Cédula de Control y Registro de Manuales de Procedimientos del CONALEP

a) Datos del registro

Folio de inscripción	Fecha	Volumen no.	Página
CCR-080	24 de noviembre 2022	2	4 de 10

b) Datos del Manual

Unidad Administrativa	Código	No. de Versión
Dirección Corporativa de Tecnologías Aplicadas	Pr-ADMVO-CONALEP-006	01

Fecha del Manual	No. de Fojas	Total de Páginas	No. de Ejemplar
26 de septiembre de 2022	46	90	1 de 2

FIRMAS

Samantha Belén Carballo Gutiérrez
Visto Bueno
Secretaría de Planeación y Desarrollo Institucional

Carolina Maribel Martínez Loyo
Responsable
Directora de Evaluación Institucional

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

conalep

Manual de Procedimientos

Dirección Corporativa de Tecnologías Aplicadas

Octubre, 2022

		Fecha		
EDUCACIÓN	**Cédula de Autorización**	**Día**	**Mes**	**Año**
		20	10	2022

Nuevo: (X)	**Modificación ( )**	**Versión No. (1)**

Nombre:	Manual de procedimientos de la Dirección Corporativa de Tecnologías Aplicadas, medidas complementarias al Manual de Organización del CONALEP.
Objetivo:	Prever, planear, coordinar y controlar los servicios que proporciona la Dirección Corporativa de Tecnologías Aplicadas, en cumplimiento de la normatividad, políticas y lineamientos aplicables, y contribuir a la efectiva administración de las tecnologías, en beneficio de la calidad de los servicios que se ofrecen en la Institución.
Contenido:	**Macroproceso** I. Soporte gestión de recursos. **Proceso** I. Tecnologías de la información. **Procedimientos** I. Planeación estratégica. II. Administración del presupuesto y contrataciones. III. Administración de la configuración. IV. Administración de la seguridad de la información.

Firmas de Autorización i)

Unidad Administrativa	Titular
Dirección Corporativa de Tecnologías Aplicadas	**José Cartagena Subdias**

Glosario

Concepto	Descripción
Acuerdo	Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, en la Administración Pública Federal.
Activo de información	La información, los datos y los recursos que la contienen, procesan y transmiten, que por su importancia y el valor que representa para una Institución, deben ser protegidos.
Acuerdo de confidencialidad	El instrumento que se celebra entre partes para restringir el uso o divulgación pública o hacia terceros de la información o conocimiento que se trate con motivo de la relación existente.
Activo de información esencial	El activo de información cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura de TIC o en los servicios que soporta.
Amenaza	El posible acto o circunstancia interna o externa que puede explotar, de manera intencional o circunstancial, la debilidad presente en un activo de información. Una amenaza puede tener diferente nivel de riesgo de acuerdo con los escenarios en los que se presente.
Arquitectura Institucional	El enfoque mediante el cual se estructuran los componentes de la Institución (procesos, información, arquitectura tecnológica y personas) delineando sus relaciones y evolución en el tiempo, permite a las áreas de TIC entender y atender sus necesidades desde una perspectiva integral y estratégica, aportando valor.
Arquitectura tecnológica	La estructura de hardware, software y redes de telecomunicación requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC en la Institución.
Autenticación electrónica	El procedimiento informático que permite identificar de manera individual e inequívoca los atributos de un usuario, con la finalidad de que éste pueda acceder a un aplicativo de cómputo o a un servicio electrónico.
Borrado seguro	El proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.
Centro de Datos	El espacio físico donde se concentran los recursos necesarios, consistentes en equipo informático y redes de comunicaciones para el procesamiento de la información de una Institución o proveedor de servicios.

Elaboró	Revisó y Autorizó
Angelica Olin Sánchez	José Cartagena Subdias

Concepto	Descripción
Componente tecnológico	El producto de hardware o software con una funcionalidad específica que permite satisfacer una necesidad y que, junto con otros elementos tecnológicos proporcionan un beneficio integral o mayor funcionalidad técnica.
Contrato marco de TIC	Instrumento celebrado entre la Oficialía Mayor de la SHCP y posibles proveedores de TIC, con el apoyo técnico de la CEDN para estandarizar las características y precios sobre adquisiciones, arrendamientos y servicios de TIC.
Contrataciones consolidadas	La integración de los procedimientos de contratación de bienes o servicios tecnológicos, entre entes públicos
Contrataciones anticipadas	La excepción otorgada por la Secretaría de Hacienda y Crédito Público para que las dependencias o entidades, de forma previa a la autorización de sus presupuestos, puedan convocar, adjudicar y formalizar contratos cuya vigencia inicie en el ejercicio fiscal siguiente de aquel en el que se formalizan, de conformidad con lo señalado en el segundo párrafo del artículo 25 de la LAASSP.
Controles de seguridad de la información	Las medidas establecidas para preservar la confidencialidad, integridad y disponibilidad de los activos de información Institucionales contra las amenazas latentes o existentes y, que coadyuvan en la gestión de riesgos inherentes a su uso.
Controles mínimos de seguridad de la información	Los controles de seguridad de la información mínimos, indispensables y obligatorios establecidos por la CEDN para la protección de los activos de información.
Datos abiertos	Los datos digitales de carácter público que pueden ser usados, reutilizados y redistribuidos por cualquier interesado.
Estrategia Digital Nacional (EDN)	El plan de acción del Ejecutivo Federal para aprovechar el potencial de las tecnologías de la información y comunicación, incluidos los servicios de banda ancha e Internet, como elemento catalizador del desarrollo del país, mediante su incorporación a la vida cotidiana de las personas, y a la Administración Pública Federal, mediante el uso de la informática y el desarrollo del gobierno digital.
Estándares abiertos	Los desarrollados o aprobados, y mantenidos a través de un proceso impulsado por la colaboración y el consenso, facilitan la interoperabilidad y el intercambio de datos entre los diferentes productos o servicios, y están destinados para la adopción generalizada.

Elaboró	**Revisó y Autorizó**
Angelica Olin Sánchez	José Cartagena Subdias

Concepto	Descripción
Estándares técnicos	Las características técnicas de bienes y servicios de TIC definidas por la CEDN, así como las mejores prácticas aplicables a la gestión de las TIC que deberán ser consideradas por las Instituciones en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información, y en los proyectos de desarrollo que se realicen con recursos humanos internos, a fin de homologar la capacidad tecnológica, garantizar la interoperabilidad entre éstas, y fomentar el ahorro en el ejercicio del gasto público.
Firma Electrónica Avanzada	El conjunto de datos y caracteres que permite la identificación del firmante, creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa.
Gobierno Digital	Las actividades basadas en tecnologías de información y comunicación que el Estado desarrolla para aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a los ciudadanos y dar transparencia a las acciones de gobierno.
Herramienta de Gestión de Política TIC	La plataforma web administrada por la CEDN disponible para el control y gestión de las actividades que realicen las Instituciones establecidas en el presente Acuerdo.
Incidente de seguridad de la información	El evento o serie de eventos de seguridad de la información no deseados o inesperados, con probabilidad significativa de comprometer las funciones esenciales de la Institución y amenazar la seguridad de la información.
Infraestructura de TIC	El hardware, software, aplicativos de cómputo, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.
Instituciones	Las dependencias y entidades integrantes de la Administración Pública Federal.
Instrumento de colaboración	Acuerdo o convenio formalizado entre Instituciones para establecer acciones que mejoren el aprovechamiento de las TIC, su infraestructura o recursos, con base en los principios de austeridad y eficiencia.

Concepto	Descripción
Interoperabilidad	La capacidad de organizaciones y sistemas dispares y diversos, para interactuar con objetivos consensuados y comunes con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las Instituciones compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnología de información y comunicación.
Inventario Institucional de bienes y servicios de TIC	El listado que comprende el equipo de cómputo, aplicaciones, software, bases de datos, servicios e infraestructura de cada Institución; constituye uno de los elementos de la Arquitectura Institucional.
Inventario de bienes y servicios de TIC de la APF	El listado que integra los Inventarios Institucionales de bienes y servicios de TIC, concentrado por la CEDN.
Niveles de servicio	El establecimiento de las características y parámetros de un servicio contratado incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución.
Oficio de pronunciamiento del OCF	El documento mediante el cual el OCF en la Institución que planea llevar acabo la contratación, emite su pronunciamiento favorable o sugerencias u observaciones de manera fundada y motivada respecto de la contratación de que se trate.
Plan de continuidad de operaciones	Al instrumento Institucional que indica los insumos técnicos, humanos, roles específicos y organización interna que garanticen la continuidad de las operaciones tecnológicas en las Instituciones.
Plan de recuperación ante desastres	Al instrumento Institucional que marca las pautas para la estabilización y restauración de los servicios o activos de información esenciales a partir de un estado de contingencia o interrupción, provocado por la naturaleza o por el ser humano.
Procesamiento de Datos	El tratamiento de datos (elementos básicos de información) que se lleva a cabo de manera automática por medio de sistemas o aplicativos de cómputo.
Proceso esencial	El que está relacionado con la generación y entrega de valor a los ciudadanos, ya sea en forma de productos o servicios; representa las actividades clave de la Institución para alcanzar sus objetivos.
Programa de gestión de vulnerabilidades:	Al proceso de identificación, clasificación y priorización para la atención y remediación o mitigación de vulnerabilidades encontradas en los activos de información de la Institución en un periodo determinado.

Elaboró	Revisó y Autorizó
Angelica Olin Sánchez	José Cartagena Subdias

Concepto	Descripción
Proyecto estratégico de TIC	El que requiere un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC, que puede o no requerir la contratación de bienes o servicios en materia de TIC para su ejecución y cuya implementación contribuye significativamente al logro de los objetivos estratégicos y metas de la Institución.
Proyecto operativo de TIC	El proyecto no considerado como estratégico que requiere de un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC que soporta la operación diaria de la Institución; puede o no requerir la contratación de bienes o servicios en materia de TIC para su ejecución.
Riesgo	La probabilidad de que una amenaza pueda explotar una vulnerabilidad, generando un impacto sobre la infraestructura de TIC y los activos de información de la Institución.
Repositorio de software de la APF	El espacio administrado por la CEDN para concentrar el código fuente de las aplicaciones o programas desarrollados o con titularidad de las Instituciones, que les permita usar, estudiar, compartir y modificar el software con la finalidad de mejorar la calidad y seguridad de la gestión de la información, fomentando el desarrollo colaborativo entre instituciones para cubrir sus necesidades comunes y generar ahorros en el gasto público.
Sistema CONALEP	Sistema conformado por 30 Colegios Estatales las Oficinas Nacionales del CONALEP, La Unidad de Operación desconcentrada para el Distrito Federal, La Representación del CONALEP en el Estado de Oaxaca, 8 Centros de Asistencia y Servicios Tecnológicos y 307 planteles.
Seguridad de la Información	La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
Seguridad Nacional	Las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, de conformidad con lo señalado en el Artículo 3 de la Ley de Seguridad Nacional.
Servicios en la Nube	Al modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente, que se encuentren localizados fuera o dentro del territorio nacional, en instalaciones del Estado o en instalaciones privadas.

Elaboró	Revisó y Autorizó
Angelica Olin Sánchez	José Cartagena Subdias

Concepto	Descripción
Software Libre	El programa informático cuyo código fuente cumple con las cuatro Libertades del Software Libre y por ende se encuentra disponible para ser ejecutado, estudiado, modificado o distribuido libremente, independientemente de su costo o gratuidad.
Tecnologías de la Información y Comunicación	El equipo de cómputo, software, dispositivos de impresión, infraestructura y servicios que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.
Visto bueno de la CEDN	La aprobación que otorga la CEDN a las UTIC de las Instituciones, a partir del cumplimiento que éstas realicen de las políticas, disposiciones, lineamientos, criterios técnicos, metodologías, guías, instructivos y demás instrumentos análogos que sean emitidos por la CEDN.
Vulnerabilidad	A la debilidad presente en un activo de información que potencialmente permitirá que una amenaza lo impacte de manera negativa, con posibles afectaciones para la seguridad de la información dentro de la Institución.

