ON DE TECNOLOGIAS E IN

DE SEGURIDAD DE LA INF

Tipo de riesgo	Descripción del Riesgo	Plan de Acción	Responsable	PERIODICIDAD	Seguimiento	Estado
Perdida de disponibilidad	La ausencia de mecanismos alternos de respaldo podría desencadenar en perdida de información reservada y/o confidencial por un ataque informatico sobre las bases de datos y los sistemas de información críticos.	Realizar (1) una copia mensual de las bases de datos, sistemas de información e información institucional de los usuarios de las diferentes dependencias.	Profesional Sistemas	Mensual Indicador de Backups (Trimestral)	En cuanto al proceso La ausencia de mecanismos alternos de respaldo podría desencadenar en perdida de informacion reservada y/o confidencial por un ataque informatico sobre las bases de datos y los sistemas de informacion, como medida de control La CPSM realiza copias de seguridad de manera mensual, cubriendo los sistemas de información institucionales, la página web oficial y los aplicativos misionales, estratégicos y de soporte. Este procedimiento se ejecuta bajo lineamientos previamente definidos y siguiendo las mejores prácticas en gestión de la continuidad del servicio, garantizando así la integridad, disponibilidad y recuperación . Se concluye que la probabilidad de Riesgo es BAJA teniendo en cuenta que esta actividad se ejecuta 12 veces al año.	**EVALUACION DE RIESGO BAJA**
Perdida de Integridad	La ausencia de actualizaciones de seguridad en las aplicaciones podría poner en riesgo la integridad y disponibilidad de los sistemas, permitiendo la ejecución de código malicioso.	Realizar (2) dos Informes analisis de vulnerabilidad en el año de manera semestral sobre los sistemas de información criticos con el fin de identificar posibles vulnerabilidades que puedan afectar la seguridad de los aplicativos.	Profesional Sistemas	28 de Junio y 10 diciembre de 2025	28 de Junio y 10 diciembre de 2025	**SE EVALUARA EN LA FECHAS INDICADAS**
		Ejecutar de manera oportuna y permanente las actualizaciones y controles necesarios para remediar las vulnerabilidades destectadas durante las pruebas de seguridad.	Profesional Sistemas	05 de Julio y 17 Diciembre de 2025	05 de Julio y 17 Diciembre de 2025	**SE EVALUARA EN LA FECHAS INDICADAS**
Perdida de Disponibilidad	La falta de mantenimiento tanto en los elementos físicos como lógicos de la infraestructura tecnológica podría ocasionar pérdida de disponibilidad de los sistemas críticos que respaldan los diversos servicios y procesos de la entidad.	Definir y realizar como mínimo (1) un mantenimiento preventivo durante el año donde se incluyan tanto los elementos lógicos y físicos que componen la infraestructura tecnológica. Estos mantenimientos deben ser programados y contar con un cronograma de actividades, responsables, seguimiento y monitoreo a su vez teniendo en cuenta los riesgos que se pueden presentar en la ejecución del mantenimiento.Formato para el Registro de Mantenimientos.	Profesional Sistemas	Anual	**ANUAL**	**ANUAL**
Perdida de Disponibilidad	La falta de claridad en la definición y ejecución de un plan de recuperación ante desastres tecnológicos podría dar lugar a la indisponibilidad en la prestación de servicios de la entidad debido a daños o interrupciones en los sistemas e infraestructura tecnológica.	Definir y ejecutar el plan de recuperación ante desastres tecnológicos cuando se requiera, a su vez realizar (2) dos veces en el año, pruebas a las actividades establecidas en en dicho plan. Estas pruebas deben generar unos resultados y lecciones aprendidas los cuales serviran de soporte para generar posibles planes de mejoramiento sobre las actividades que no generaron un resultado satisfactorio.	Profesional Sistemas	24 de marzo y 22 octubre de 2025	Frente a la falta de claridad en la definición y ejecución de un plan de recuperación ante desastres tecnológicos que podría dar lugar a la indisponibilidad en la prestación de servicios de la entidad debido a daños o interrupciones en los sistemas e infraestructura tecnológica Como medida de control la CPSM por parte del Profesional de Sistemas realizó La prueba al Plan de Recuperación ante Desastres Tecnológicos la cual se llevó a cabo satisfactoriamente, evidenciando que los sistemas críticos fueron restaurados conforme a los tiempos y procedimientos establecidos, Segun consta en el informe presentado a la Direccion General el dia 24 de marzo de 2025. Se concluye que la probabilidad de Riesgo es MUY BAJA teniendo en cuenta que esta actividad se ejecuta como minimo 2 veces al año.	**EVALUACION DE RIESGO MUY BAJA**
