existen políticas para el uso de dispositivos portátiles	3											
							No existen procedimiento para devolución de activos	2											
					Elevación de privilegios	1	Fallos conocidos en inversiones	3							12.6.1 Gestión de vulnerabilidades técnicas 12.6.2 Restricciones en la instalación de programas 14.2.4 Restricciones en cambios a paquetes de aplicaciones 12.5.1 Instalación de programas en sistemas en producción 14.2.2 Procedimiento de control de cambio en sistemas de información 14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación 9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación				
							Gestión de actualizaciones de seguridad ineficiente	2								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			
							Gestión ineficiente de contraseñas	2								14.1.1 Análisis y especificaciones de requisitos de seguridad de la información 14.2.1 Política de desarrollo seguro 14.2.5 Principios para la ingeniería de sistemas seguros 14.2.6 Entorno seguro de desarrollo 14.2.7 Desarrollo externalizado			
							No existen registros de auditoria	3								9.4.5 Control de acceso a código fuente de programa	De conformidad con la		
							Configuración de parámetros errónea	3											
					Especificaciones para desarrolladores incompletas o confusas	3													

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles																							
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD																			
Servicios de nube pública	Software	1	1	4	Pérdida de disponibilidad del activo	Fallo de sistemas	Fallos conocidos en inversiones	3	0	0	24	0	0	16	Aceptar	12.6.1 Gestión de vulnerabilidades técnicas	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 TIC																
							Gestión de actualizaciones de seguridad ineficiente	3								14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación																		
							No existen registros de auditoría	3								14.2.4 Restricciones en cambios a paquetes de aplicaciones																		
							Pruebas de software insuficientes	3								12.5.1 Instalación de programas en sistemas en producción																		
						Incumplimiento legal, reglamentario o contractual	2	Validación de la legislación aplicable								3			12.6.1 Gestión de vulnerabilidades técnicas															
						Uso de sistemas por usuarios no autorizados	1	Acceso remoto no seguro								3			12.6.2 Restricciones en la instalación de programas															
								Asignación errónea de derechos de acceso								2			14.2.2 Procedimiento de control de cambio en sistemas de información															
																					Elevar de privilegios	2								10.1.1 Política en el uso de controles criptográficos				
																														Fallos conocidos en inversiones			3	18.1.2 Derechos de propiedad intelectual
																														Gestión de actualizaciones de seguridad ineficiente			2	10.1.1 Política en el uso de controles criptográficos
Gestión ineficiente de contraseñas	2	10.1.2 Gestión de claves de criptografía																																
		9.1.2 Acceso a redes y servicios de red																																
		9.4.2 Procesos de inicio seguro de sesión																																
		9.4.3 Sistema de gestión de contraseña																																
		9.2.2 Provisión de acceso a usuarios																																
		9.2.3 Gestión de derechos de acceso privilegiado																																
		9.2.5 Revisión de los derechos de acceso de usuarios																																
		9.2.6 Retirada o ajuste de los derechos de acceso																																
															12.6.1 Gestión de vulnerabilidades técnicas																			
															12.6.2 Restricciones en la instalación de programas																			
															14.2.4 Restricciones en cambios a paquetes de aplicaciones																			
															12.5.1 Instalación de programas en sistemas en producción																			
															14.2.2 Procedimiento de control de cambio en sistemas de información																			
															14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación																			
															9.2.3 Gestión de derechos de acceso privilegiado																			
															9.2.4 Gestión de información secreta de autenticación																			

Identificación del riesgo			Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles										
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
					Inundación	2	Ubicaciones susceptibles a inundación	3							11.1.3 Seguridad de oficinas, salas e instalaciones 11.1.4 Protección contra amenazas externas y ambientales 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 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 12.1.2 Gestión del cambio 6.2.1 Política de dispositivos móviles 8.1.3 Uso aceptable de los activos 11.1.4 Protección contra amenazas externas y ambientales 11.2.1 Ubicación y protección de equipos 11.2.4 Mantenimiento de equipos 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 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 11.2.1 Ubicación y protección de equipos 8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 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 8.1.4 Devolución de los activos				
					Manipulación de los equipos	1	No existe control de los activos fuera de las instalaciones No existe gestión de activos No existe procedimiento para el control de cambios No existen políticas para el uso de dispositivos portátiles Uso no aceptable de activos	3 2 2 2 2											
					Polvo, humedad, corrosión	2	Exposición a humedad, polvo, suciedad	3											
					Recuperación de medios reciclados o descartados	1	No existe gestión de activos No existe procedimiento para devolución de activos	2 2											
					Robo de equipamiento	1	Instalación desprotegida No existe gestión de activos No existen políticas para el uso de dispositivos portátiles No existen procedimientos para devolución de activos	3 2 3 2											
					Elevación de privilegios	2	Fallos conocidos en inversiones Gestión de actualizaciones de seguridad ineficiente	3 2							12.6.1 Gestión de vulnerabilidades técnicas 12.6.2 Restricciones en la instalación de programas 14.2.4 Restricciones en cambios a paquetes de aplicaciones 12.5.1 Instalación de programas en sistemas en producción 14.2.2 Procedimiento de control de cambio en sistemas de información 14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación				