Elaboró	Revisó y Autorizó
Angelica Olin Sánchez	José Cartagena Subdias

Siglas

Sigla	Significado
ASN	Autonomous System Number - Número de Sistema Autónomo
CEDN	Coordinación de Estrategia Digital Nacional de la Oficina de la Presidencia de la República.
CONALEP	Colegio Nacional de Educación Profesional Técnica
Coordinaciones	Las coordinaciones adscritas a la Dirección Corporativa de Tecnologías Aplicadas.
CNI	Centro Nacional de Inteligencia, Órgano Administrativo Desconcentrado de la Secretaría de Seguridad y Protección Ciudadana
DCTA	Dirección Corporativa de Tecnologías Aplicadas
DOF	Diario Oficial de la Federación
ERISC	Equipo de Respuesta a Incidentes de Seguridad en TIC
GTDTIC	Grupo de Trabajo para la Dirección de TIC.
Herramienta	Herramienta de Gestión de la Política TIC 2.0
HGPTIC	Herramienta de Gestión de la Política TIC 2.0
IPv4 (Internet Protocol version 4)	Protocolo de Internet versión 4
IPv6 (Internet Protocol version 6)	Protocolo de Internet versión 6
LAASSP	Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público
MGSI	Marco de Gestión de Seguridad de la Información
NIC (Network Information Center)	Autoridad que se encarga de administrar los nombres de dominio de un país y de asignarlos a quien los solicita; así como la asignación de ASN o bloques de IPv4 ó IPv6
OCF	Órgano de Control y Fiscalización de las Instituciones, el cual considera a los Órganos Internos de Control y/o análogos dependientes de la Secretaría de la Función Pública
ON	Unidades administrativas adscritas a Oficinas Nacionales del Colegio Nacional de Educación Profesional Técnica.
POTIC	Portafolio de proyectos de Tecnologías de la Información y Comunicación
PNCCIMGP	Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública
RCEO	Representación del CONALEP en el Estado de Oaxaca
RSII	Responsable de la Seguridad de la Información en la Institución.
SATYC	Sistema de archivo de trámite y concentración.
SEP	Secretaría de Educación Pública
SFP	Secretaría de la Función Pública

Elaboró	Revisó y Autorizó
Angelica Olin Sánchez	José Cartagena Subdias

Sigla	Significado
SGSI	Sistema de Gestión de Seguridad de la Información.
SHCP	Secretaría de Hacienda y Crédito Público
SI	Seguridad de la Información
TIC	Tecnologías de la Información y Comunicación
UODCDMX	Unidad de Operación Desconcentrada para la Ciudad de México.
UPCP	Unidad de Política y Control Presupuestario de la SHCP
UTIC	Unidad de Tecnologías de Información y Comunicaciones o área responsable de las TIC en cada Institución.

Elaboró	**Revisó y Autorizó**
Angelica Olin Sánchez	José Cartagena Subdias

Presentación.

El Colegio Nacional de Educación Profesional Técnica (CONALEP) ha mantenido un liderazgo en la prestación de servicios de educación Profesional Técnica y Profesional Técnica Bachiller, y en su carácter vanguardista ha consolidado su Sistema Corporativo de Gestión de la Calidad, lo cual ha permitido tener un esquema de operación académica y administrativa eficiente y transparente, que favorece la corresponsabilidad en las relaciones intergubernamentales y la articulación de esfuerzos entre el CONALEP (Oficinas Nacionales), Colegios Estatales, la Unidad de Operación Desconcentrada para la Ciudad de México, y la Representación del CONALEP en el Estado de Oaxaca, con el propósito permanente de contribuir al desarrollo local, regional, estatal y nacional, y de esa manera lograr su Misión y Visión. Asimismo, ha enfrentado los retos de promover la equidad social y educativa y contribuir en el mayor acceso al conocimiento, entrelazados para potenciar la educación en México.

En este marco de ideas, la gestión de las tecnologías de la información es de suma importancia en la gestión institucional, ya que el elemento tecnológico es fundamental en las herramientas utilizadas para el logro de los objetivos y cumplimiento de metas institucionales, es por ello, que se tiene la obligación de contar con procedimientos actualizados que conduzcan al cumplimiento y mejor desempeño de las funciones y actividades asignadas a cada una de las áreas que conforman el Colegio, proporcionando las herramientas tecnológicas como apoyo para su cumplimiento.

El propósito del presente documento, es contribuir en la optimización de beneficios para el buen servicio de las herramientas tecnológicas en el CONALEP y dar cumplimiento a las funciones de la Dirección Corporativa encomendadas en al Manual de Organización del Sistema CONALEP, y a su vez, agilizar y cubrir oportunamente, las necesidades en materia de TIC identificadas en cada una de las Unidades Administrativas, a fin de que su operación, se oriente hacia el logro de la Misión y Visión de la Institución, desarrollo de los objetivos, estrategias y líneas de acción establecidas por el Colegio Nacional de Educación Profesional Técnica.

Elaboró	**Revisó y Autorizó**
Angelica Olin Sánchez	José Cartagena Subdias

1 Objetivo del Manual.

El objetivo del manual es describir los procedimientos de la Dirección Corporativa de Tecnologías Aplicadas para proporcionar los bienes y servicios informáticos que soliciten las Unidades Administrativas del CONALEP, Unidad de Operación Desconcentrada para la Ciudad de México, Representación del CONALEP en el Estado de Oaxaca, Colegios Estatales, Planteles y CAST, en cumplimiento de la normatividad, políticas y lineamientos aplicables, y contribuir al desarrollo de una efectiva administración de los servicios en materia de TIC, en servicio y seguridad de la información conforme a sus atribuciones, en coordinación con las Unidades Administrativas del CONALEP.

2 Sustento Legal y Marco Jurídico- Administrativo.

Sustento Legal.

Las atribuciones de la Dirección Corporativa de Tecnologías Aplicadas que dan sustento a los procedimientos actualizados que se encuentran establecidos en el Artículo 24° del Estatuto Orgánico del Colegio Nacional de Educación Profesional Técnica y en el Manual de Organización del Sistema CONALEP.

Marco Jurídico – Administrativo.

Constitución Política de los Estados Unidos Mexicanos.

Leyes.

Ley Federal de las Entidades Paraestatales.
Ley Federal de los Trabajadores al Servicio del Estado.
Ley Federal de Presupuesto y Responsabilidad Hacendaria.
Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
Ley General de Transparencia y acceso a la Información Pública.
Ley Federal de Transparencia y Acceso a la Información Pública.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Ley Federal de Procedimiento Administrativo.
Ley General de Responsabilidades Administrativas.
Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Reglamentos.

Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.
Reglamento de la Ley de la Propiedad Industrial.
Reglamento de la Ley Federal del Derecho de Autor.
Reglamento de la Ley de Obras Públicas y Servicios relacionados con las mismas.

Reglamento de la Ley Federal de las Entidades Paraestatales.
Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Decreto.

Decreto por el que crea el Colegio Nacional de Educación Profesional Técnica.
Decreto del Presupuesto de Egresos de la Federación para el Ejercicio Fiscal correspondiente.
DECRETO por el que se aprueba el Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública 2019-2024.
Decreto por el que se expide la Ley General de Transparencia y acceso a la Información Pública.

Estatutos.

Estatuto Orgánico del CONALEP.

Acuerdos.

Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.
ACUERDO por el que se emite la Política de Transparencia, Gobierno Abierto y Datos Abiertos de la Administración Pública Federal 2021-2024.

Manuales.

Manual General de Organización del CONALEP.
Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.

Planes y Programas

Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública 2019-2024.
Plan Nacional de Desarrollo 2019-2024.

Documentos Normativos – Administrativos

Estándares Técnicos de bienes y servicios de TIC emitidos por la Coordinación de Estrategia Digital Nacional.
Estrategia Digital Nacional 2021-2024.

Elaboró	**Revisó y Autorizó**
Angelica Olin Sánchez	José Cartagena Subdias

Bases técnicas de Seguridad Informática para las dependencias y entidades de la Administración Pública Federal, emitido por la Coordinación de Estrategia Digital Nacional.
Guía para la Transición al Protocolo de Internet versión 6 (IPv6) en la Administración Pública Federal que emite la Coordinación de Estrategia Digital Nacional.

Elaboró	**Revisó y Autorizó**
Angelica Olin Sánchez	José Cartagena Subdias

3 Descripción del Macroproceso

En el marco del Macroproceso: Gestión de recursos, se describe como Apoyo del Sistema CONALEP que se encarga de la Gestión de: Recursos Humanos, Recursos Financieros, Recursos Materiales, Servicios y de la Gestión de Tecnologías de la Información en la atención de las necesidades de las Unidades Administrativas, Colegios Estatales, Unidad de Operación Desconcentrada para la Ciudad de México y Representación del CONALEP en el Estado de Oaxaca.

El Macroproceso Gestión de recursos está integrado por los siguientes procesos:

- Planeación, organización y administración de los recursos humanos.
- Infraestructura y servicios.
- Tecnologías de la información.
- Apoyo Jurídico

Por lo antes expuesto, en este manual se desarrolla la descripción de los procedimientos que soportan el proceso de Tecnologías de la Información y de las políticas y disposiciones en las tecnologías de la información y comunicaciones, y en la seguridad de la información.

4 Proceso: Tecnologías de la información y comunicación.

Derivado de la recepción de los lineamientos para los programas de mantenimiento al equipamiento, inmuebles, instalaciones y de las tecnologías, su coordinación y supervisión, hasta la evaluación de su eficacia, identificación de las TIC y TAC para el proceso de enseñanza aprendizaje, su mantenimiento y supervisión hasta el establecimiento de acciones de mejora, con el propósito de contar con las herramientas tecnológicas de apoyo para la Comunidad CONALEP, impactando en el mejoramiento del desempeño y desarrollo en la Institución y en el logro de los objetivos institucionales, alineados a la Misión y Visión que tiene encomendados el Colegio.

Asimismo, a la Dirección Corporativa de Tecnologías Aplicadas le corresponde gestionar los recursos tecnológicos del Colegio, para lo cual se administra a través de cuatro procedimientos.

Procedimientos:

I. Planeación estratégica.
II. Administración del presupuesto y contrataciones.
III. Administración de la configuración.
IV. Administración de la seguridad de la información.

4.1 Objetivo del Proceso.

Describir los procedimientos de la Dirección Corporativa de Tecnologías Aplicadas para proponer y establecer las normas, lineamientos y políticas que permitan obtener una mejor

planeación, organización y administración de TIC, asimismo los mecanismos que permitan la administración de la seguridad de la información conforme a las atribuciones de la Institución, basado en el cumplimiento de perfil de un modelo de gobierno de Tecnologías de Información y Comunicación (TIC) en la Institución y contribuir al cumplimiento de los objetivos que tiene encomendados el Colegio.

4.2 Responsables.

- Dirección Corporativa de Tecnologías Aplicadas
- Coordinación de Comunicaciones
- Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar
- Coordinación de Tecnologías Aplicadas a la Educación

La Dirección Corporativa de Tecnologías Aplicadas (DCTA) será responsable de: establecer, dirigir y evaluar un modelo de gobierno de Tecnologías de Información y Comunicación (TIC) en la Institución; así como definir, evaluar, controlar, vigilar e informar del cumplimiento de los planes estratégicos de TIC y los mecanismos que permitan la administración de la seguridad de la información conforme a sus atribuciones, en coordinación con las Unidades Administrativas del CONALEP, a fin de coadyuvar en la consecución de los objetivos del Sistema CONALEP y en la generación de mayores oportunidades de cobertura, equidad y calidad educativa para los estudiantes.

Las Coordinaciones tendrán la responsabilidad de desarrollar y controlar los proyectos en su ámbito de competencia y, en el caso de que algún proyecto requiera de contratación, deberá apoyar técnicamente en la gestión de la adquisición, permitiendo al CONALEP contar con un sistema de información a nivel nacional, la incorporación de metodologías y tecnología de punta, necesidades de capacitación, actualización, automatización y adopción de TIC, a fin de mantener los niveles de servicios acordados con el fin de coadyuvar en la formación escolarizada, y en su caso, la no escolarizada y mixta, en coordinación con las Unidades Administrativas del Sistema CONALEP, conforme a sus atribuciones y la normatividad aplicable.

4.3 Alcance

Desde la recepción de normas y lineamientos emitidos por las dependencias globalizadoras hasta su aplicación, en el ámbito de la administración de Tecnologías de Información y Comunicación (TIC) y Seguridad de la Información en las Unidades Administrativas del CONALEP, la Unidad de Operación Desconcentrada para la Ciudad de México y la Representación del CONALEP en el Estado de Oaxaca.

