El futuro digital es de todos | MinTIC

MATRIZ DE RIESGOS DIGITALES - CODECHOCO

Proceso	Referencia	Activo de Información	Descripción del Riesgo	Clasificación riesgo	Control Anexo A	Descripción del control	Afectación		Atributos						Probabilidad residual	Impacto residual	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento	Plan de Acción	Responsable	Fecha de Implementación	Primer Seguimiento		Segundo Seguimiento		Tercer Seguimiento / a 31 de dic de 2023	
							Probabilidad	Impacto	Tipo	%	Implementación	%	Calificación del Control	Documentación	Frecuencia	Evidencia										Seguimiento	Estado	Seguimiento	Estado	Seguimiento	Estado
Gestión Tecnológica	1	Servicio de internet	Perdida de disponibilidad por vandalismo del servicio de internet.	Fraude Externo	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	Reducir	1. Realizar estudios previos para contratar canal alterno, de acuerdo a la oferta del mercado 2. Realizar contratación 3. Administración del canal	Oficina TIC Oficina Contratación Dirección	mar-23	Actividad sin iniciar	Sin Iniciar	Estudio de posibles proveedores del servicio a la espera de viabilidad por parte de la dirección general para iniciar trámite	En ejecución	Se logró Contratar el servicio de internet satelital con la empresa Innovtics, quien le ofrece a la entidad un canal con un ancho que oscila entre 10 y 100 Mb.	Finalizada
Gestión Tecnológica	2	Servicio de internet.	Perdida de disponibilidad por falla técnica del servicio de internet.	Fallas tecnológicas	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									
Gestión Tecnológica	3	Página web	Perdida de disponibilidad por espionaje remoto a la página web de le entidad.	Fraude Externo	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	Realizar la configuración de analizadores XML para que no acepten definiciones de documentos personalizados (DTD)	Oficina TIC Contratista página web	abr-22	La actividad está siendo implementada por NEXURA contratista encargado del diseño del sitio web	En ejecución	La actividad sigue siendo implementada por NEXURA contratista encargado del diseño del sitio web	En ejecución	La actividad sigue siendo implementada por NEXURA contratista encargado del diseño del sitio web	En ejecución
					A.12.3.1 Respaldo de información	Se realiza un backup quinceral del sitio web (bases de datos, documentos, configuración).		X	Correctivo	10%	Manual	15%	25%	Documentado	Continua	Con registro	15%	100%	Muy Baja	15%	Catastrófico	100%	Extremo	Reducir	Realizar copias de seguridad cada 15 días, de las bases de datos, documentos y configuración del sitio	Oficina TIC	dic-23	El sitio aún está en manos del contratista, por lo que él se encarga de las copias de seguridad	En ejecución	El sitio aún está en manos del contratista, por lo que él se encarga de las copias de seguridad	En ejecución	El sitio aún está en manos del contratista, por lo que él se encarga de las copias de seguridad	En ejecución
Gestión Tecnológica	4	Servidor de aplicaciones	Posibilidad de pérdida de la disponibilidad del servidor de aplicaciones, por fallas en el mismo, ocasionadas por mantenimientos preventivos insuficientes.	Fallas tecnológicas	A.11.2.4 Mantenimiento de equipos	La Oficina TIC se encargará de mantener correctamente los equipos, para asegurar su disponibilidad e integridad continuas.	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	12%	40%	Muy Baja	12%	Menor	40%	Bajo	Evitar	1. Realizar plan de mantenimiento 2. Socializar el cronograma de mantenimiento 3. Ejecutar el cronograma de mantenimiento	Oficina TIC	31-dic-23	Se realizó el inventario de equipos Se realizó el plan de mantenimiento Se está ejecutando el cronograma por areas	En ejecución	Los mantenimientos se esta ejecutando de acuerdo al inventario de equipos existentes en la entidad y el plan establecido para ello.	En ejecución	Se realizaron los mantenimientos programados, luego de la socialización del respectivo cronograma.	Finalizada
					A.12.3.1 Respaldo de información	Se realiza la generación de un backup diario tipo Snap, con el estado actual de la maquina.		X	Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro	6%	40%	Muy Baja					Reducir	Realizar copias de seguridad semestral (sistema opeativo, archivos)	Oficina TIC	31-dic-23	Se tiene una copia del primer semestre del año	Pendiente	A la fecha las copias de seguridad van en %	En ejecución	Se realiza copia permanente de la información institucional de cada funcionario, adicional a lo anterior se realizan copias de los sistemas misionales(PCT, página web)	Finalizada
Gestión Tecnológica	5	Servidor de datos	Posibilidad de pérdida de la disponibilidad del servidor de datos, por fallas en el mismo ocasionadas por mantenimientos preventivos insuficientes.	Fallas tecnológicas	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	1. Realizar plan de mantenimiento 2. Socializar el cronograma de mantenimiento 3. Ejecutar el cronograma de mantenimiento	Oficina TIC	31-dic-23	Se realizó el inventario de equipos Se realizó el plan de mantenimiento Se está ejecutando el cronograma por areas	En ejecución		En ejecución	Se realizaron los mantenimientos programados, luego de la socialización del respectivo cronograma.	Finalizada
					A.12.3.1 Respaldo de información	Se realiza la generación de un backup diario tipo Snap, con el estado actual de la maquina.	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro	6%	60%	Muy Baja					Reducir	1. Diseñar el procedimiento para la realización de copias de seguridad de archivos importantes de cada usuario 2. Instruir a los usuarios para la realización las copias de los archivos mas importantes. 3. Realizar seguimiento a los usuarios para verificar la realizacón de la tarea.	Oficina TIC Funcionarios Éntidad	31-dic-23	Se diseñó el procedimiento de realizacion de copias de seguridad , además, se instruyó a cada usuario la forma de realizarlo.		Verificaciones periodicas de las copias de seguridad realizadas por los usuarios de acuerdo a las directrices establecidas por la oficina TIC.			Finalizada