Identificación del riesgo			Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles												
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD						
Sistemas Operativos de Usuario Final	Software	1	1	2	Pérdida de disponibilidad del activo	Fallo de sistemas	2	Gestión ineficiente de contraseñas	2	0	0	12	0	0	8	Adequar	9.2.3 Gestión de derechos de acceso privilegiado	De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin	Jefe Oficina TIC		
								No existen registros de auditoría	3								9.2.4 Gestión de información secreta de autenticación				
								Configuración de parámetros errónea	3								12.4.1 Registro de eventos				
								Especificaciones para desarrolladores incompletas o confusas	3								12.4.2 Protección de la información del registro de eventos				
								Fallos conocidos en inversiones	3								12.4.3 Registro de administrador y operador				
								Gestión de actualizaciones de seguridad ineficiente	3								12.4.4 Sincronización de reloj				
								No existen registros de auditoría	3								14.1.1 Análisis y especificaciones de requisitos de seguridad de la información				
								Pruebas de software insuficientes	3								14.2.1 Política de desarrollo seguro				
								Incumplimiento legal, reglamentario o contractual	2								Validación de la legislación aplicable			3	14.2.5 Principios para la ingeniería de sistemas seguros
								Uso de sistemas por usuarios no autorizados	1								Acceso remoto no seguro			3	14.2.6 Entorno seguro de desarrollo
																					14.2.7 Desarrollo externalizado
																					9.4.5 Control de acceso a código fuente de programa
																					12.6.1 Gestión de vulnerabilidades técnicas

Identificación del riesgo					Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles							
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
							Pruebas de software insuficientes	0							14.2.9 Pruebas de aceptación del sistema 14.3.1 Protección de la información de prueba				
					Incumplimiento legal, reglamentario o contractual	2	Validación de la legislación aplicable	3							10.1.1 Política en el uso de controles criptográficos 18.1.2 Derechos de propiedad intelectual				
					Uso de sistemas por usuarios no autorizados	1	Acceso remoto no seguro	3							10.1.1 Política en el uso de controles criptográficos 10.1.2 Gestión de claves de criptografía 9.1.2 Acceso a redes y servicios de red 9.4.2 Procesos de inicio seguro de sesión 9.4.3 Sistema de gestión de contraseñas 9.2.2 Provisión de acceso a usuarios				
							Asignación errónea de derechos de acceso	2								9.2.3 Gestión de derechos de acceso privilegiado 9.2.5 Revisión de los derechos de acceso de usuarios 9.2.6 Retirada o ajuste de los derechos de acceso			
					Elevación de privilegios	2	Fallos conocidos en inversiones	3							12.6.1 Gestión de vulnerabilidades técnicas 12.6.2 Restricciones en la instalación de programas				
							Gestión de actualizaciones de seguridad ineficiente	2								14.2.4 Restricciones en cambios a paquetes de aplicaciones 12.5.1 Instalación de programas en sistemas en producción 14.2.2 Procedimiento de control de cambio en sistemas de información 14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación			
							Gestión ineficiente de contraseñas	2								9.2.3 Gestión de derechos de acceso privilegiado 9.2.4 Gestión de información secreta de autenticación			
							No existen registros de auditoría	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			
							Configuración de parámetros errónea	3							14.1.1 Análisis y especificaciones de requisitos de seguridad de la información 14.2.1 Política de desarrollo seguro 14.2.5 Principios para la ingeniería de sistemas seguros 14.2.6 Entorno seguro de desarrollo 14.2.7 Desarrollo externalizado				
							Especificaciones para desarrolladores incompletas o confusas	3								9.4.5 Control de acceso a código fuente de programa			
							Fallos conocidos en inversiones	3								12.6.1 Gestión de vulnerabilidades técnicas 14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación			
Software de Escritorio	Software	1	1	2	Pérdida de disponibilidad del activo					0	0	12	0	0	8	Aceptar	14.2.4 Restricciones en cambios a paquetes de aplicaciones	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	Jefe Oficina TIC

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles																			
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD															
Software de Seguridad Local	Software	1	1	3	Pérdida de disponibilidad del activo	Fallo de sistemas	1	Configuración de parámetros errónea	3	0	0	18	0	0	12	Aceptar	14.1.1 Análisis y especificaciones de requisitos de seguridad de la información	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 TIC											
								Especificaciones para desarrolladores incompletas o confusas	3								14.2.1 Política de desarrollo seguro			14.2.5 Principios para la ingeniería de sistemas seguros	14.2.6 Entorno seguro de desarrollo	14.2.7 Desarrollo externalizado	9.4.5 Control de acceso a código fuente de programa	12.6.1 Gestión de vulnerabilidades técnicas	14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación	14.2.4 Restricciones en cambios a paquetes de aplicaciones	12.5.1 Instalación de programas en sistemas en producción	12.6.1 Gestión de vulnerabilidades técnicas	12.6.2 Restricciones en la instalación de programas	14.2.2 Procedimiento de control de cambio en sistemas de información
					Incumplimiento legal, reglamentario o contractual	2	Validación de la legislación aplicable	3									10.1.1 Política en el uso de controles criptográficos													
					Uso de sistemas por usuarios no autorizados	1	Acceso remoto no seguro	3									10.1.1 Política en el uso de controles criptográficos													
							Asignación errónea de derechos de acceso	2									10.1.2 Gestión de claves de criptografía													
																	9.1.2 Acceso a redes y servicios de red													
																	9.4.2 Procesos de inicio seguro de sesión													
																	9.4.3 Sistema de gestión de contraseñas													
																	9.2.2 Provisión de acceso a usuarios													
																	9.2.3 Gestión de derechos de acceso privilegiado													
																	9.2.5 Revisión de los derechos de acceso de usuarios													
																	9.2.6 Retirada o ajuste de los derechos de acceso													
					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													