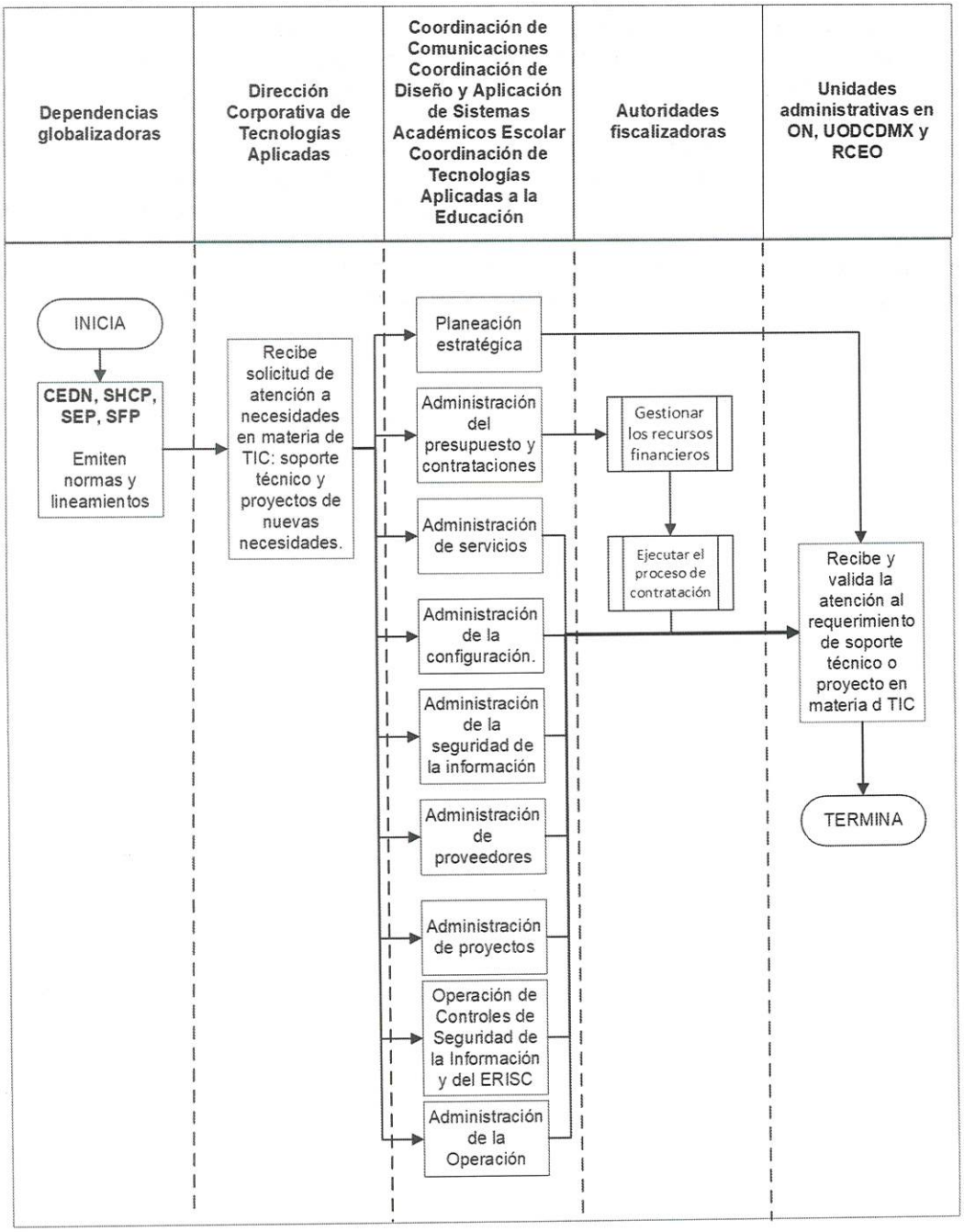
4.4 Requisitos Generales de Operación del Proceso.

a. Identificación de necesidades y planeación de los recursos necesarios para la operación de los servicios en Tecnologías de Información y Comunicaciones;

b. Coordinar el proceso de adquisición de bienes informáticos de usuario final en su aspecto técnico, proponiendo su asignación en las Unidades administrativas del Sistema CONALEP; llevar a cabo la implementación y coordinación de los programas de mantenimiento de los mismos, así como apoyar a los Colegios Estatales, Representaciones y Planteles del Sistema CONALEP en la implementación de sus programas de mantenimiento.
c. Proponer la arquitectura tecnológica de sistemas y aplicaciones institucionales así como coordinar su análisis, diseño, desarrollo, operación y mantenimiento.
d. Fomentar la cultura informática en el Sistema CONALEP a través de la implementación de aplicaciones y cursos de capacitación que se proporcione a los usuarios el conocimiento y herramientas necesarias para lograr que la infraestructura instalada de cómputo y comunicaciones del CONALEP, se aproveche adecuadamente.

Elaboró	**Revisó y Autorizó**
Angelica Olin Sánchez	José Cartagena Subdias

4.5 Diagrama de Bloque del Proceso Tecnologías de la información.



Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

5 Integración de los Procedimientos

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

5.1 Procedimiento Planeación estratégica

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

Historial de Cambios

Revisión número: 01 Fecha de aprobación: 26 de septiembre de 2022

Descripción y motivo del cambio.

Describir los cambios realizados considerando lo siguiente:

1. Derogación del Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información.
2. Publicación del Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.
3. Describir el procedimiento para la integración del Portafolio de proyectos en materia de Tecnologías de Información y Comunicaciones del Colegio y elaborar el informe de seguimiento del avance trimestral del portafolio de proyectos.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

5.1.1 Procedimiento.

Planeación estratégica

5.1.2 Objetivo del Procedimiento.

Mantener la operación de un modelo de gobierno de TIC en la Institución, para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC, la planeación estratégica de TIC y asegurar la adecuada organización al interior de la UTIC para la gestión de sus procesos y vinculación ordenada con sus usuarios.

5.1.3 Responsables.

- Dirección Corporativa de Tecnologías Aplicadas (DCTA).
- Coordinación de Comunicaciones
- Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar
- Coordinación de Tecnologías Aplicadas a la Educación

Serán responsables de:

- La Dirección Corporativa de Tecnologías Aplicadas (DCTA) será responsable de mantener la operación un modelo de gobierno de TIC en la Institución, para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC, la planeación estratégica de TIC y asegurar la adecuada organización al interior de la DCTA para la gestión de sus procesos y vinculación ordenada con sus usuarios. Todos los proyectos de TIC que se pretendan ejecutar a través de prácticas de desarrollo, implementación propia o a través de contrataciones, deben apegarse a un proceso de planeación estratégica alineado a las disposiciones del Plan Nacional de Desarrollo y programas que de él deriven, la Estrategia Digital Nacional, así como a la legislación en materia de desarrollo nacional, presupuesto, austeridad y transparencia.
- Las Coordinaciones tendrán la responsabilidad de desarrollar y controlar los proyectos en su ámbito de competencia y, en el caso de que algún proyecto requiera de contratación, deberá apoyar técnicamente con la gestión de la adquisición, permitiendo al CONALEP contar con un sistema de información a nivel nacional, la incorporación de metodologías y tecnología de punta, necesidades de capacitación, actualización, automatización y adopción de TIC, a fin de mantener los niveles de servicios acordados con el fin de coadyuvar a la formación escolarizada, y en su caso, la no escolarizada y mixta, en coordinación con las Unidades Administrativas del Sistema CONALEP, conforme a sus atribuciones y la normatividad aplicable. Asimismo, valorarán la factibilidad y priorización de la necesidad de cada uno de los proyectos recibidos e identificados en el Colegio, tomando en cuenta los recursos con los que se cuenta al interior de la DCTA y los que se encuentren respaldados con la programación financiera definida en el Programa Anual de Trabajo de cada una de las Unidades Administrativas solicitantes.

5.1.4 Alcance.

La planeación de TIC se formaliza con la integración y registro del Portafolio de Proyectos de Tecnologías de la Información y Comunicación (POTIC), contemplando los proyectos estratégicos y operativos en materia de TIC y de Seguridad de la Información que el Colegio planee llevar a cabo en el siguiente ejercicio fiscal y con su respectivo seguimiento, los proyectos se desarrollarán con recursos técnicos y humanos con que cuente la Institución, así como aquellos que requieran ser contratados.

5.1.5 Requisitos Generales de Operación del Procedimiento.

Solicitar a las Unidades Administrativas de Oficinas Nacionales, a la Unidad de Operación Desconcentrada para la Ciudad de México y a la Representación del CONALEP en el Estado de Oaxaca, sus necesidades en materia de TIC que se planean llevar a cabo en el siguiente ejercicio fiscal, conformando de esta manera el Portafolio de proyectos mismos que serán sometidos para la autorización en primera instancia por los directivos del CONALEP que conforman el Grupo de Trabajo para la Dirección de TIC y en segunda por la Coordinación de Estrategia Digital Nacional a través de la Herramienta de Gestión de Política TIC.

5.1.6 Identificación de Riesgos.

Descripción del Riesgo.

Asignación insuficiente de recursos financieros, humanos y materiales para el desarrollo de los proyectos que se requieran en el Colegio, por lo que no se puedan llevar a cabo con las características especificadas por las áreas requirentes.

Tipo.

Externo y Financiero

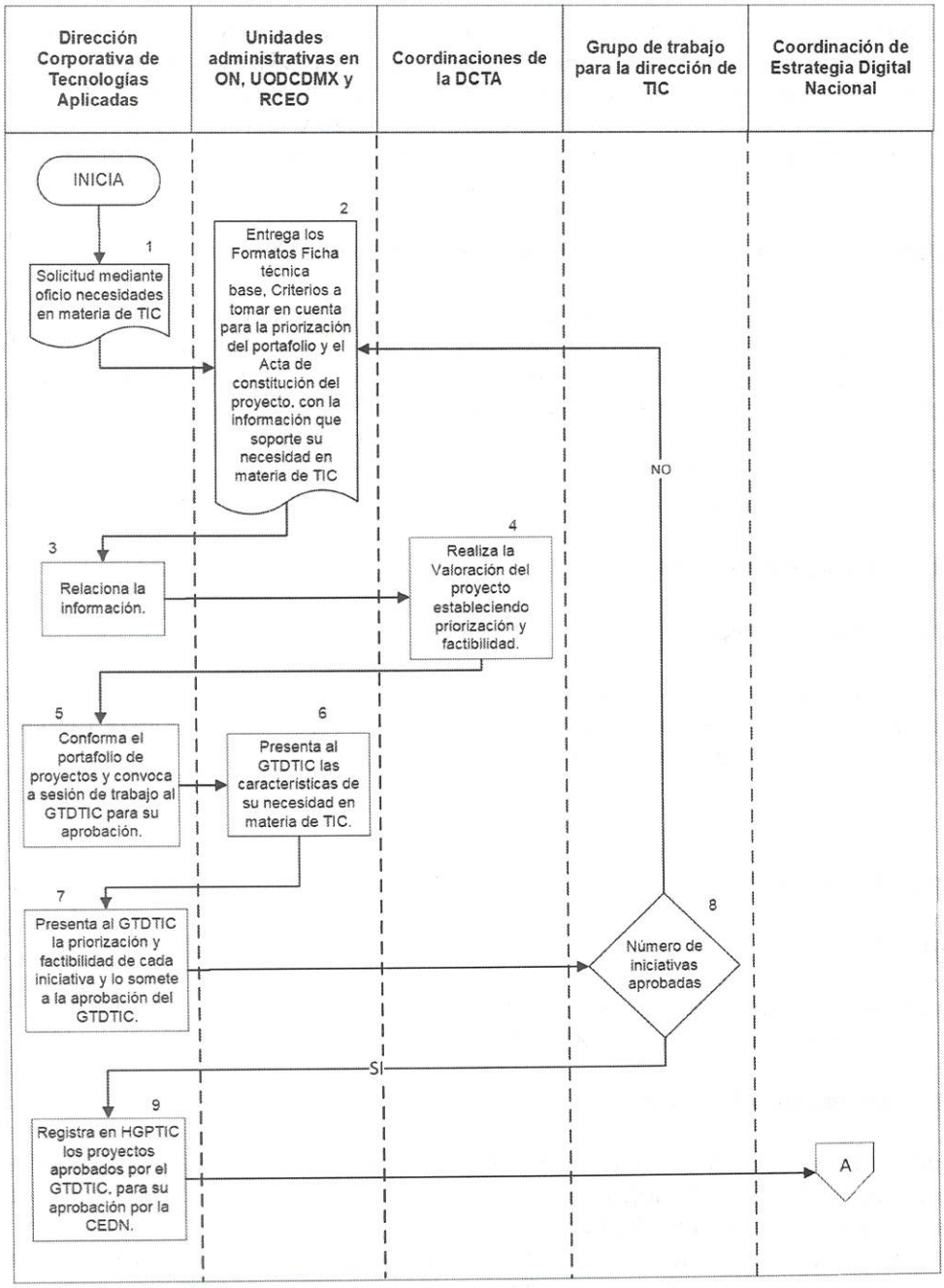
Responsables.

Unidades administrativas, UODCDMX, RCEO.
Dirección Corporativa de Tecnologías Aplicadas

Oportunidades de Atención.

