MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024

Proceso	Referencia	Activo de Información	Tipo de activo	Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raiz)	Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de Riesgo inherente	No Control	Control Anexo A	Descripción del control	Afectación		Atributos								Probabilidad residual	Impacto residual	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento
																		Probabilidad	Impacto	Tipo	%	Implementación	%	Calificación del Control	Documentación	Frecuencia	Evidencia								
Identificación, ordenamiento y administración de los recursos natulares	1	Liquidaciones de trámites ambientales	Inforlmación o datos	Hurto de medios o documentos	Exposición de datos confidencialeSs	Perdida de confidencialidad	Perdida de confidencialidad por el hurto de documentos relacionados con la liquidación de trámites ambientales, que son almacenados en sitios de facil acceso al público en general.	Fraude interno / Externo	1920 (Horas/ año)	Baja	40%	Leve	20%	Bajo	1	A.9.4.1 Restricción de acceso Información	El responsable de la información establece procedimientos para el acceso a la misma, teneindo en cuenta los roles y responsabilidades de usuariols internos y externos	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	24%	20%	Baja	24%	Leve	20%	Bajo	Reducir
Identificación, ordenamiento y administración de los recursos natulares	2	Informes técnicos de visitas	Inforlmación o datos	Alteración de la información	Exposición de datos confidenciales	Perdida de integridad	Perdida de integridad por alteración de la información de informes técnicos generados a partir de las visitas realizadas a campo para obtener o corroborar, de primera mano los datos suministrados por los usuarios para acceder a trámites ambientales o para atender denuncias ambientales.	Fraude interno / Externo	1920 (Horas/ año)	Media	60%	Mayor	80%	Alto	1	A.9.4.1 Restricción de acceso Información	El responsable de la información establece procedimientos para el acceso a la misma, teneindo en cuenta los roles y responsabilidades de usuariols internos y externos	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	36%	80%	Baja	36%	Mayor	80%	Alto	Reducir
															2	A.11.1.3 Seguridad de oficinas, recintos e instalaciones	La alta gerencia debería diseñar y aplicar mecanismos para garantizar la seguridad física a oficinas, recintos e instalaciones.	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	22%	80%							
Identificación, ordenamiento y administración de los recursos natulares	3	Subsistemas del Sistema de Información Ambiental de Colombia - SIAC	Aplicación	Hurto de información	Exposición de datos confidenciales	Perdida de integridad	Perdida de integridad por hurto de información de credenciales de acceso a los subsistemas del SIAC), permitiendo que se cargue a dichos subsistemas información errónea o no aujtorizada por la entidad.	Fraude Externo	8760 (Horas/ año)	Baja	40%	Moderado	60%	Moderado	1	A.9.4 Control de acceso a sistemas y aplicaciones	El responsable de la seguridad de la información establece autenticaciones de doble factor que permitan comprobar la identidad del usuario que intenta acceder a las aplicaciones.	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro	20%	60%	Muy Baja	20%	Moderado	60%	Moderado	Reducir
Identificación, ordenamiento y administración de los recursos natulares	4	Equipo de cómputo para almacenar y gestionar Base de datos de estadísticas forestales	Hardware	Falla de equipo	Fallas eléctricas	Perdida de disponibilidad	Perdida de disponibilidad por falla del equipo donde se almacena información de estadística forestal.	Fallas tecnológicas	8760 (Horas/ año)	Media	60%	Moderado	60%	Moderado	1	A.11.2.2 Servicios de suministro	El responsable del mantenimiento en la entidad dispondrá la adquisición e instalación de UPS´s a los eauipos para protegerlos contra fallas eléctricas.	X		Preventivo	25%	Automático	25%	50%	NA	Continua	NA	30%	60%	Baja	30%	Moderado	60%	Moderado	Evitar
Gestión Tecnológica	5	Servicio de internet	Servicio	vandalismo	Ausencia de canal alterno	Perdida de disponibilidad	Perdida de disponibilidad por vandalismo del servicio de internet.	Fraude Externo	8760 (Horas/ año)	Baja	40%	Catastrófico	100%	Extremo	1	A.13.1.2 Seguridad de los servicios de red	Gestionar un canal de internet alterno, que permita mantener el servicio activo en caso el canal principal falle	X		Correctivo	10%	Automático	25%	35%	Documentado	Continua	Con registro	26%	100%	Baja	26%	Catastrófico	100%	Extremo	Evitar
Gestión Tecnológica	6	Servicio de internet	Servicio	Falla técnica	Ausencia de canal alterno	Perdida de disponibilidad	Perdida de disponibilidad por falla técnica del servicio de internet.	Fallas tecnológicas	8760 (Horas/ año)	Media	60%	Catastrófico	100%	Extremo	1	A.13.1.2 Seguridad de los servicios de red	Gestionar un canal de internet alterno, que permita mantener el servicio activo en caso el canal principal falle	X		Correctivo	10%	Automático	25%	35%	Documentado	Continua	Con registro	39%	100%	Baja	39%	Catastrófico	100%	Extremo	Evitar
