	FORMATO		
Corporación para el Fomento Educación Superior	PLAN DE MEJORAMIENTO	Código	
		Versión	
		Vigencia	
		Copia Controlada	SI ____ NO___

NOMBRE REPRESENTANTE LEGAL:	Claudia Elene Mejia Acosta
PERIODO AUDITADO:	2017
FECHA DE REALIZACION DE LA AUDITORIA:	A partir del 20 de diciembre de 2017
NOMBRE DEL INFORME:	Auditoría de Sistemas
TIPO DE AUDITORIA:	Auditoría de Sistemas
FECHA DE SUSCRIPCIÓN:	

Aspecto Evaluado	*N° Hallazgo*	*Descripción Hallazgo (Observación)*	*Recomendaciones*	*Disposiciones de la Corporación*	*Causa*	*Acción de Mejora*	*Proceso responsable*	*Responsable(s) de recolectar las evidencias del tratamiento*	*Cronograma de Ejecución*	*Fecha de Iniciación*	*Fecha Finalizacion*	*Evidencias*	*Observaciones*
Plan de Recuperación de Desastres	1	Implementación y aplicación de un DRP Durante nuestra revisión, encontramos un plan de contingencias para respaldar la infraestructura de TI a nivel de servidores, sin embargo, no se tiene lo siguiente: 1. Actividades a realizar por servicio de TI 2. Periodicidad y cronograma de pruebas del plan de contingencias 3. Responsables por actividad y escalamiento de aprobaciones 4. Identificación de riesgos, servicios e infraestructura critica	Ampliar y mejorar el plan de contingencias que se tiene documentado actualmente, de acuerdo con los puntos nombrados, más lo que se recomienda en marcos como ISO27001 y COBIT 5. Cabe resaltar que las pruebas al DRP se deben realizar por lo menos dos veces al año (semestral), con el fin de asegurar su operatividad y continuidad en los sistemas de información e infraestructura.	Actividades a realizar por servicio de TI: • Las actividades a realizar están direccionadas por el sistema de mesa de ayuda, adicional en los subprocesos del área se menciona que perfil atiende los subprocesos 2. Periodicidad y cronograma de pruebas del plan de contingencias. • Se elaborará un plan en el cuál se evidencia el resultado de las pruebas para el plan de contingencia 3. Responsables por actividad y escalamiento de aprobaciones. • Las actividades a realizar están direccionadas por el sistema de mesa de ayuda, adicional en los subprocesos del área se menciona que perfil atiende los subprocesos. Las aprobaciones en la documentación son realizadas por la Subdirectora Técnica. 4. Identificación de riesgos, servicios e infraestructura critica. • Se elaborará documento en el que se especifique los riesgos que se tienen en sistemas a la	1. Hace falta mayor precisión y descripción de las acciones en cuanto a actividades, perodicidad y cronograma, responsables e identificación de riesgos que comprenden el Plan de Recuperación de Desastres. 2. Disponibilidad presupuestal para la adquisición de los elementos necesarios para evitar los desastres informáticos 3. Estaba en proceso de identificación y actualización el mapa de riesgos	1.Actualizar, ampliar y mejorar el documento DRP con mayor alcance, descripción identificación y detalle de los elementos que lo componen, específicamente en lo que se refiere a actividades, cronograma, responsables y la identificación de riesgos que actualmente se está elaborando junto con el área de procesos y riesgos para la identificación y la documentación de los mismos. 2.Alimentar el documento con la información que está contenida en otros documentos del área que contienen información importante, por ejemplo, la caracterización del proceso, politicas, plan de back up, etc. El documento se continuará revisando semestralmente para validar su actualización y pertinencia con el contexto organizacional. 3. Realizar trimestralmente una mesa de trabajo que permita hacer seguimiento oportuno al DRP (levantar evidencias de cada reunión con actas)	Área de sistemas	Equipo del área de sistemas vinculados y contratistas (profesionales, tecnólogos)	Todas las acciones de mejora se desarrollarán en el periodo de tiempo comprendido entre el 03 y el 30 de abril de 2018.	03 de abril de 2018	30 de abril de 2018	1.Documento DRP actualizado - Versiones mejoradas del documento 2.Caracterización procesos 3.Presupuesto aprobado 4.Correos 5.Politicas 6.Planes 7.Niveles de servicio (mesa de ayuda) 8.Actas 9. Listas de asistencia	Establecer en el "Cronograma de Ejecución" las fechas en las cuales se desarrollara como acción de mejora las mesas de trabajo que permitirán hacer seguimiento oportuna al DRP, con sus correspondientes evidencias. Igualmente atender la recomendación presentada por la firma auditora en lo referente a observar y analizar las recomendaciones que se pueden dar en el marco de la ISO 27001, la cual proporciona una metodología para implementar la gestión de la seguridad de la información en una organización basada en la gestión del Riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente, a la par en COBIT 5 empleado por quienes tienen como responsabilidad primaria los procesos de negocio y la tecnología, aquellos de quien depende la tecnología y la información confiable, y los que proveen calidad, confiabilidad y control de TI.