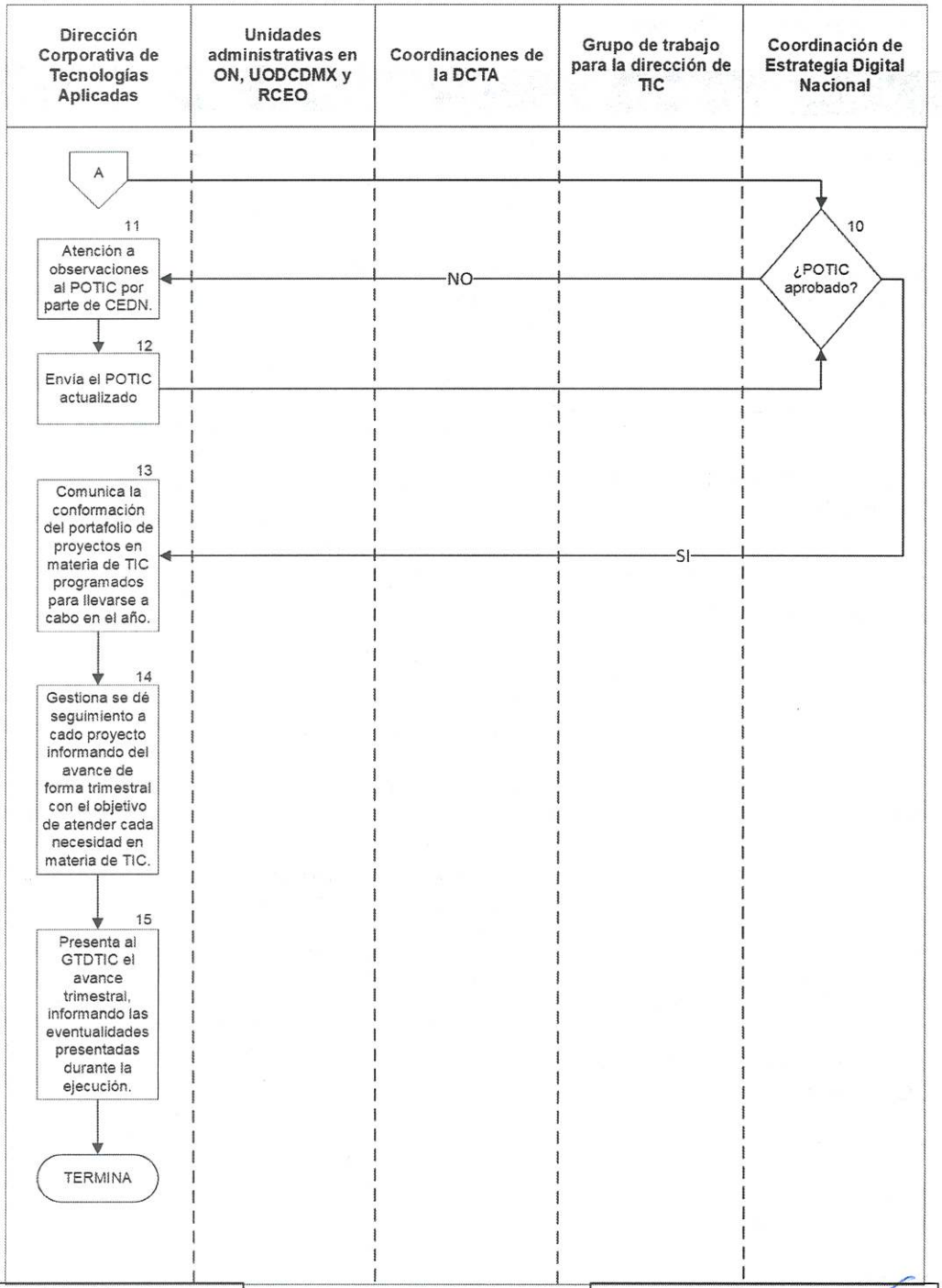
Respaldar la necesidad en materia de TIC que requiera un proceso de contratación, con la programación financiera definida en el Programa Anual de Trabajo de cada una de las Unidades Administrativas solicitantes.
Identificación oportuna de la necesidad en materia de TIC, anticipando la planeación de los recursos necesarios para llevarlo a cabo.

5.1.7 Diagrama de Flujo del Procedimiento Planeación estratégica.



Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias



Elaboró	Revisó y Autorizó
Angelica Olin Sánchez	José Cartagena Subdias

5.1.8 Descripción del Procedimiento

No.	Unidad Administrativa	Descripción de la actividad
		INICIA
1.	Dirección Corporativa de Tecnologías Aplicadas	Solicitud mediante oficio a las Unidades Administrativas adscritas a Oficinas Nacionales, Unidad de Operación Desconcentrada para la Ciudad de México, Representación del CONALEP en el Estado de Oaxaca, sus necesidades en materia de TIC a llevarse a cabo en el siguiente año fiscal, proporcionando los formatos para su llenado: Ficha técnica base, Criterios a tomar en cuenta para la priorización del portafolio y el Acta de constitución del proyecto
2.	Unidades Administrativas del CONALEP	Autoriza la entrega de los formatos (Ficha técnica base, Criterios a tomar en cuenta para la priorización del portafolio y el Acta de constitución del proyecto) requeridos con la información que soporte su necesidad en materia de TIC, debidamente firmados.
3.	Dirección Corporativa de Tecnologías Aplicadas	Gestiona a las coordinaciones de la Dirección Corporativa para establecer la valoración del proyecto identificando si se atiende con personal interno o con proceso de contratación.
4.	Coordinaciones de la DCTA.	La Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar, define y propone la valoración del proyecto en desarrollo de sistemas o aplicativos, priorizando y determinando la factibilidad de llevarse a cabo. La Coordinación de Comunicaciones y la Coordinación de Tecnologías Aplicadas a la Educación, definen y proponen la valoración del proyecto de contratación, priorizando y determinando la factibilidad de llevarse a cabo
5.	Dirección Corporativa de Tecnologías Aplicadas	Autoriza la conformación del portafolio de proyectos y convoca a sesión de trabajo al GTDTIC para su aprobación.
6.	Unidades Administrativas del CONALEP	Cada una de las unidades administrativas que requirió una necesidad en materia de TIC, presenta su proyecto al GTDTIC indicando los antecedentes, planteamiento del problema justificación, objetivo, impacto y alcance de su proyecto.
7.	Dirección Corporativa de Tecnologías Aplicadas	De las iniciativas presentadas, define el valor de factibilidad y priorización para llevar a cabo cada proyecto, tomando en cuenta el conjunto total de proyectos a programar su atención y solicita la aprobación del portafolio al GTDTIC.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

No.	Unidad Administrativa	Descripción de la actividad
8.	Grupo de Trabajo para la Dirección de TIC.	Evalúa cada una de las necesidades presentadas y emite sus comentarios de acuerdo al cumplimiento de las metas del Colegio. ¿Aprueba los proyectos? SI – Continua en la actividad 9. NO – Continua en la actividad 2.
9.	Dirección Corporativa de Tecnologías Aplicadas	Gestiona el registro en la Herramienta de Gestión de Política TIC, los proyectos aprobados por el GTDTIC, para su validación por la Coordinación de Estrategia Digital Nacional.
10.	Coordinación de Estrategia Digital Nacional	A través de la Herramienta de Gestión de Política TIC, revisa y aprueba o, emite las observaciones con respecto al Portafolio de proyectos en materia de TIC (POTIC). ¿POTIC aprobado? SI – Continua en la actividad 13. NO – Continua en la actividad 11
11.	Dirección Corporativa de Tecnologías Aplicadas	En atención a observaciones emitidas por la CEDN, gestiona la actualización de los proyectos observados.
12.		A través de la Herramienta, autoriza y envía el POTIC actualizado solicitando la aprobación del mismo por la Coordinación de Estrategia Digital Nacional. Regresa a la actividad 10.
13.	Dirección Corporativa de Tecnologías Aplicadas	Comunica al GTDTIC la conformación del portafolio de proyectos en materia de TIC programados para llevarse a cabo en el año.
14.		Gestiona a las Coordinaciones en su ámbito de competencia, se dé seguimiento a cada proyecto informando del avance de forma trimestral con el objetivo de atender cada necesidad en materia de TIC.
15.		Presenta al GTDTIC el avance trimestral, informando las eventualidades presentadas durante la ejecución.
		TERMINA

Total de actividades: 15
Duración total estimada: 255 días

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

5.1.9 Formatos que intervienen en el Procedimiento.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

Formato: Ficha técnica base PE F03
Clave: PE F03
Formulación a cargo de: Unidades administrativa que solicita su proyecto en materia de TIC.
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: Mediante oficio de solicitud vía electrónica y/o SATYC de la DCTA a las Unidades Administrativas adscritas a Oficinas Nacionales, Unidad de Operación Desconcentrada para la Ciudad de México, Representación del CONALEP en el Estado de Oaxaca, de acuerdo a la actividad 1 del Procedimiento Planeación Estratégica.

5.1.9.1 Instructivo de llenado del Formato.
PE F03

Campo	Descripción.
Nombre del proyecto.	Nombre corto con el que se identifica al proyecto, en caso de que el sistema o servicio ya exista, agregar el módulo o característica adicional que será atendida.
Año de reporte.	Año en que se atenderá la necesidad requerida.
Tipo de proyecto.	Seleccionar una de las siguientes 2 opciones: • Proyecto operativo: soporta la operación diaria de la operación de la institución incluyendo el desarrollo de plataformas tecnológicas, indicar si requiere o no presupuesto para su ejecución y contratación, especificando el trimestre en el que se requiere el producto o servicio. • Proyecto estratégico: El esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC; considerando que los proyectos estratégicos aquellos que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales o de la EDN, indicar si requiere o no presupuesto para su ejecución y contratación, especificando el trimestre en el que se requiere el producto o servicio.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

Campo	Descripción.
Categoría.	Seleccionar la categoría del proyecto, de acuerdo a lo siguiente: • Optimización. En donde por medio de la aplicación de TIC se logra una mejor manera de llevar a cabo actividades. • Digitalización. Aplicación de TIC para la conversión de contenidos a medios digitales en la generación de trámites y servicios por este medio, así como el acceso e información en este formato. • Simplificación. Aplicación de TIC para la reducción de tiempos, costos, y requisitos en los trámites y servicios, así como en la eliminación y automatización de actividades de los procesos. • Racionalización. Reducción en el costo de los recursos e insumos obtenidos de mejores prácticas y estrategias en la contratación.
Antecedentes del proyecto.	Deberá describir de manera precisa, el contexto previo que da origen al proyecto.
Planteamiento del problema.	Se deberá exponer de manera clara y breve el asunto que se requiere atender, en el que se incluya un diagnóstico general de la problemática.
Justificación del proyecto.	Se deberán describir puntualmente los motivos por los que se debe realizar el proyecto, explicando cómo se determinó el alcance del mismo.
Objetivo estratégico del proyecto.	Se deberán describir de manera clara y precisa, los resultados que se esperan alcanzar mediante la ejecución de las actividades que formen parte del proyecto.
Impacto.	Se deberá describir puntualmente la contribución o efecto significativo que producirá la implementación del proyecto.
Alcance del proyecto.	Se deberá definir de manera general el producto, servicio o resultado de TIC y SI que se logrará al término del proyecto.
Riesgo del proyecto.	Seleccionar el nivel de riesgo que pudieran afectar el éxito del proyecto o de no llevarse a cabo, asimismo indicar si se cuenta o no con un plan de mitigación.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

Campo	Descripción.
¿Planea desarrollar aplicativos móviles?	Indicar si este proyecto tiene como fin el desarrollo o no de una solución tecnológica en plataforma móvil y especificar la justificación de la respuesta seleccionada.
Línea base del proyecto – fecha de inicio.	Especificar la fecha en que el recurso humano y/o financiero se encontrará disponible para el inicio del proyecto.
Línea base del proyecto – Fecha de término:	Especificar la fecha en que el recurso humano y/o financiero se libera / ejerce para el cierre del proyecto.
Línea base del proyecto – Presupuesto Estimado:	Indicar el monto presupuestal con el que la unidad solicitante cuenta para el proyecto.
Línea base del proyecto – Partida presupuestal:	Indicar la partida presupuestal en la que la unidad solicitante tiene asignado el recurso presupuestal.
Etapas para su desarrollo – Planeación.	Indicar la fecha de inicio y fin para el cumplimiento del proceso de planeación, la cual puede estar comprendida de manera previa al año del POTIC.
Etapas para su desarrollo – Inicio.	Indicar la fecha que deberá reflejar el inicio efectivo del proyecto y la fecha fin para la etapa, periodo que tendrá que estar comprendida dentro del año del POTIC.
Etapas para su desarrollo – Desarrollo.	Indicar la fecha de inicio y fin, periodo en el que se deberán completar las actividades definidas en el plan de gestión del proyecto
Etapas para su desarrollo – Cierre del proyecto.	Indicar la fecha de inicio y fin, periodo en el que se requiere que lleve a cabo el cierre formal del proyecto, entendiéndose por éste la aceptación de la totalidad de entregables del mismo, y a partir de la cual correrán los tiempos para integrar el Informe final de la implementación.
En caso de que el proyecto requiera se gestione un proceso de contratación:	
Fecha de obtención de Dictamen Técnico de la UGD	Indicar la fecha de inicio, término y el porcentaje que representa dicha actividad para contar con las autorizaciones del OIC y de la CEDN e iniciar el proceso de contratación.
Firma del contrato	Indicar la fecha de inicio, término y el porcentaje que representa dicha actividad para contar con la firma del contrato.
Requerimiento a solicitarse al proveedor.	Indicar cuales características deberá contar el proveedor al que se le solicitará el servicio o producto.