Identificación del riesgo			Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles														
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD								
Equipos de Seguridad Informática	Físico	1	1	4	Pérdida de disponibilidad del activo		Uso no aceptable de activos	3							Aceptar	7.2.2 Concienciación, educación y capacitación de la seguridad de la información	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 TIC					
																				7.2.3 Proceso disciplinario			
																					8.1.3 Uso aceptable de los activos		
																						11.1.4 Protección contra amenazas externas y ambientales	
																						11.2.1 Ubicación y protección de equipos	
																						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 comunicación en la cadena de suministro	
																							7.2.1 Responsabilidades de la dirección
																							7.2.2 Concienciación, educación y capacitación de la seguridad de la información
																							11.1.3 Seguridad de oficinas, salas e instalaciones
																							15.2.2 Gestión de cambios en la provisión de servicios
																							7.1.2 Términos y condiciones del puesto de trabajo
																							11.1.4 Protección contra amenazas externas y ambientales
														11.2.2 Servicios de suministro									
														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									
														12.1.2 Gestión del cambio									
														11.2.4 Mantenimiento de equipos									
														8.1.1 Inventario de activos									
														8.1.2 Propiedad de los activos									
														8.1.3 Uso aceptable de los activos									
									0	0	24	0	0	16	12.1.3 Gestión de la capacidad								
															11.1.3 Seguridad de oficinas, salas e instalaciones								
															11.1.3 Seguridad de oficinas, salas e instalaciones								
															11.1.4 Protección contra amenazas externas y ambientales								
															11.1.3 Seguridad de oficinas, salas e instalaciones								
															11.1.4 Protección contra amenazas externas y ambientales								
															11.2.1 Ubicación y protección de equipos								
															11.2.5 Retirada de activos								

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
															11.2.6 Seguridad de equipos y activos fuera de las instalaciones 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 12.1.2 Gestión del cambio 6.2.1 Política de dispositivos móviles 8.1.3 Uso aceptable de los activos 11.1.4 Protección contra amenazas externas y ambientales 11.2.1 Ubicación y protección de equipos 11.2.4 Mantenimiento de equipos 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 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 11.2.1 Ubicación y protección de equipos 8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 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 8.1.4 Devolución de los activos				
					Manipulación de los equipos	1	No existe control de los activos fuera de las instalaciones	3											
							No existe gestión de activos	2											
							No existe procedimiento para el control de cambios	2											
							No existen políticas para el uso de dispositivos portátiles	2											
							Uso no aceptable de activos	2											
					Polvo, humedad, corrosión	2	Exposición a humedad, polvo, suciedad	3											
					Recuperación de medios reciclados o descartados	1	No existe gestión de activos	2											
							No existe procedimiento para devolución de activos	2											
					Robo de equipamiento	1	Instalación desprotegida	3											
							No existe gestión de activos	2											
							No existen políticas para el uso de dispositivos portátiles	3											
							No existen procedimiento para devolución de activos	2											
Servicio de Telefonía	Servicios	1	1	2	Pérdida de disponibilidad del activo	2	No existe procedimiento para el control de cambios	2				12		8	15.2.2 Gestión de cambios en la provisión de servicios 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 comunicación en la cadena de suministro 15.2.1 Monitorización y revisión de la provisión de servicios	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 TIC		
Servicio de Conectividad	Servicios	1	1	4	Pérdida de disponibilidad del activo	2	No existe procedimiento para el control de cambios	2				24		16	15.2.2 Gestión de cambios en la provisión de servicios 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 comunicación en la cadena de suministro	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	Jefe Oficina TIC		

Identificación del riesgo					Análisis del riesgo inherente					Evaluación del nivel de riesgos y definición de controles									
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
															15.2.1 Monitorización y revisión de la provisión de servicios	se realiza directamente en la plataforma dispuesta para tal fin			
Servidores Virtuales	Software	1	1	4	Pérdida de disponibilidad del activo	Elevación de privilegios	Fallos conocidos en inversiones	3	0	0	24	0	0	16	Aceptar	12.6.1 Gestión de vulnerabilidades técnicas	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 TIC	
							Gestión de actualizaciones de seguridad ineficiente	2								12.6.2 Restricciones en la instalación de programas			
							Gestión ineficiente de contraseñas	2								14.2.4 Restricciones en cambios a paquetes de aplicaciones			
							No existen registros de auditoría	3								12.5.1 Instalación de programas en sistemas en producción			
						Fallo de sistemas	1	Configuración de parámetros errónea								3			14.2.2 Procedimiento de control de cambio en sistemas de información
								Especificaciones para desarrolladores incompletas o confusas								3			14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación
								Fallos conocidos en inversiones								3			9.2.3 Gestión de derechos de acceso privilegiado
								Gestión de actualizaciones de seguridad ineficiente								3			9.2.4 Gestión de información secreta de autenticación
								No existen registros de auditoría								3			12.4.1 Registro de eventos
								Pruebas de software insuficientes								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
																			14.1.1 Análisis y especificaciones de requisitos de seguridad de la información
																			14.2.1 Política de desarrollo seguro
		14.2.5 Principios para la ingeniería de sistemas seguros																	
		14.2.6 Entorno seguro de desarrollo																	
		14.2.7 Desarrollo externalizado																	
		9.4.5 Control de acceso a código fuente de programa																	
		12.6.1 Gestión de vulnerabilidades técnicas																	
		14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación																	
		14.2.4 Restricciones en cambios a paquetes de aplicaciones																	
		12.5.1 Instalación de programas en sistemas en producción																	
		12.6.1 Gestión de vulnerabilidades técnicas																	
		12.6.2 Restricciones en la instalación de programas																	
		14.2.2 Procedimiento de control de cambio en sistemas de información																	
		14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación																	
		14.2.4 Restricciones en cambios a paquetes de aplicaciones																	
		12.4.1 Registro de eventos																	
		14.2.8 Pruebas de seguridad del sistema																	
		14.2.9 Pruebas de aceptación del sistema																	
		14.3.1 Protección de la información de prueba																	