	7	Página web	Aplicación	Espionaje remoto	Entidades Externas XML (XXE)	Perdidad de Disponibilidad	Perdida de disponibilidad por espionaje remoto a la página web de le entidad.	Fraude Externo	8760 (Horas/ año)	Baja	40%	Catastrófico	100%	Extremo	1	A.18.2 Revisiones de seguridad de la información	Se realiza la configuración de analizadores XML para que no acepten definiciones de documentos personalizados (DTD).	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro	20%	100%	Muy Baja	20%	Catastrófico	100%	Extremo	Evitar
Gestión Tecnológica	8	Servidor de aplicaciones	Hardware	Falla de equipo	Mantenimiento insuficiente	Perdidad de disponibilidad	Posibilidad de pérdida de la disponibilidad del servidor de aplicaciones, por fallas en el mismo, ocasionadas por mantenimientos preventivos insuficientes.	Fallas tecnológicas	365 días al año	Muy Baja	20%	Menor	40%	Bajo	1	A.11.2.4 Mantenimiento de equipos	Se realiza tareas de verificación manuales, realizando pruebas de: continuidad, Vulnerabilidades y Carga	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	12%	40%	Muy Baja	12%	Menor	40%	Bajo	Evitar
															2	A.12.3.1 Respaldo de información	Se realiza la generación de un backup diario tipo Snapchat, con el estado actual de la maquina.	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro	6%	40%	Muy Baja						
Gestión Tecnológica	9	Servidor de datos	Hardware	Falla de equipo	Mantenimiento insuficiente	Perdidad de disponibilidad	Posibilidad de pérdida de la disponibilidad del servidor de datos, por fallas en el mismo ocasionadas por mantenimientos preventivos insuficientes.	Fallas tecnológicas	365 días al año	Muy Baja	20%	Moderado	60%	Moderado	1	A.11.2.4 Mantenimiento de equipos	Se realiza tareas de verificación manuales, realizando pruebas de: continuidad, Vulnerabilidades y Carga	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	12%	60%	Muy Baja	12%	Moderado	60%	Moderado	Evitar
															2	A.12.3.1 Respaldo de información	Se realiza la generación de un backup diario tipo Snapchat, con el estado actual de la maquina.	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro	6%	60%	Muy Baja						
Gestión Tecnológica	10	Servidor de PCT	Hardware	Falla de equipo	Mantenimiento insuficiente	Perdidad de disponibilidad	Posibilidad de pérdida de la disponibilidad del servidor de PCT, por fallas en el mismo ocasionadas por mantenimientos preventivos insuficientes.	Fallas tecnológicas	365 días al año	Muy Baja	20%	Catastrófico	100%	Extremo	1	A.11.2.4 Mantenimiento de equipos	Se realiza tareas de verificación manuales, realizando pruebas de: continuidad, Vulnerabilidades y Carga	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	12%	100%	Muy Baja	12%	Catastrófico	100%	Extremo	Evitar
															2	A.12.3.1 Respaldo de información	Se realiza la generación de un backup diario tipo Snapchat, con el estado actual de la maquina.	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro	6%	100%	Muy Baja						
Gestión Tecnológica	11	Servidor de PCT	Hardware	Virus informático	Software desactualizado	Perdidad de disponibilidad	Posibilidad de pérdida de la disponibilidad del servidor de PCT, por virus informático y desactualización del software	Fallas tecnológicas	365 días al año	Baja	40%	Mayor	80%	Alto	1	A.12.2 Protección contra códigos maliciosos	La oficina de TI realiza las gestiones para la adquisición de antivirus para los equipos y servidores	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	24%	80%	Baja	24%	Mayor	80%	Alto	Evitar
															2	A.12.3.1 Respaldo de información	El profesional responsable de la administración del servidolr realiza copias de respaldo diarias	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	14%	80%	Muy Baja						
Gestión Tecnológica	12	Servidor de Datos	Hardware	Virus informático	Software desactualizado	Perdidad de disponibilidad	Posibilidad de pérdida de la disponibilidad del servidor de datgos, por virus informático y desactualización del software	Fallas tecnológicas	365 días al año	Baja	40%	Mayor	80%	Alto	3	A.12.2 Protección contra códigos maliciosos	La oficina de TI realiza las gestiones para la adquisición de antivirus para los equipos y servidores	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	24%	80%	Baja	24%	Mayor	80%	Alto	Evitar
															4	A.12.3.1 Respaldo de información	El profesional responsable de la administración del servidolr realiza copias de respaldo diarias	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	14%	80%	Muy Baja						
Gestión Tecnológica	13	Switches y Router	Hardware	Falla de equipo	Sistema eléctrico deficiente	Perdidad de disponibilidad	Posibilidad de pérdida de la disponibilidad del servicio soportado por switches y routers (internet y datos), por falla de los mismos y ausencia de un sistema eléctrico robusto (corriente regulada y soportada por planta eléctrica de respaldo y UPSs)	Fallas tecnológicas	366 días al año	Baja	40%	Mayor	80%	Alto	5	A.12.2 Protección contra códigos maliciosos	La oficina de TI realiza las gestiones para la adquisición de antivirus para los equipos y servidores	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	24%	80%	Baja	24%	Mayor	80%	Alto	Evitar
															6	A.12.3.1 Respaldo de información	El profesional responsable de la administración del servidolr realiza copias de respaldo diarias	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	14%	80%	Muy Baja						