Elaboró	Revisó y Autorizó
Angelica Olin Sánchez	José Cartagena Subdias

Campo	Descripción.
Consideraciones estratégicas.	Indicar que consideración de la Estrategia Digital Nacional se cumple con la solicitud del proyecto: • ¿La Iniciativa o Proyecto favorece el cómputo en la nube? • ¿La Iniciativa o Proyecto privilegia la aplicación de Tecnologías Verdes? • ¿La Iniciativa o Proyecto considera la digitalización de trámites o servicios de CNTSE? • ¿La Iniciativa o Proyecto considera la optimización de trámites o servicios? • Unidad administrativa solicitante. • Líder de proyecto designado: nombre, cargo y extensión telefónica. • ¿Su proyecto ha sido solicitado en el Programa Anual de Trabajo?
Dominios tecnológicos	En esta sección se deberán seleccionar los dominios tecnológicos o características que se considera deba de tener el proyecto y/o producto solicitado, indicando las características, especificaciones y estándares: • Seguridad • Cómputo central y distribuido • Cómputo de usuario final • Comunicaciones • Colaboración y correo electrónico • Internet / Intranet • Aplicativos • Bases de Datos y Datawarehousing • Sistemas de control industriales
Políticas tecnológicas generales	Indicar si el proyecto institucional que comprenda servicios e implementaciones tecnológicas y de seguridad de la información, deba atender las políticas y disposiciones generales.
Análisis FODA	El objetivo primordial es obtener conclusiones sobre la forma en que el proyecto será capaz de afrontar los cambios en el contexto (llamadas Oportunidades y Amenazas) en que desarrolla sus actividades, a partir de sus características o atributos internos (Fortalezas y Debilidades), por lo que se deberá indicar cada una de sus características en este aspecto.

Campo	Descripción.
Alineación del Proyecto	En esta sección en caso de que sea un proyecto estratégico deberá atender las metas nacionales, estrategias, objetivos y líneas de acción e indicadores, los cuales se observan en los apartados: 1. Plan Nacional de Desarrollo. 2. Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública (PNCCIMGP), indicando el Objetivo, Estrategia y Acción. 3. Objetivos y Principios de la Estrategia Digital Nacional 4. Programa Institucional del CONALEP
Fecha de elaboración / actualización.	Indicar la fecha de elaboración y/o actualización de formato.
Firmas de elaboración / actualización, revisión y aprobación	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el titular del área.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

Formato: Acta de Constitución del Proyecto. ADP F1
Clave: ADP F1
Formulación a cargo de: Unidades administrativa que solicita su proyecto en materia de TIC.
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: Mediante oficio de solicitud vía electrónica y/o SATYC de la DCTA a las Unidades Administrativas adscritas a Oficinas Nacionales, Unidad de Operación Desconcentrada para la Ciudad de México, Representación del CONALEP en el Estado de Oaxaca, de acuerdo a la actividad 1 del Procedimiento Planeación Estratégica.

5.1.9.2 Instructivo de llenado del Formato.
ADP F1

Campo	Descripción.
Clave de identificación del Programa/Proyecto	Clave que solo será especificada por la DCTA.
Fecha	Fecha de elaboración del proyecto.
Revisión.	En el momento de la creación del formato será la versión 1.0, una vez que se lleve a cabo la reunión de inicio del proyecto se actualizará dicho documento y el número de versión.
I. Nombre y Objetivo del proyecto.	Nombre corto con el que se identifica al proyecto, en caso de que el sistema o servicio ya exista, agregar el módulo o característica adicional que será atendida. Indicar el objetivo del proyecto.
II. Justificación general del proyecto	Indicar la justificación que sustenta la necesidad del proyecto en materia de TIC.
III. Datos generales del proyecto	Indicar la unidad administrativa que solicita el proyecto en materia de TIC. Indicar la unidad administrativa que impulsa el llevar a cabo el proyecto.
Necesidades del área a la que va dirigido	Indicar las necesidades que serán atendidas o cubiertas por el hecho de llevar a cabo el proyecto.
Objetivos del área a la que va dirigido	Indicar los objetivos del área a los cuales se da cumplimiento con el desarrollo del proyecto. Indicar los objetivos estratégicos a los cuales se da cumplimiento con el desarrollo del proyecto.
Descripción del proyecto	Describir en qué consistirá el resultado del proyecto.
Alcance del proyecto.	Se deberá definir de manera general el producto, servicio o resultado de TIC y SI que se logrará al término del proyecto.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

Campo	Descripción.
Fecha inicio y término del proyecto	Indicar la fecha de inicio y término en que se considera que se llevará a cabo el desarrollo del proyecto.
Supuestos o consideraciones	Indicar los supuestos o consideraciones que se tienen o que se presenten antes o durante el desarrollo del proyecto.
Entregables	Especificar los productos o los aspectos por los cuales se podrá medir el avance o el resultado del proyecto.
Gobernabilidad y Responsabilidades	Indicar los datos de los servidores públicos involucrados durante el desarrollo del proyecto: nombre y cargo, rol / responsabilidad, unidad administrativa, extensión telefónica y correo electrónico.
Datos para estimación del tamaño del proyecto	Indicar el Impacto en las operaciones de la institución (Clientes internos), Impacto en socios en términos de procesos y servicio (clientes externos), Importancia Estratégica.
Situación actual en definición y documentación de procesos	Indicar el nivel o avance que se tiene la situación actual en cuanto a definición y documentación de sus procesos.
Dependencias y Proyectos Relacionados.	Seleccionar el proyecto o dependencia con la cual se tiene relación para el desarrollo del proyecto.
Datos personales	Indicar el nivel de manejo de datos personales en el proyecto.
Planeación de Presupuesto por partida (soportado, en su caso, por un estudio de mercado)	Indicar el presupuesto planeado para este proyecto, se deberá contar el sustento con lo solicitado en el PAT de la unidad administrativa solicitante.
Relación de anexos del Acta de constitución del proyecto	Solo se deberá de indicar como resultado de la reunión inicial para llevar a cabo el proyecto.
Firmas y fechas de elaboración, revisión y aprobación de ejecución del proyecto	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el titular del área.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

Formato: Criterios a tomar en cuenta para la priorización del Portafolio. ADP FL1
Clave: ADP FL1
Formulación a cargo de: Unidades administrativa que solicita su proyecto en materia de TIC.
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: Mediante oficio de solicitud vía electrónica y/o SATYC de la DCTA a las Unidades Administrativas adscritas a Oficinas Nacionales, Unidad de Operación Desconcentrada para la Ciudad de México, Representación del CONALEP en el Estado de Oaxaca, de acuerdo a la actividad 1 del Procedimiento Planeación Estratégica.

5.1.9.3 Instructivo de llenado del Formato.
ADP FL1

Campo	Descripción.
Nombre del Proyecto/Iniciativa.	Nombre corto con el que se identifica al proyecto, en caso de que el sistema o servicio ya exista, agregar el módulo o característica adicional que será atendida.
Clave de identificación del Programa/Proyecto	Clave que solo será especificada por la DCTA.
Unidad Administrativa Solicitante	Indicar la unidad administrativa que solicita el proyecto en materia de TIC.
Especificación de criterios	Con el objetivo de determinar la factibilidad de llevar a cabo el proyecto, se deberá indicar si contribuye o no cada uno de los criterios: Contribución a los objetivos de la EDN y estrategias de la institución. • Atiende metas nacionales, estrategias, objetivos y líneas de acción e indicadores establecidos en el Plan Nacional de Desarrollo 2021-2024(Gaceta Parlamentaria Anexo XVIII y XVIII-Bis), la EDN, o alguna disposición establecida en el Decreto y Bases de Colaboración que haya Suscrito la Institución • Atiende alguno de los supuestos de: Cómputo en la nube; Digitalización de trámites o servicios del Catálogo; Tecnologías Verdes; Nacional de Trámites y Servicios del Estado; Optimización de trámites y servicios • ¿Involucra elementos de innovación? Financieros. • El presupuesto estimado se basa en algún estudio o presupuesto.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

Campo	Descripción.
	○ ( ) Sustentado en un estudio del mercado o no se requiere (por ser un desarrollo interno) ○ ( ) Cuenta con al menos una cotización ○ ( ) No se cuenta con ningún sustento formal • ¿Se cuenta con la disponibilidad presupuestal para realizar el proyecto? ○ ( ) No está registrado en el POA, ni se ha solicitado en el anteproyecto del mismo ○ ( ) Se ha solicitado en el anteproyecto del POA, pero falta la aprobación del mismo ○ ( ) Esta registrado y aprobado en el POA ○ ( ) No se requieren recursos presupuestales en el POA Riesgos • Cuenta con un plan de trabajo estimado ○ ( ) El plan de trabajo está al menos a nivel gerencial, contempla las diferentes etapas en la realización del proyecto, indicando en cada una de ellas la duración y sus productos asociados ○ ( ) El calendario solo tiene una fecha estimada de inicio y fin, y solo indican los productos asociados ○ ( ) No se cuenta con ningún plan de trabajo • El proyecto se asocia a un riesgo. ○ ( ) Ninguno ○ ( ) De bajo impacto sin plan de mitigación de riesgos ○ ( ) De bajo impacto con plan de mitigación de riesgos ○ ( ) De mediano impacto sin plan de mitigación de riesgos ○ ( ) De mediano impacto con plan de mitigación de riesgos ○ ( ) De alto impacto sin plan de mitigación de riesgos ○ ( ) De alto impacto con plan de mitigación de riesgos Aspectos normativos y legales. • Se deriva y/o asegura el cumplimiento de una norma o regulación con carácter obligatorio. Recursos humanos.

Campo	Descripción.
	• ¿El área requirente del CONALEP, con base a su ámbito de competencia, cuenta con la cantidad de capital humano necesario (en cuanto su disponibilidad, cantidad, conocimientos y experiencia) en la definición, revisión y aprobación durante toda la ejecución del proyecto, hasta su cierre?
Resultados esperados y aportación del proyecto tecnológico.	Especificar los resultados o la aportación que tendrá la implementación del proyecto.
Fecha de elaboración / actualización.	Indicar la fecha de elaboración y/o actualización de formato.
Firmas y fechas de elaboración, revisión y aprobación de ejecución del proyecto	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el titular del área.

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

Elaboró
Angelica Olin Sánchez

Revisó y Autorizó
José Cartagena Subdias

5.2 Administración del presupuesto y contrataciones

Elaboró	Revisó	Autorizó
Christian Rodríguez Fuertes	Joel Olvera Velázquez	José Cartagena Subdias

Historial de Cambios

Revisión número: 01 Fecha de aprobación: 26 de septiembre de 2022

Descripción y motivo del cambio.

Describir los cambios realizados considerando lo siguiente:

1. Derogación del Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información.
2. Publicación del Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.
3. Coordinar las acciones para el ejercicio del presupuesto destinado a las TIC, a fin de maximizar su aplicación en las contrataciones de TIC requeridas por el Colegio, así como las acciones para efectuar el acompañamiento necesario a las unidades facultadas para realizar los procedimientos de contrataciones, de manera que se asegure su ejecución en tiempo y forma, alineado al presupuesto autorizado; así como el seguimiento a los contratos que se celebren.

Elaboró	Revisó	Autorizó
Christian Rodríguez Fuertes	Joel Olvera Velázquez	José Cartagena Subdias

5.2.1 Procedimiento.

Administración del presupuesto y contrataciones

5.2.2 Objetivo del Procedimiento.

Coordinar las acciones para el ejercicio del presupuesto destinado a las TIC, a fin de maximizar su aplicación en las contrataciones de TIC requeridas por el Colegio, así como las acciones para efectuar el acompañamiento necesario a las unidades facultadas para realizar los procedimientos de contrataciones, de manera que se asegure su ejecución en tiempo y forma, alineado al presupuesto autorizado; así como el seguimiento a los contratos que se celebren.