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
					Incumplimiento legal, reglamentario o contractual	2	Validación de la legislación aplicable	3							10.1.1 Política en el uso de controles criptográficos				
					Uso de sistemas por usuarios no autorizados	1	Acceso remoto no seguro	3							18.1.2 Derechos de propiedad intelectual				
							Asignación errónea de derechos de acceso	2								10.1.1 Política en el uso de controles criptográficos			
					Acceso a soportes no autorizado	2	Instalación desprotegida	3							10.1.2 Gestión de claves de criptografía				
							Uso no aceptable de activos	3								9.1.2 Acceso a redes y servicios de red			
					Daños por agua	2	Susceptibilidad a polvo, humedad	3							9.4.2 Procesos de inicio seguro de sesión				
					Daño por tercera parte	2	Gestión inadecuada de terceras partes	3							9.4.3 Sistema de gestión de contraseñas				
							No existe concienciación y formación en seguridad	3								9.2.2 Provisión de acceso a usuarios			
							No existe supervisión de terceros dentro de la organización	3								9.2.3 Gestión de derechos de acceso privilegiado			
							Proceso de contratación ineficiente	3								9.2.5 Revisión de los derechos de acceso de usuarios			
					Destrucción	2	Exposición a temperaturas extremas	3							9.2.6 Retirada o ajuste de los derechos de acceso				
							No existe sistema estabilizador de tensión	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				
															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				
															11.1.4 Protección contra amenazas externas y ambientales				
															11.2.1 Ubicación y protección de equipos				
															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 comunicación en la cadena de suministro				
															7.2.1 Responsabilidades de la dirección				
															7.2.2 Concienciación, educación y capacitación de la seguridad de la información				
															11.1.3 Seguridad de oficinas, salas e instalaciones				
															15.2.2 Gestión de cambios en la provisión de servicios				
															7.1.2 Términos y condiciones del puesto de trabajo				
															11.1.4 Protección contra amenazas externas y ambientales				
															11.2.2 Servicios de suministro				
															11.2.6 Seguridad de equipos y activos fuera de las instalaciones				

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
Equipos de Energía	Físico	1	1	4	Pérdida de disponibilidad del activo		Uso incorrecto de equipos	3	0	0	24	0	0	16	Aceptar	7.2.2 Concienciación, educación y capacitación de la seguridad de la información	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 TIC	
						Deterioro de los soportes	1	Mantenimiento insuficiente								2			8.1.3 Uso aceptable de los activos
						Falta de mantenimiento de equipos	1	Gestión de cambios ineficiente								2			11.2.4 Mantenimiento de equipos
								Mantenimiento insuficiente								2			12.1.2 Gestión del cambio
								No existe gestión de activos								2			11.2.4 Mantenimiento de equipos
						Fuego	2	No existen equipos de detección de incendios								3			8.1.1 Inventario de activos
								No existen equipos de extinción de incendios								3			8.1.2 Propiedad de los activos
						Inundación	2	Ubicaciones susceptibles a inundación								3			8.1.3 Uso aceptable de los activos
																			12.1.3 Gestión de la capacidad
						Manipulación de los equipos	1	No existe control de los activos fuera de las instalaciones								3			11.1.3 Seguridad de oficinas, salas e instalaciones
								No existe gestión de activos								2			11.1.4 Protección contra amenazas externas y ambientales
								No existe procedimiento para el control de cambios								2			11.1.3 Seguridad de oficinas, salas e instalaciones
								No existen políticas para el uso de dispositivos portátiles								2			11.1.4 Protección contra amenazas externas y ambientales
								Uso no aceptable de activos								2			11.2.1 Ubicación y protección de equipos
						Polvo, humedad, corrosión	2	Exposición a humedad, polvo, suciedad								3			11.2.5 Retirada de activos
																			11.2.6 Seguridad de equipos y activos fuera de las instalaciones
						Recuperación de medios reciclados o descartados	1	No existe gestión de activos								2			8.1.1 Inventario de activos
																			No existe procedimiento para devolución de activos
						Robo de equipamiento	1	Instalación desprotegida								3			8.1.3 Uso aceptable de los activos
																			No existe gestión de activos
		12.1.2 Gestión del cambio																	
				6.2.1 Política de dispositivos móviles															
				8.1.3 Uso aceptable de los activos															
				11.1.4 Protección contra amenazas externas y ambientales															
				11.2.1 Ubicación y protección de equipos															
				11.2.4 Mantenimiento de equipos															
				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															
				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															
				11.2.1 Ubicación y protección de equipos															
				8.1.1 Inventario de activos															
				8.1.2 Propiedad de los activos															
				11.2.5 Retirada de activos															