Gestión Tecnológica	6	Servidor de PCT	Posibilidad de pérdida de la disponibilidad del servidor de PCT, por fallas en el mismo ocasionadas por mantenimientos preventivos insuficientes.	Fallas tecnológicas	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	1. Realizar plan de mantenimiento 2. Socializar el cronograma de mantenimiento 3. Ejecutar el cronograma de mantenimiento	Oficina TIC	31-dic-23	Se realizó el inventario de equipos Se realizó el plan de mantenimiento Se está ejecutando el cronograma por areas	En ejecución	Los mantenimientos se esta ejecutando de acuerdo al inventario de equipos existentes en la entidad y el plan establecido para ello. De igual forma las copias de seguridad diarias estan siendo guardadas en un dispositivo externo.	En ejecución	Los mantenimientos se estan ejecutando de acuerdo al inventario de equipos existentes en la entidad y el plan establecido para ello. De igual forma las copias de seguridad diarias estan siendo guardadas en un dispositivo externo.	Finalizada
					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						Realizar copias de seguridad diarias, de la base de datos del software financiero	Oficina TIC	31-dic-23	A la fecha se ha realizado 95 copias		A la fecha se ha realizado 227 copias		Se realiza copias diarias del sistema PCT, las cuales están almacenadas en el servidor respectivo y en dispositivos de almacenamiento externo.	
Gestión Tecnológica	7	Servidor de PCT	Posibilidad de pérdida de la disponibilidad del servidor de PCT, por virus informático y desactualización del software	Fallas tecnológicas	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	1. Realizar plan de mantenimiento 2. Socializar el cronograma de mantenimiento 3. Ejecutar el cronograma de mantenimiento 4.Realiza las gestiones para la adquisición de antivirus para los equipos y servidores	Oficina TIC	31-dic-23	Se realizó el inventario de equipos Se realizó el plan de mantenimiento Se está ejecutando el cronograma por areas	En ejecución	Se tiene estudio de las caracteristicas técnicas del antivirus requerido para la entidad y el invetario de equipos que requieren dicha protección	En ejecución		En ejecución
					A.12.3.1 Respaldo de información	El profesional responsable de la administración del servidoir realiza copias de respaldo diarias	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	14%	80%	Muy Baja						1. Revisar la actualizaciones vigentes del sistema operativo y aplicaciones. 2. Realizar copias de seguridad diarias, de la base de datos del software financiero	Oficina TIC	31-dic-23	A la fecha se ha realizado 95 copias		A la fecha se ha realizado 227 copias		A la fecha se ha realizado 240 copias	
Gestión Tecnológica	8	Servidor de Datos	Posibilidad de pérdida de la disponibilidad del servidor de datgos, por virus informático y desactualización del software	Fallas tecnológicas	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	1. Realizar plan de mantenimiento 2. Socializar el cronograma de mantenimiento 3. Ejecutar el cronograma de mantenimiento 4.Realiza las gestiones para la adquisición de antivirus para los equipos y servidores	Oficina TIC	31-dic-23	Se realizó el inventario de equipos Se realizó el plan de mantenimiento Se está ejecutando el cronograma por areas	En ejecución	Se tiene estudio de las caracteristicas técnicas del antivirus requerido para la entidad y el invetario de equipos que requieren dicha protección	En ejecución		
					A.12.3.1 Respaldo de información	El profesional responsable de la administración del servidoir realiza copias de respaldo diarias	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	14%	80%	Muy Baja						1. Revisar la actualizaciones vigentes del sistema operativo y aplicaciones. 2. Realizar copias de seguridad diarias, de la base de datos del software financiero	Oficina TIC	31-dic-23	A la fecha se ha realizado 5 copias de la información contenida en los equipos incluidos en el dominio		A la fecha se ha realizado XXX copias de la información contenida en los equipos incluidos en el dominio		A la fecha se ha realizado XXX copias de la información contenida en los equipos incluidos en el dominio	
Gestión Tecnológica	9	Switches y Router	Posibilidad de pérdida de la disponibilidad del servicio soportado por switches y routers (internet y datos), por falla de los mismos	Fallas tecnológicas	A.11.2 Equipos	La Oficina TIC se encargará de Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro	24%	80%	Baja	24%	Mayor	80%	Alto	Aceptar	1. Solicitar a la alta gerencia la realización de mantenimiento periódico del sistema eléctrico (red eléctrica, UPSs y planta eléctrica).	Dirección	31-dic-23	1. La entidad adquirió una planta eléctrica que soporta varias dependencias, entre ellas la oficina TIC. 2. Se solicitó a la Dirección contratar la revisión del sistema eléctrico de la dependencia.	En ejecución	Se realizó el estudio, compra, instalación y puesta en funcionamiento de la planta electrica de la oficina TIC	En ejecución	Se realizó el estudio, compra, instalación y puesta en funcionamiento de la planta electrica de la oficina TIC. Se instaló una plata electrica a nivel de toda la entidad, y adicioonal a ello se instalaron dos UPS de 5 KVA para soportar los equipos de la oficina de TI	En ejecución