5.2.3 Responsables.

- Dirección Corporativa de Tecnologías Aplicadas (DCTA).
- Coordinación de Comunicaciones
- Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar
- Coordinación de Tecnologías Aplicadas a la Educación

Serán responsables de:

- Evaluar, gestionar, priorizar y autorizar, en coordinación con las Unidades Administrativas del CONALEP, el ejercicio del presupuesto destinado a las adquisiciones de infraestructura, servicios y soluciones tecnológicas requeridas por la Institución, en congruencia a los diferentes tipos de modalidades académicas y opciones de formación, con apego al modelo académico institucional, asegurando la capacidad, disponibilidad, operatividad, calidad, seguridad y continuidad, de servicios y activos de TIC, conforme a la normatividad aplicable.
- Las Coordinaciones tendrán la responsabilidad de desarrollar y controlar los proyectos en su ámbito de competencia, asimismo deberán apoyar en la gestión de la adquisición, permitiendo al CONALEP contar con un sistema de información a nivel nacional, la incorporación de metodologías y tecnología de punta, necesidades de capacitación, actualización, automatización y adopción de TIC, a fin de mantener los niveles de servicios acordados con el fin de coadyuvar a la formación escolarizada, y en su caso, la no escolarizada y mixta, en coordinación con las Unidades Administrativas del Sistema CONALEP, conforme a sus atribuciones y la normatividad aplicable. Asimismo, valorarán la factibilidad y priorización de la necesidad de cada uno de los proyectos, tomando en cuenta los recursos con los que se cuenta al interior de la DCTA y los que se encuentren respaldados con la programación financiera definida en el Programa Anual de Trabajo de cada una de las Unidades Administrativas solicitantes.

5.2.4 Alcance.

La administración del presupuesto y contrataciones en materia de TIC y de Seguridad de la información, se formaliza con la integración y registro del Portafolio de Proyectos de Tecnologías de la Información y Comunicación (POTIC) que requieran un proceso de contratación para llevarse a cabo, coordinando las acciones necesarias para el adecuado ejercicio del presupuesto destinado para tal fin.

5.2.5 Requisitos Generales de Operación del Procedimiento.

Que se encuentre formalizado el Portafolio de Proyectos de Tecnologías de la Información y Comunicación (POTIC), así como el presupuesto autorizado para cada uno de los proyectos.

5.2.6 Identificación de Riesgos.

Descripción del Riesgo.

Insuficiencia presupuestal, por asignación o recorte presupuestal, para el desarrollo de los proyectos que requieran ser contratados, por lo que no se pueden llevar a cabo con las características especificadas por las áreas requirentes.

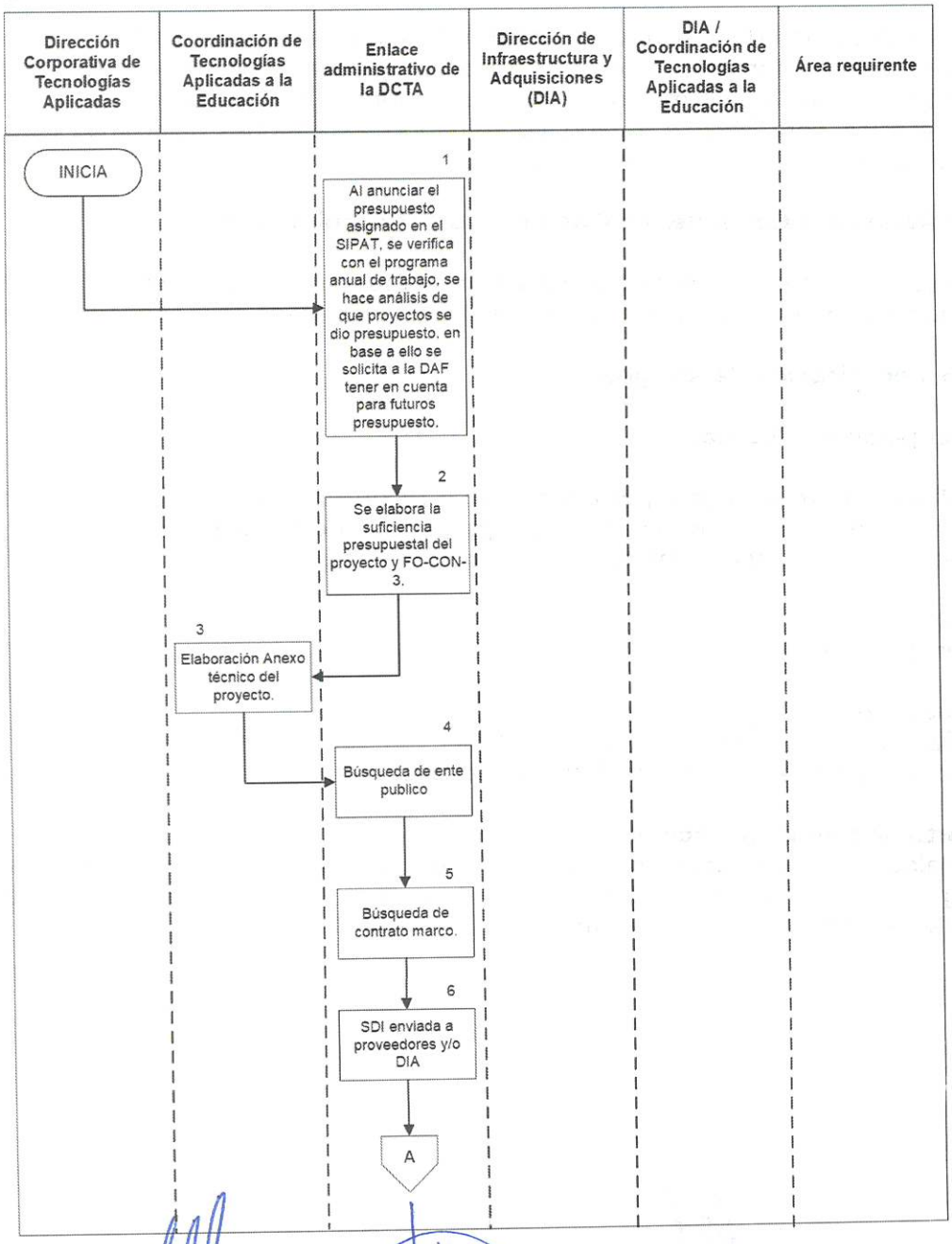
Tipo.
Externo y Financiero

Responsables.
Unidades administrativas, UODCDMX, RCEO.
Dirección Corporativa de Tecnologías Aplicadas

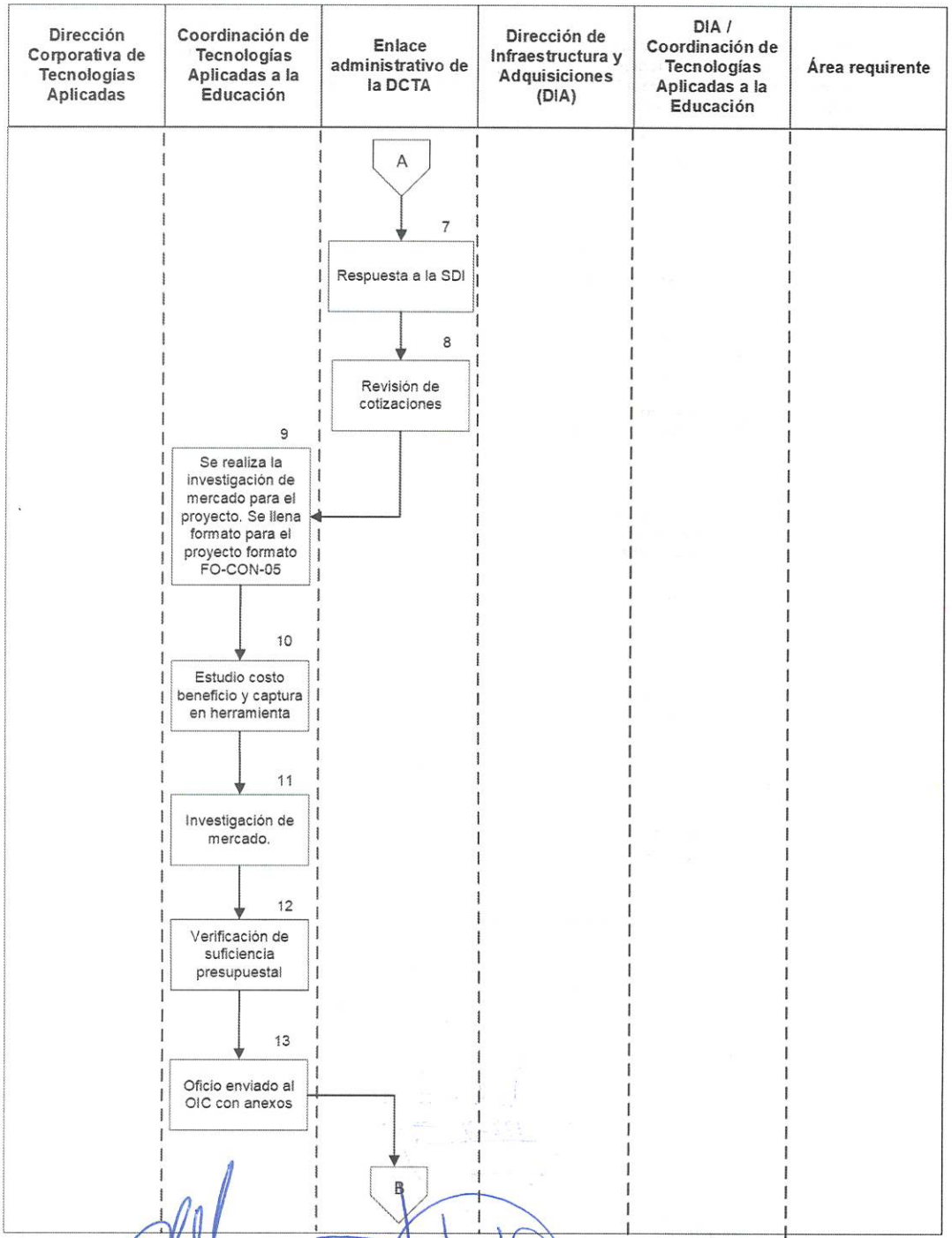
Oportunidades de Atención.
Respaldar la necesidad en materia de TIC que requiera un proceso de contratación, con la programación financiera definida en el Programa Anual de Trabajo de cada una de las Unidades Administrativas solicitantes.

Elaboró	Revisó	Autorizó
Christian Rodríguez Fuertes	Joel Olvera Velázquez	José Cartagena Subdias

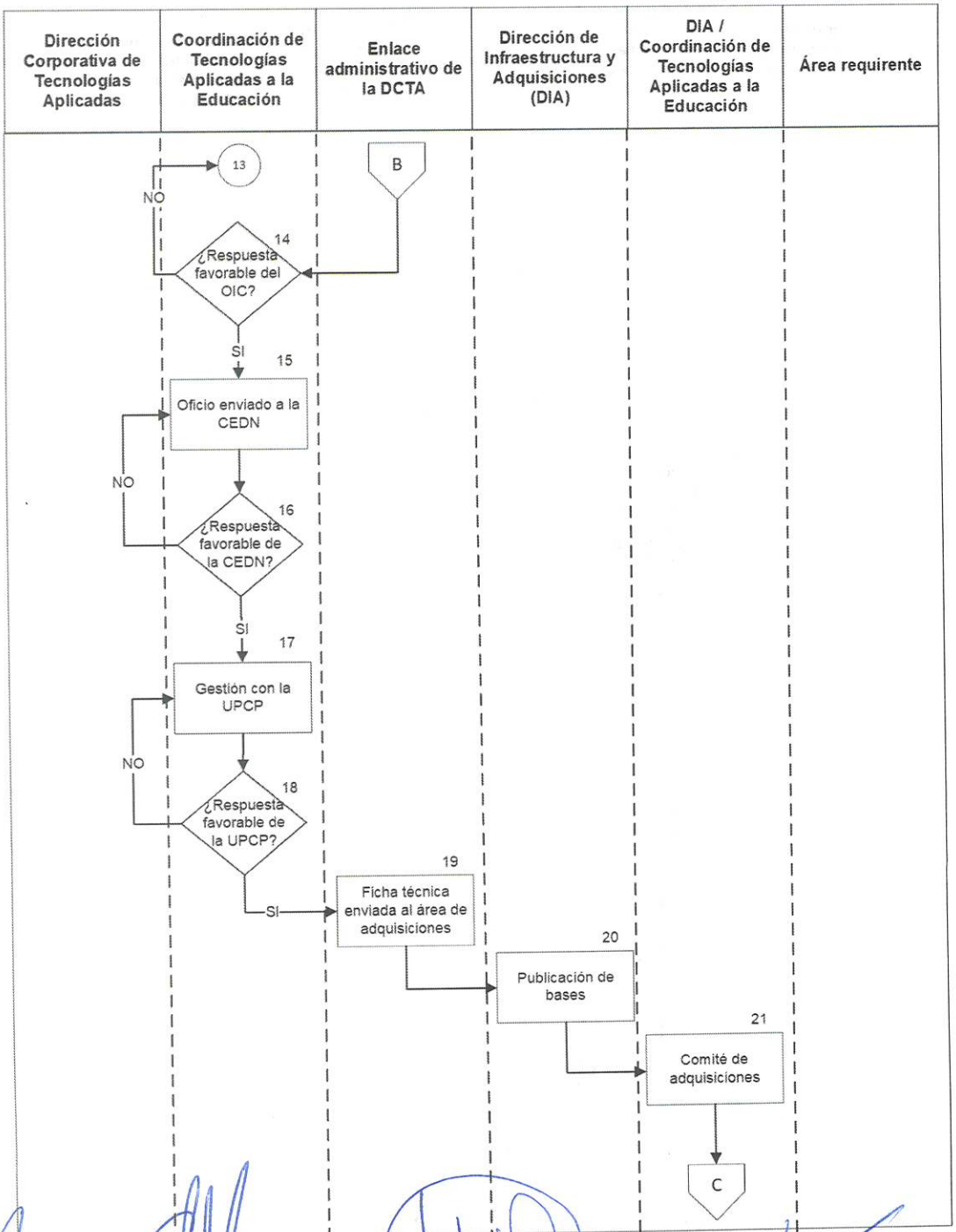
5.2.7 Diagrama de Flujo del Procedimiento Administración del presupuesto y contrataciones