Identificación del riesgo					Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles							
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
							No existen políticas para el uso de dispositivos portátiles	3							11.2.6 Seguridad de equipos y activos fuera de las instalaciones				
							No existen procedimiento para devolución de activos	2							6.2.1 Política de dispositivos móviles				
							No existe procedimiento para el control de cambios	2							8.1.4 Devolución de los activos				
Servicios de Administración, Gestión y Soporte	Servicios	1	1	4	Perdida de disponibilidad del activo	Fallo en la provisión	No existen acuerdos de calidad del servicio (SLA)	3				24			15.2.2 Gestión de cambios en la provisión de servicios	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 TIC		
						Acceso a soportes no autorizado	Instalación desprotegida	3							11.1.3 Seguridad de oficinas, salas e instalaciones				
							Uso no aceptable de activos	3							11.1.5 Trabajo en áreas seguras				
															11.1.6 Áreas de entrega y carga				
															11.2.1 Ubicación y protección de equipos				
															11.2.3 Seguridad del cableado				
															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				
															11.1.4 Protección contra amenazas externas y ambientales				
															11.2.1 Ubicación y protección de equipos				
															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 comunicación en la cadena de suministro				
															7.2.1 Responsabilidades de la dirección				
															7.2.2 Concienciación, educación y capacitación de la seguridad de la información				
															11.1.3 Seguridad de oficinas, salas e instalaciones				
															15.2.2 Gestión de cambios en la provisión de servicios				
															7.1.2 Términos y condiciones del puesto de trabajo				
															11.1.4 Protección contra amenazas externas y ambientales				
															11.2.2 Servicios de suministro				
															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				

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles										
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD						
Equipos de Conectividad Críticos	Físico	1	1	4	Pérdida de disponibilidad del activo	Deterioro de los soportes	1	Mantenimiento insuficiente	2	0	0	24	0	0	16	Aceptar	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	Jefe Oficina TIC		
						Gestión de cambios ineficiente	2	12.1.2 Gestión del cambio													
						Falta de mantenimiento de equipos	1	Mantenimiento insuficiente	2								11.2.4 Mantenimiento de equipos				
								No existe gestión de activos	2								8.1.1 Inventario de activos				
								Planificación y monitorización de capacidad inadecuada	2								8.1.2 Propiedad de los activos				
						Fuego	2	No existen equipos de detección de incendios	3								8.1.3 Uso aceptable de los activos				
								No existen equipos de extinción de incendios	3								12.1.3 Gestión de la capacidad				
						Inundación	2	Ubicaciones susceptibles a 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								11.1.3 Seguridad de oficinas, salas e instalaciones				
																	No existe gestión de activos			2	11.1.4 Protección contra amenazas externas y ambientales
																	No existe procedimiento para el control de cambios			2	11.2.1 Ubicación y protección de equipos
																	No existen políticas para el uso de dispositivos portátiles			2	11.2.5 Retirada de activos
																	Uso no aceptable de activos			2	11.2.6 Seguridad de equipos y activos fuera de las instalaciones
						Polvo, humedad, corrosión	2	Exposición a humedad, polvo, suciedad	3								8.1.1 Inventario de activos				
																	8.1.2 Propiedad de los activos				
						Recuperación de medios reciclados o descartados	1	No existe gestión de activos	2								8.1.3 Uso aceptable de los activos				
																	No existe procedimiento para devolución de activos			2	8.1.4 Devolución de los activos
						Robo de equipamiento	1	Instalación desprotegida	3								12.1.2 Gestión del cambio				
																	No existe gestión de activos			2	6.2.1 Política de dispositivos móviles
No existen políticas para el uso de dispositivos portátiles	3	8.1.3 Uso aceptable de los activos																			
																11.1.4 Protección contra amenazas externas y ambientales					
																	11.1.4 Protección contra amenazas externas y ambientales				
																	11.2.1 Ubicación y protección de equipos				
																	11.2.4 Mantenimiento de equipos				
																	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				
																	12.1.2 Gestión del cambio				
																	6.2.1 Política de dispositivos móviles				
																	8.1.3 Uso aceptable de los activos				
																	11.1.4 Protección contra amenazas externas y ambientales				
																	11.2.1 Ubicación y protección de equipos				
																	11.2.4 Mantenimiento de equipos				
																	8.1.1 Inventario de activos				
																	8.1.2 Propiedad de los activos				
																	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				