Copias y Respaldo de la Información	2	Copias de Seguridad y restauración de las mismas. Encontramos que actualmente se están realizando el respaldo de la información de acuerdo con la estructura que se nombra dentro del documento "plan de contingencias", es decir, abuelo, padre e hijo, asegurando que la totalidad de la información sea respaldada, sin embargo, no se han realizado ni documentado pruebas de respaldo en sitios alternos o sistemas de información diferentes al productivo, situación que genera posibles vulnerabilidades por falta de evaluaciones e indicadores en las restauraciones de la información.	Al igual que la recomendación anterior, es importante no solo realizar copias de seguridad sino también sus pruebas de restauración e integridad de datos, con el fin de asegurar la calidad en la información y la estabilidad y funcionamiento de los sistemas de información y bases de datos. La minimización del riesgo en cuanto a perdida y/o daño de la información, es uno de los principales aspectos para asegurar la continuidad y respaldo en la información corporativa.	Se elaborará un plan en el cuál se evidencia el resultado de las pruebas para el plan de contingencia, actualmente se están evaluando varias herramientas para validar la integridad y confiabilidad de los respaldos	1. En el plan de contingencia (DRP) que se tenia al momento de la auditoria no contemplaba las pruebas de integridad, ni laspruebas de restauración y respaldos.	1.Diseñar politica de verificación e integridad de los respaldos de la Corporación 2.Generar y almacenar las evidencias de las verificaciones realizadas. 3.Determinar la periodicidad de las pruebas y configurarlas en el calendario de la persona responsable 4.Incluir este proceso en el documento de DRP 5. Realizar mesas de trabajo para verificar el cumplimiento de las actividades, asi como su respectiva actualización y mejoramiento. La politica y la consignación de las evidencias se inició inmediatamente se identificó el hallazgo. Propiamente, desde el 01 de febrero.	Área de sistemas	Equipo del área de sistemas vinculados y contratistas (profesionales, tecnólogos)	Todas las acciones de mejora se desarrollarán en el periodo de tiempo comprendido entre el 01 de febrero de 2018 y el 30 de abril de 2018.	01 de febrero de 2018	30 de abril de 2018	1.Creación de politica de verificación de respaldos 2. Generacion de las evidencias de las verificaciones de los respaldos creados 3.Creación de actividades en el calendario de los responsables. 4. Listas de asistencia a las capacitaciones. 5. Actas	Se invita a definir periodos de continuidad en la realización de las "Mesas de trabajo" como acción permanente en el análisis de control al cumplimiento de las actividades definidas como acción de mejora para contrarrestar el hallazgo presentado por la firma auditora. Igualmente analizar el riesgo "pérdida y/o daño de la información " como uno de los principales aspectos para asegurar la continuidad y respaldo en la información corporativa, descrito por el ente auditor, realizando su valoración y calificación correspondiente para diseñar los controles adecuados y mitigar su posible materialización.