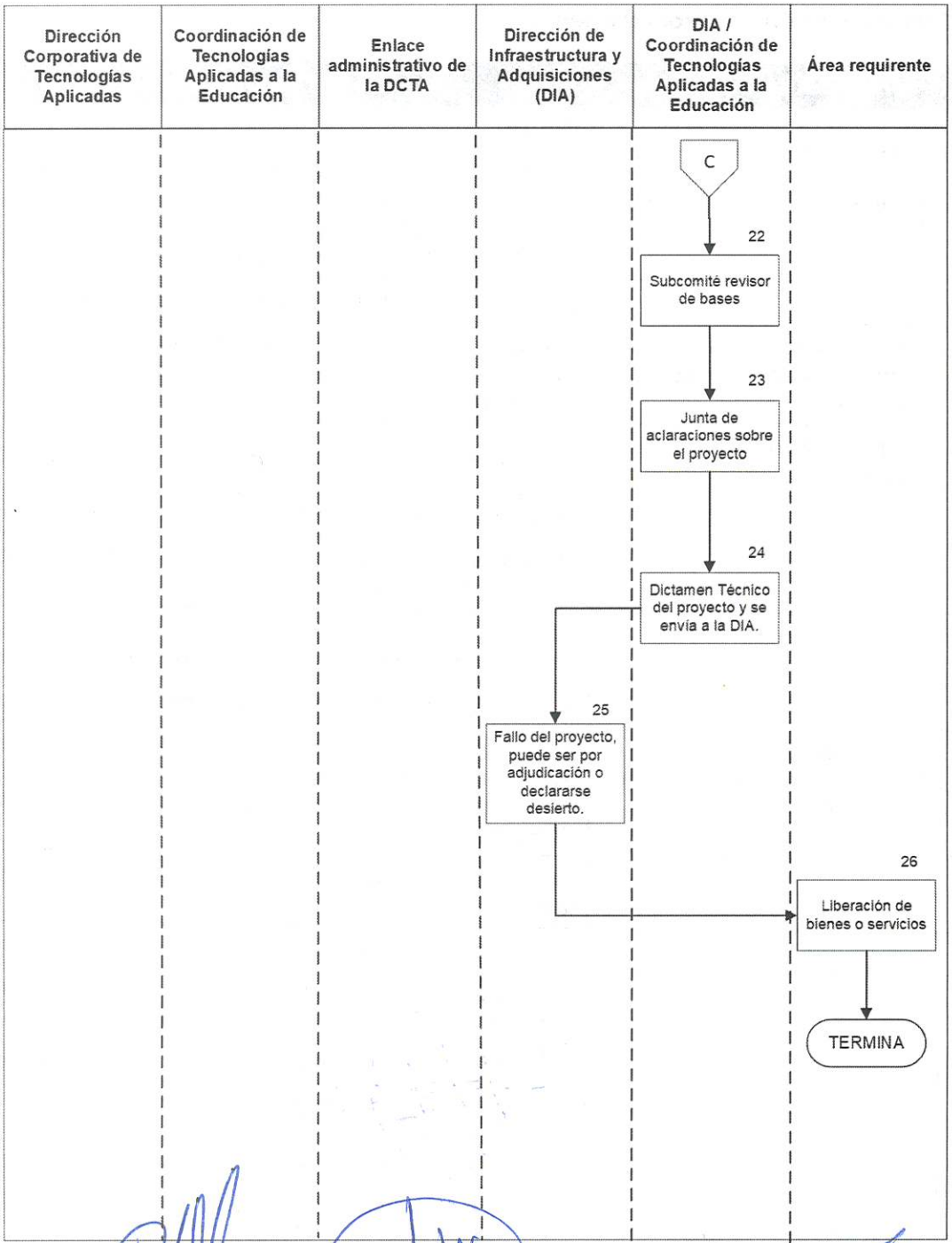
Elaboró	Revisó	Autorizó
Christian Rodríguez Fuertes	Joel Olvera Velázquez	José Cartagena Subdias



Elaboró	Revisó	Autorizó
Christian Rodríguez Fuertes	Joel Olvera Velázquez	José Cartagena Subdias



Elaboró	Revisó	Autorizó
Christian Rodríguez Fuertes	Joel Olvera Velázquez	José Cartagena Subdias



Elaboró	Revisó	Autorizó
Christian Rodríguez Fuertes	Joel Olvera Velázquez	José Cartagena Subdias

5.2.8 Descripción del Procedimiento

No.	Unidad Administrativa	Descripción de la actividad
		INICIA
1.	Enlace administrativo de la DCTA	Al anunciar el presupuesto asignado en el SIPAT, se verifica con el programa anual de trabajo, se hace análisis de que proyectos se dio presupuesto, en base a ello se solicita a la DAF tener en cuenta para futuros presupuesto.
2.		Se elabora la suficiencia presupuestal del proyecto y FO CON 3.
3.	Coordinación de Tecnologías Aplicadas a la Educación	A través de la Subcoordinación de Tendencias Tecnológicas Aplicadas a la Educación, se elabora el anexo técnico del proyecto
4.	Enlace administrativo de la DCTA	Se realiza la búsqueda de un ente público para el proyecto.
5.		Se realiza la búsqueda del contrato marco para el proyecto.
6.		Se elabora el formato SDI (FO-CON-4) del proyecto y se envía a los proveedores y/o a la Dirección de Infraestructura.
7.		Se obtiene la respuesta del formato SDI del proyecto. Propuesta técnica apegada a la SDI y propuesta económica.
8.		Se realiza la revisión de cotizaciones del proyecto.
9.	Coordinación de Tecnologías Aplicadas a la Educación	A través de la Subcoordinación de Tendencias Tecnológicas Aplicadas a la Educación, se realiza la investigación de mercado para el proyecto. Se llena formato para el proyecto formato FO-CON-05
10.		Se realiza el estudio costo beneficio del proyecto y se captura en la herramienta.
11.		Se realiza la investigación de mercado para el proyecto.
12.		De acuerdo a los resultados de la investigación de mercado, verificar que se cuenta con la suficiencia presupuestal.
13.		Se elabora y envía oficio al OIC con los anexos técnicos.
14.		¿Respuesta favorable del OIC sobre el proyecto? 1. Si, ir al punto 15 2. No, atender observaciones del OIC y regresar al punto 13.
15.		Se elabora y envía oficio sobre el proyecto a la CEDN

Elaboró	Revisó	Autorizó
Christian Rodríguez Fuertes	Joel Olvera Velázquez	José Cartagena Subdias

No.	Unidad Administrativa	Descripción de la actividad
16.		¿Respuesta favorable de la CEDN sobre el proyecto? 1. Si, ir al punto 17 2. No, atender observaciones del CEDN y regresar al punto 15
17.		Gestión del proyecto con la UPCP
18.		¿Respuesta favorable de la UPCP sobre el proyecto? 3. Si, ir al punto 19 4. No, atender observaciones de la UPCP y regresar al punto 17
19.	Enlace administrativo de la DCTA	La ficha técnica del proyecto se envía al área de adquisiciones
20.	Dirección de Infraestructura y Adquisiciones	Se realiza la publicación de las bases del proyecto
21.	Dirección de Infraestructura y Adquisiciones / Coordinación de Tecnologías Aplicadas a la Educación	Se realiza la gestión con el comité de adquisiciones del proyecto
22.		El subcomité de adquisiciones revisa las bases del proyecto
23.		Se realiza la junta de aclaraciones sobre el proyecto
24.		Se realiza el dictamen técnico del proyecto y se envía a la DIA.
25.	Dirección de Infraestructura y Adquisiciones	Fallo del proyecto, puede ser por adjudicación o declararse desierto.
26.	Área requirente	Se realiza la liberación de los bienes o servicios del proyecto (fecha del acuse del recibido por la Coordinación de Administración y Servicios.)
		TERMINA

Total de actividades: 26
Duración total estimada: 255 días

Elaboró	Revisó	Autorizó
Christian Rodríguez Fuertes	Joel Olvera Velázquez	José Cartagena Subdias

5.3 Administración de la configuración

Historial de Cambios.

Revisión número: 01 Fecha de aprobación: 26 de septiembre de 2022

Descripción y motivo del cambio.

A partir de la derogación del Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información se actualizan formatos con fundamento en el Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal

Los formatos actualizados son el ACNF-F01 Cobertura y Alcance de la Administración de la Configuración, así como el ACNF-F02 Definición de la Estructura del Repositorio de la Configuración.

El procedimiento para la integración del inventario de bienes y servicios de TIC desplegados en la infraestructura tecnológica, con la finalidad de facilitar su acceso a los involucrados en los procesos de la DCTA y proporcionar la información requerida para el Inventario de bienes y servicios de TIC de la APF, se detona desde la Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar, a través de una solicitud expresa a los titulares de la Coordinación de Comunicaciones y de la Coordinación de Tecnologías Aplicadas a la Educación.

Tras la solicitud a los titulares de las coordinaciones, se realiza el barrido y actualización del repositorio con base en las altas, bajas y modificaciones en el uso y disponibilidad de la infraestructura en materia de hardware y software considerando lo siguiente:

Hardware se refiere a los equipos de redes y telecomunicaciones, a los servidores asociados al alojamiento de los sistemas académico-escolar, de gestión administrativa, portal institucional y directorio activo; El equipo de cómputo para uso administrativo.

Software considera los sistemas Académico-Escolar y de gestión administrativa, al portal institucional, correo electrónico, sistemas operativos, motores de bases de datos, servidores Web, software de paquetería, aplicaciones de uso específico y otros servicios.

Elaboró	Revisó	Autorizó
Luis Alfonso Sosa Ortega	Eduardo Gómez Garduño	José Cartagena Subdias

5.3.1 Procedimiento.

Administración de la configuración

5.3.2 Objetivo del Procedimiento.

Establecer y actualizar un repositorio de configuraciones que comprenda el Inventario Institucional de bienes y servicios de TIC, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas de la DCTA, como elementos de configuración, con la finalidad de facilitar su acceso a los involucrados en los procesos de la DCTA, cuando éstos así lo requieran para la operación del proceso respectivo.

5.3.3 Responsables.

- Dirección Corporativa de Tecnologías Aplicadas (DCTA).
- Coordinación de Comunicaciones
- Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar
- Coordinación de Tecnologías Aplicadas a la Educación

Serán responsables de:

- La Dirección Corporativa de Tecnologías Aplicadas (DCTA) será responsable de dirigir y autorizar los elementos que contendrá el repositorio de configuraciones.
- La Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar será la responsable de mantener actualizada la información contenida en el repositorio de configuraciones y disponible para los servidores públicos de la DCTA involucrados en los diversos procesos.
- Las Coordinaciones serán las responsables de identificar, registrar, controlar y verificar los datos de los elementos de configuración, así como la información relacionada con los mismos.

5.3.4 Alcance.

La administración del repositorio de configuraciones, se formaliza con la integración del inventario de bienes y servicios de TIC y SI validado y autorizado, que cumplan con la definición de los datos de los elementos de configuración establecidos.

Elaboró	Revisó	Autorizó
Luis Alfonso Sosa Ortega	Eduardo Gómez Garduño	José Cartagena Subdias

5.3.5 Requisitos Generales de Operación del Procedimiento.

Identificar las soluciones tecnológicas y sus componentes, así como los diversos ambientes y arquitecturas tecnológicas de la UTIC, como elementos de configuración, para establecer la cobertura que tendrá el proceso, así como el alcance de la administración sobre los elementos de la configuración y sus componentes.

5.3.6 Identificación de Riesgos.

Descripción del Riesgo
Omisión del registro de alguna solución tecnológica y componentes que pudieran ser objeto de observación de auditoría.