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles									
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD					
Esquemas bases de datos de los sistemas de información Misional	Software	1	1	4	Pérdida de disponibilidad del activo	Fallo de sistemas	Fallos conocidos en inversiones	3	0	0	24	0	0	16	Aceptar	9.4.5 Control de acceso a código fuente de programa	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 TIC		
							Gestión de actualizaciones de seguridad ineficiente	3								12.6.1 Gestión de vulnerabilidades técnicas				
							No existen registros de auditoría	3								14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación				
							Pruebas de software insuficientes	3								14.2.4 Restricciones en cambios a paquetes de aplicaciones				
							Incumplimiento legal, reglamentario o contractual	2								Validación de la legislación aplicable			3	12.5.1 Instalación de programas en sistemas en producción
							Uso de sistemas por usuarios no autorizados	2								Acceso remoto no seguro			3	12.6.1 Gestión de vulnerabilidades técnicas
						Asignación errónea de derechos de acceso	2									12.6.2 Restricciones en la instalación de programas				
																14.2.2 Procedimiento de control de cambio en sistemas de información				
																14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación				
																			14.2.4 Restricciones en cambios a paquetes de aplicaciones	
				12.4.1 Registro de eventos																
				14.2.8 Pruebas de seguridad del sistema																
				14.2.9 Pruebas de aceptación del sistema																
				14.3.1 Protección de la información de prueba																
				10.1.1 Política en el uso de controles criptográficos																
				18.1.2 Derechos de propiedad intelectual																
				10.1.1 Política en el uso de controles criptográficos																
				10.1.2 Gestión de claves de criptografía																
				9.1.2 Acceso a redes y servicios de red																
				9.4.2 Proceso de inicio seguro de sesión																
				9.4.3 Sistema de gestión de contraseña																
				9.2.2 Provisión de acceso a usuarios																
				9.2.3 Gestión de derechos de acceso privilegiado																
				9.2.5 Revisión de los derechos de acceso de usuarios																
				9.2.6 Retirada o ajuste de los derechos de acceso																
				12.6.1 Gestión de vulnerabilidades técnicas																
				12.6.2 Restricciones en la instalación de programas																
				14.2.4 Restricciones en cambios a paquetes de aplicaciones																
				12.5.1 Instalación de programas en sistemas en producción																
				14.2.2 Procedimiento de control de cambio en sistemas de información																
				14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación																
				9.2.3 Gestión de derechos de acceso privilegiado																

Identificación del riesgo			Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles										
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
Sistemas Operativos de Servidores	Software	1	1	4	Pérdida de disponibilidad del activo	Fallo de sistemas	1	contraseñas	4	0	0	24	0	0	16	Aceptar	9.2.4 Gestión de información secreta de autenticación	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 TIC
								No existen registros de auditoría	3								12.4.1 Registro de eventos		
								Configuración de parámetros errónea	3								12.4.2 Protección de la información del registro de eventos		
								Especificaciones para desarrolladores incompletas o confusas	3								12.4.3 Registro de administrador y operador		
								Fallos conocidos en inversiones	3								12.4.4 Sincronización de reloj		
								Gestión de actualizaciones de seguridad ineficiente	3								14.1.1 Análisis y especificaciones de requisitos de seguridad de la información		
								No existen registros de auditoría	0								14.2.1 Política de desarrollo seguro		
								Pruebas de software insuficientes	0								14.2.5 Principios para la ingeniería de sistemas seguros		
								Incumplimiento legal, reglamentario o contractual	2								14.2.6 Entorno seguro de desarrollo		
								Uso de sistemas por usuarios no autorizados	1								14.2.7 Desarrollo externalizado		
								Asignación errónea de derechos de acceso	2								9.4.5 Control de acceso a código fuente de programa		
																	12.6.1 Gestión de vulnerabilidades técnicas		
		14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación																	
		14.2.4 Restricciones en cambios a paquetes de aplicaciones																	
		12.5.1 Instalación de programas en sistemas en producción																	
		12.6.1 Gestión de vulnerabilidades técnicas																	
		12.6.2 Restricciones en la instalación de programas																	
		14.2.2 Procedimiento de control de cambio en sistemas de información																	
		14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación																	
		14.2.4 Restricciones en cambios a paquetes de aplicaciones																	
		12.4.1 Registro de eventos																	
		14.2.8 Pruebas de seguridad del sistema																	
		14.2.9 Pruebas de aceptación del sistema																	
		14.3.1 Protección de la información de prueba																	
		10.1.1 Política en el uso de controles criptográficos																	
		18.1.2 Derechos de propiedad intelectual																	
		10.1.1 Política en el uso de controles criptográficos																	
		10.1.2 Gestión de claves de criptografía																	
		9.1.2 Acceso a redes y servicios de red																	
		9.4.2 Procesos de inicio seguro de sesión																	
		9.4.3 Sistema de gestión de contraseña																	
		9.2.2 Provisión de acceso a usuarios																	
		9.2.3 Gestión de derechos de acceso privilegiado																	
		9.2.5 Revisión de los derechos de acceso de usuarios																	