Perdida de la Confidencialidad	La ausencia de capacitación, sensibilización y entrenamiento en seguridad y ciberseguridad para todas las partes interesadas podría comprometer la confidencialidad de la información en diversos sistemas y activos por medio de un ataque de ingeniería social.	Llevar a cabo las acciones y actividades definidas en la estrategia de capacitación, sensibilización y entrenamiento, estableciendo un cronograma con fechas y temas específicos a tratar. Estas actividades deben abarcar campañas de sensibilización, entrenamiento en técnicas de ingeniería social como el phishing, ejercicios de simulación de ataques de suplantación de identidad, así como evaluaciones que permitan medir la eficacia de las estrategias implementadas. Estas acciones deben llevarse a cabo al menos (3) cuatro veces durante el año.	Profesionale Sistemas	23 de abril, agosto 13, octubre 15 de 2025	Frente a La ausencia de capacitación, sensibilización y entrenamiento en seguridad y ciberseguridad para todas las partes interesadas podría comprometer la confidencialidad de la información en diversos sistemas y activos por medio de un ataque de ingeniería social. para el periodo evaluado (enero abr) de 2025, el profesional de sistemas realizará la primera capacitación sobre ciberseguridad en el mes de mayo, ya que en el mes de abril el Profesional en Sistemas se encontraba en vacaciones. Se concluye que la probabilidad de Riesgo es BAJA teniendo en cuenta que esta actividad se ejecuta como mínimo 3 veces en el año.	**EVALUACION DE RIESGO BAJA**
Perdida de la Integridad	La falta de un monitoreo y seguimiento efectivos de los incidentes de seguridad y ciberseguridad podría propiciar la vulneración de los controles de seguridad, comprometiendo así la integridad de los diversos activos de información de la Entidad.	Llevar a cabo registros cuando se requiera ante la ocurrencia de un evento o incidente de seguridad y Ciberseguridad que represente una amenaza para la seguridad de la información. Dichos registros deben ser detallados en la bitácora de incidentes de seguridad de la información y ciberseguridad establecida por la entidad.	Profesional Sistemas	Cuando se requiera	Frente a la falta de un monitoreo y seguimiento efectivos de los incidentes de seguridad y ciberseguridad que podría propiciar la vulneración de los controles de seguridad, comprometiendo así la integridad de los diversos activos de información de la Entidad.Durante la vigencia evaluada, no se presentaron incidentes de seguridad digital ni ciberseguridad que representan una amenaza directa a la confidencialidad, integridad o disponibilidad de la información institucional. Por tanto, no fue necesario realizar registros en la bitácora de incidentes de seguridad de la información y ciberseguridad, la cual se encuentra establecida y disponible para uso inmediato ante cualquier eventualidad conforme al procedimiento documentado por la entidad. Se concluye que la Evaluacion de Riesgo es muy BAJA, teniendo en cuenta que la actividad se ejecutara cuando se requiera	**EVALUACION DE RIESGO MUY BAJA**
Perdida de la Integridad	La ausencia de mecanismos de monitoreo para supervisar la gestión efectuada por el encargado de administrar las plataformas podría dar lugar a actividades inapropiadas que atenten contra la seguridad y privacidad de la información en los sistemas y aplicaciones.	Llevar a cabo control de publicaciones en página web o modificaciones de aplicativos de las diferentes plataformas tecnológicas y sistemas de información, presentando posteriormente un informe detallado de los hallazgos y situaciones identificadas que pudieran representar un riesgo para la seguridad y privacidad de los sistemas y plataformas. F-Formato Control de Publicaciones en Página Web	Profesional Sistemas	Cuando se requiera	En cuanto a la ausencia de mecanismos de monitoreo para supervisar la gestión efectuada por el encargado de administrar las plataformas podría dar lugar a actividades inapropiadas que atenten contra la seguridad y privacidad de la información en los sistemas y aplicaciones, para el periodo evaluado, la entidad realiza un proceso de control riguroso sobre las publicaciones y modificaciones efectuadas en la página web institucional, así como en los aplicativos y plataformas tecnológicas que conforman los sistemas de información. Este procedimiento tiene como objetivo mitigar riesgos asociados a la seguridad y privacidad de la información publicada o modificada. Para tal fin, se utiliza el Formato de Control de Publicaciones en Página Web, el cual permite registrar y hacer seguimiento a cada solicitud. Las solicitudes son canalizadas exclusivamente a través del correo oficial del área de sistemas, lo que garantiza trazabilidad y validación previa antes de su implementación. Se concluye que la Evaluacion de Riesgo es muy BAJA, teniendo en cuenta que la actividad se ejecutara periodicamente.	**EVALUACION DE RIESGO BAJA**