Identificación del riesgo					Análisis del riesgo inherente					Evaluación del nivel de riesgos y definición de controles																									
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD																				
															9.2.6 Retirada o ajuste de los derechos de acceso																				
Sistemas de información Misionales	Software	1	1	4	Pérdida de disponibilidad del activo	Elevación de privilegios	2	Fallos conocidos en inversiones	3	0	0	24	0	0	16	12.6.1 Gestión de vulnerabilidades técnicas	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 TIC																	
								Gestión de actualizaciones de seguridad ineficiente	2							12.6.2 Restricciones en la instalación de programas																			
								Gestión ineficiente de contraseñas	2							14.2.4 Restricciones en cambios a paquetes de aplicaciones																			
								No existen registros de auditoría	3							12.5.1 Instalación de programas en sistemas en producción																			
						Fallo de sistemas	1	Configuración de parámetros errónea	3							14.2.2 Procedimiento de control de cambio en sistemas de información																			
																Especificaciones para desarrolladores incompletas o confusas			3	14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación															
																Fallos conocidos en inversiones			3	9.2.3 Gestión de derechos de acceso privilegiado															
																Gestión de actualizaciones de seguridad ineficiente			3	9.2.4 Gestión de información secreta de autenticación	12.4.1 Registro de eventos														
																					No existen registros de auditoría	3	12.4.2 Protección de la información del registro de eventos												
																					Pruebas de software insuficientes	3	12.4.3 Registro de administrador y operador												
																					14.2.4 Sincronización de reloj		12.4.4 Registro de eventos												
																14.1.1 Análisis y especificaciones de requisitos de seguridad de la información				14.2.1 Política de desarrollo seguro		14.2.5 Principios para la ingeniería de sistemas seguros		14.2.6 Entorno seguro de desarrollo		14.2.7 Desarrollo externalizado		9.4.5 Control de acceso a código fuente de programa							
																12.6.1 Gestión de vulnerabilidades técnicas				14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación		14.2.4 Restricciones en cambios a paquetes de aplicaciones		12.5.1 Instalación de programas en sistemas en producción		12.6.1 Gestión de vulnerabilidades técnicas		12.6.2 Restricciones en la instalación de programas		14.2.2 Procedimiento de control de cambio en sistemas de información		14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación		14.2.4 Restricciones en cambios a paquetes de aplicaciones	
																12.4.1 Registro de eventos				14.2.8 Pruebas de seguridad del sistema		14.2.9 Pruebas de aceptación del sistema		14.3.1 Protección de la información de prueba											



Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
Equipos de almacenamiento	Físico	1	1	4	Pérdida de disponibilidad del activo		Uso incorrecto de equipos	3	0	0	24	0	0	16	Aceptar	7.2.2 Concienciación, educación y capacitación de la seguridad de la información	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 TIC	
						Deterioro de los soportes	1	Mantenimiento insuficiente								2			8.1.3 Uso aceptable de los activos
						Falta de mantenimiento de equipos	1	Gestión de cambios ineficiente								2			11.2.4 Mantenimiento de equipos
								Mantenimiento insuficiente								2			12.1.2 Gestión del cambio
								No existe gestión de activos								2			11.2.4 Mantenimiento de equipos
						Fuego	2	No existen equipos de detección de incendios								3			8.1.1 Inventario de activos
								No existen equipos de extinción de incendios								3			8.1.2 Propiedad de los activos
						Inundación	2	Ubicaciones susceptibles a inundación								3			8.1.3 Uso aceptable de los activos
																			12.1.3 Gestión de la capacidad
						Manipulación de los equipos	1	No existe control de los activos fuera de las instalaciones								3			11.1.3 Seguridad de oficinas, salas e instalaciones
								No existe gestión de activos								2			11.1.4 Protección contra amenazas externas y ambientales
								No existe procedimiento para el control de cambios								2			11.1.3 Seguridad de oficinas, salas e instalaciones
								No existen políticas para el uso de dispositivos portátiles								2			11.1.4 Protección contra amenazas externas y ambientales
								Uso no aceptable de activos								2			11.2.1 Ubicación y protección de equipos
						Polvo, humedad, corrosión	2	Exposición a humedad, polvo, suciedad								3			11.2.5 Retirada de activos
11.2.6 Seguridad de equipos y activos fuera de las instalaciones																			
Recuperación de medios reciclados o descartados	1	No existe gestión de activos	2	8.1.1 Inventario de activos															
				No existe procedimiento para devolución de activos	2	8.1.2 Propiedad de los activos													
Robo de equipamiento	1	Instalación desprotegida	3	8.1.3 Uso aceptable de los activos															
				No existe gestión de activos	2	8.1.4 Devolución de los activos													
						12.1.2 Gestión del cambio													
				6.2.1 Política de dispositivos móviles															
				8.1.3 Uso aceptable de los activos															
				11.1.4 Protección contra amenazas externas y ambientales															
				11.2.1 Ubicación y protección de equipos															
				11.2.4 Mantenimiento de equipos															
				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															
				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															
				11.2.1 Ubicación y protección de equipos															
				8.1.1 Inventario de activos															
				8.1.2 Propiedad de los activos															
				11.2.5 Retirada de activos															

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
							No existen políticas para el uso de dispositivos portátiles	3							11.2.6 Seguridad de equipos y activos fuera de las instalaciones				
							No existen procedimiento para devolución de activos	2							6.2.1 Política de dispositivos móviles				
															8.1.4 Devolución de los activos				
					Acceso a soportes no autorizado	2	Instalación desprotegida	3							11.1.3 Seguridad de oficinas, salas e instalaciones				
							Uso no aceptable de activos	3							11.1.5 Trabajo en áreas seguras				
															11.1.6 Áreas de entrega y carga				
															11.2.1 Ubicación y protección de equipos				
															11.2.3 Seguridad del cableado				
															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				
															11.1.4 Protección contra amenazas externas y ambientales				
															11.2.1 Ubicación y protección de equipos				
															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 comunicación en la cadena de suministro				
															7.2.1 Responsabilidades de la dirección				
															7.2.2 Concienciación, educación y capacitación de la seguridad de la información				
															11.1.3 Seguridad de oficinas, salas e instalaciones				
															15.2.2 Gestión de cambios en la provisión de servicios				
															7.1.2 Términos y condiciones del puesto de trabajo				
															11.1.4 Protección contra amenazas externas y ambientales				
															11.2.2 Servicios de suministro				
															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				
															12.1.2 Gestión del cambio				
															11.2.4 Mantenimiento de equipos				
															8.1.1 Inventario de activos				
															8.1.2 Propiedad de los activos				
															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 INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
							No existen procedimiento para devolución de activos	2							8.1.4 Devolución de los activos				
Equipos de Telefonía	Físico	1	1	2	Pérdida de disponibilidad del activo	2	Instalación desprotegida	3	0	0	12	0	0	8	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	Jefe Oficina TIC		
							Acceso a soportes no autorizado	2							Uso no aceptable de activos			3	11.1.5 Trabajo en áreas seguras
							Daños por agua	2							Susceptibilidad a polvo, humedad			3	11.1.6 Áreas de entrega y carga
							Daño por tercera parte	2							Gestión inadecuada de terceras partes			3	11.2.1 Ubicación y protección de equipos
															No existe concienciación y formación en seguridad			3	11.2.2 Seguridad del cableado
															No existe supervisión de terceros dentro de la organización			3	7.2.2 Concienciación, educación y capacitación de la seguridad de la información
															Proceso de contratación ineficiente			3	7.2.2 Concienciación, educación y capacitación de la seguridad de la información
							Destrucción	2							Exposición a temperaturas extremas			3	7.2.3 Proceso disciplinario
															No existe sistema estabilizador de tensión			3	8.1.3 Uso aceptable de los activos
															Uso incorrecto de equipos			3	11.1.4 Protección contra amenazas externas y ambientales
							Deterioro de los soportes	1							Mantenimiento insuficiente			2	11.2.1 Ubicación y protección de equipos
							Falta de mantenimiento de equipos	1							Gestión de cambios ineficiente			2	15.1.1 Política de seguridad en la relación con proveedores
															Mantenimiento insuficiente			2	15.1.2 Seguridad en el acuerdo con proveedores
															No existe gestión de activos			2	15.1.3 Tecnología de la información y comunicación en la cadena de suministro
Planificación y monitorización de capacidad inadecuada	2	7.2.1 Responsabilidades de la dirección																	

Identificación del riesgo					Análisis del riesgo inherente						Evaluación del nivel de riesgos y definición de controles								
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
					Fuego	2	No existen equipos de detección de incendios	3							11.1.3 Seguridad de oficinas, salas e instalaciones	realiza directamente en la plataforma dispuesta para tal fin			
							No existen equipos de extinción de incendios	3							11.1.4 Protección contra amenazas externas y ambientales				
					Inundación	2	Ubicaciones susceptibles a inundación	3							11.1.3 Seguridad de oficinas, salas e instalaciones				
					Manipulación de los equipos	1	No existe control de los activos fuera de las instalaciones	3							11.1.4 Protección contra amenazas externas y ambientales				
							No existe gestión de activos	2								11.2.1 Ubicación y protección de equipos			
							No existe procedimiento para el control de cambios	2								11.2.5 Retirada de activos			
							No existen políticas para el uso de dispositivos portátiles	2								11.2.6 Seguridad de equipos y activos fuera de las instalaciones			
							Uso no aceptable de activos	2								8.1.1 Inventario de activos			
					Polvo, humedad, corrosión	2	Exposición a humedad, polvo, suciedad	3							8.1.2 Propiedad de los activos				
					Recuperación de medios reciclados o descartados	1	No existe gestión de activos	2							8.1.3 Uso aceptable de los activos				
							No existe procedimiento para devolución de activos	2								8.1.4 Devolución de los activos			
					Robo de equipamiento	1	Instalación desprotegida	3							12.1.2 Gestión del cambio				
							No existe gestión de activos	2								6.2.1 Política de dispositivos móviles			
							No existen políticas para el uso de dispositivos portátiles	3								8.1.3 Uso aceptable de los activos			
							No existen procedimiento para devolución de activos	2								11.1.4 Protección contra amenazas externas y ambientales			
							Fallos conocidos en inversiones	3							11.2.1 Ubicación y protección de equipos				
															11.2.4 Mantenimiento de equipos				
															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				
															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				
															11.2.1 Ubicación y protección de equipos				
															8.1.1 Inventario de activos				
															8.1.2 Propiedad de los activos				
															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				
															8.1.4 Devolución de los activos				
															12.6.1 Gestión de vulnerabilidades técnicas				
															12.6.2 Restricciones en la instalación de programas				
															14.2.4 Restricciones en cambios a paquetes de aplicaciones				
															12.5.1 Instalación de programas en sistemas en producción				

Identificación del riesgo					Análisis del riesgo inherente							Evaluación del nivel de riesgos y definición de controles							
ACTIVOS DE INFORMACIÓN	TIPO DE ACTIVO	EVALUACIÓN 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	DISPONIBILIDAD						CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD				
					Uso de sistemas por usuarios no autorizados	1	Asignación errónea de derechos de acceso	2							9.2.2 Provisión de acceso a usuarios				
															9.2.3 Gestión de derechos de acceso privilegiado				
															9.2.5 Revisión de los derechos de acceso de usuarios				
															9.2.6 Retirada o ajuste de los derechos de acceso				

	REVISÓ	APROBÓ
Firma		
Nombre	John Edilson Patiño Tenorio	Alfonso Javier Celedón Simón
Cargo	Coordinador Grupo de Gestión de Gobernabilidad de la Información y Gestión del Conocimiento	Jefe Oficina de Tecnologías de la Información y las Comunicaciones.
Fecha	11 de julio de 2021	11 de julio de 2021