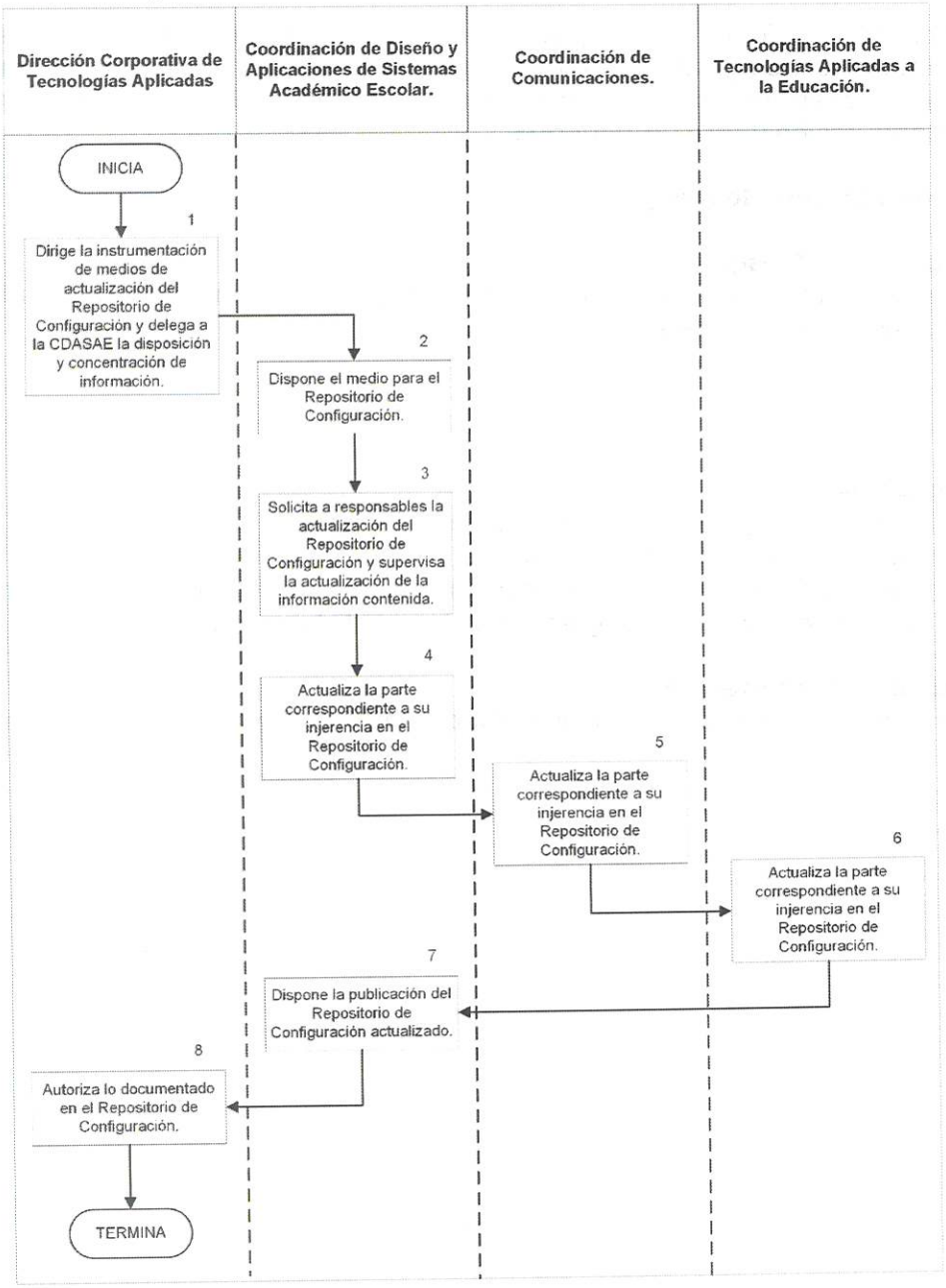
Tipo
Administrativo.

Responsables
- Dirección Corporativa de Tecnologías Aplicadas
- Coordinación de Comunicaciones
- Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar
- Coordinación de Tecnologías Aplicadas a la Educación

Oportunidades de Atención
Implementar acciones de control previendo la falta de registro de información.

Elaboró	Revisó	Autorizó
Luis Alfonso Sosa Ortega	Eduardo Gómez Garduño	José Cartagena Subdias

5.3.7 Diagrama de Flujo del Procedimiento Administración de la configuración.



Elaboró	Revisó	Autorizó
Luis Alfonso Sosa Ortega	Eduardo Gómez Garduño	José Cartagena Subdias

5.3.8 Descripción del Procedimiento

No.	Unidad Administrativa	Descripción de la actividad
		INICIA
1.	Dirección Corporativa de Tecnologías Aplicadas.	Dirige la instrumentación de medios de actualización del Repositorio de Configuración y delega a la CDASAE la disposición y concentración de información.
2.	Coordinación de Diseño y Aplicaciones de Sistemas Académico Escolar.	Dispone el medio para el Repositorio de Configuración generando los formatos Cobertura y Alcance de la Administración de la Configuración; Definición de la Estructura del Repositorio de la Configuración.
3.		Solicita a responsables la actualización del Repositorio de Configuración y supervisa la actualización de la información contenida.
4.		Actualiza la parte correspondiente a su injerencia en el Repositorio de Configuración.
5.	Coordinación de Comunicaciones.	Actualiza la parte correspondiente a su injerencia en el Repositorio de Configuración.
6.	Coordinación de Tecnologías Aplicadas a la Educación.	Actualiza la parte correspondiente a su injerencia en el Repositorio de Configuración.
7.	Coordinación de Diseño y Aplicaciones de Sistemas Académico Escolar.	Dispone la publicación del Repositorio de Configuración actualizado.
8.	Dirección Corporativa de Tecnologías Aplicadas.	Autoriza lo documentado en el Repositorio de Configuración.
		TERMINA

Total de actividades: 8
Duración total estimada: 255 días

Elaboró	Revisó	Autorizó
Luis Alfonso Sosa Ortega	Eduardo Gómez Garduño	José Cartagena Subdias

5.3.9 Formatos que intervienen en el Procedimiento

El proceso se implementa en 3 etapas

Etapa 1. Definición

1.- Se localizarán los elementos de configuración que serán administrados por el proceso con base a las necesidades y los recursos con los que cuenta la UTIC.

2.- Diseñar la estructura del repositorio de configuración (CMDB, Base de datos de la Configuración).

3.- Diseñar la estrategia a seguir para integrar los elementos de configuración en el repositorio.

4.- Identificar los elementos de configuración que servirán como línea base para la administración del registro en el repositorio de configuraciones.

Etapa 2. Ejecución

1.- Implementar las acciones de control para administrar el repositorio de configuraciones, considerando; el mantenimiento al modelo de datos, la definición y aplicación técnica para realizar modificaciones a los estados de los elementos de configuración y componentes, la incorporación de elementos de configuración o componentes para que se realice mediante cambios administrados, las relativas a la administración de perfiles de usuario.

2.- Desarrollo del sistema y el modelo de datos del repositorio de configuraciones, implantar catálogos de librerías para apoyo, establecer perfiles y permisos para el acceso a los usuarios y definir las acciones para el mantenimiento y actualización del repositorio

Etapa 3. Seguimiento

1.- Registrar las acciones autorizadas a fin de darles seguimiento, así como el registro de los resultados obtenidos.

Elaboró	Revisó	Autorizó
Luis Alfonso Sosa Ortega	Eduardo Gómez Garduño	José Cartagena Subdias

Formato: Cobertura y Alcance de la Administración de la Configuración ACNF F01
Clave: ACNF F01
Formulación a cargo de: Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: Vía electrónica a la DCTA de acuerdo a la actividad 1 del Procedimiento Administración de la configuración.

Campo	Descripción.
Objetivo.	Indicar el objetivo de llevar a cabo la administración de la configuración.
Descripción de la estrategia.	Describir la estrategia a seguir para alcanzar el objetivo de la administración de la configuración.
Elementos de la configuración.	Listar los elementos que se tomarán en cuenta para la definición de la configuración de cada uno.
Calendario.	Indicar el calendario que se define para la calendarización del respaldo del repositorio de configuraciones.
Cronograma.	Indicar el cronograma para la revisión al repositorio de configuraciones, indicando por cada elemento el Responsable de la revisión, Entregables y Periodo.
Fecha de elaboración.	Indicar la fecha de elaboración y/o actualización del formato.
Firmas y fechas de firma, revisión y autorización.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.

Elaboró	Revisó	Autorizó
Luis Alfonso Sosa Ortega	Eduardo Gómez Garduño	José Cartagena Subdias

Formato: Definición de la Estructura del Repositorio de la Configuración ACNF F02
Clave: ACNF F02
Formulación a cargo de: Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: Vía electrónica a la DCTA de acuerdo a la actividad 1 del Procedimiento Administración de la configuración.

Campo	Descripción.
Objetivo.	Definir el objetivo de la estructura del repositorio de la configuración.
Descripción.	Describir la estructura del repositorio de configuraciones de cada uno los elementos, indicando la categoría, tipo, nomenclatura, características que se consideren relevantes para su identificación: nombre, descripción, ubicación, línea base (fecha), modelo o versión, fecha última versión, sistema operativo, plataforma BD, Lenguaje de programación, servidor de aplicaciones, otros servicios, tipo de licenciamiento, estado, procedencia, nombre responsable, unidad administrativa responsable, marca, modelo, no. serie, capacidad en RAM, capacidad en disco duro, capacidad del procesador, cantidad, estado.
Atributos mínimos.	Condiciones mínimas para considerar la línea base para cada uno de los elementos.
Nomenclatura.	Indicar la descripción de la nomenclatura que funcionará como identificador único, indicando el número de factores que compone la nomenclatura.
Criterios técnicos.	Indicar los criterios técnicos que deben de considerarse para la modificación de los estados de los elementos de configuración.
Fecha de elaboración.	Indicar la fecha de elaboración y/o actualización del formato.
Firmas y fechas de firma, revisión y autorización.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.

Elaboró	Revisó	Autorizó
Luis Alfonso Sosa Ortega	Eduardo Gómez Garduño	José Cartagena Subdias

Formato: Repositorio de la Configuración Formato ACNF F03
Clave: ACNF F03
Formulación a cargo de: Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar
Medio de Elaboración: Computarizado
No. de Ejemplares: Original y Respaldo previo
Distribución: Vía electrónica a la DCTA de acuerdo a la actividad 1 del Procedimiento Administración de la configuración.

Campo	Descripción.
Elemento.	Por cada uno de los componentes identificados para conformar el repositorio de configuraciones.
Característica.	Listar las características para cada componente por el tipo de elemento.
Fecha de elaboración.	Indicar la fecha de elaboración y/o actualización del formato.
Firmas y fechas de firma, revisión y autorización.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.

Elaboró	Revisó	Autorizó
Luis Alfonso Sosa Ortega	Eduardo Gómez Garduño	José Cartagena Subdias

5.4 Administración de la seguridad de la información

Historial de Cambios.

Revisión número: 01 Fecha de aprobación: 26 de septiembre de 2022

Descripción y motivo del cambio.

Describir los cambios realizados considerando lo siguiente:

1. Derogación del Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información.
2. Publicación del Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.
3. Describir el procedimiento para establecer, operar y mantener un modelo de gobierno de seguridad de la información.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

5.4.1 Procedimiento.

Administración de la seguridad de la información.

5.4.2 Objetivo del Procedimiento.

Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional u otras instituciones de la APF.

5.4.3 Responsables.

- Dirección Corporativa de Tecnologías Aplicadas (DCTA).
- Coordinación de Comunicaciones
- Coordinación de Diseño y Aplicación de Sistemas Académicos Escolar
- Coordinación de Tecnologías Aplicadas a la Educación

Serán responsables de:

- La Dirección Corporativa de Tecnologías Aplicadas vigilará los mecanismos establecidos y el desempeño del SGSI, a fin de prever desviaciones y mantener una mejora continua.
- La Coordinación de Tecnologías Aplicadas a la Educación, efectuará la identificación de Infraestructuras de información esenciales y, en su caso, críticas, así como de activos clave de la Institución, y elaborar el catálogo respectivo; establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos; establecer mecanismos para la respuesta inmediata a incidentes a la seguridad de la información.
- Cada una de las coordinaciones deberán asegurarse de que se integren al SGSI, controles de seguridad en los equipos del ambiente operativo y de comunicaciones de la Institución, para efectuar la revisión correspondiente con la finalidad de identificar intentos de ataques o de explotación de vulnerabilidades.

5.4.4 Alcance.

La administración de la seguridad de la información se formaliza con la definición de:

- Integración y operación del grupo estratégico de seguridad de la información.
- Catálogo de infraestructuras de información esenciales y/o críticas.
- Resultados del análisis de riesgos.
- Definición del SGSI.
- Directriz rectora de respuesta a incidentes.

5.4.5 Requisitos Generales de Operación del Procedimiento.

Definir por parte del responsable de la seguridad de la información en la institución:

- Grupo estratégico de seguridad de la información o GESI.
- Equipo de respuesta a incidentes de seguridad o ERISC

5.4.6 Identificación de Riesgos.

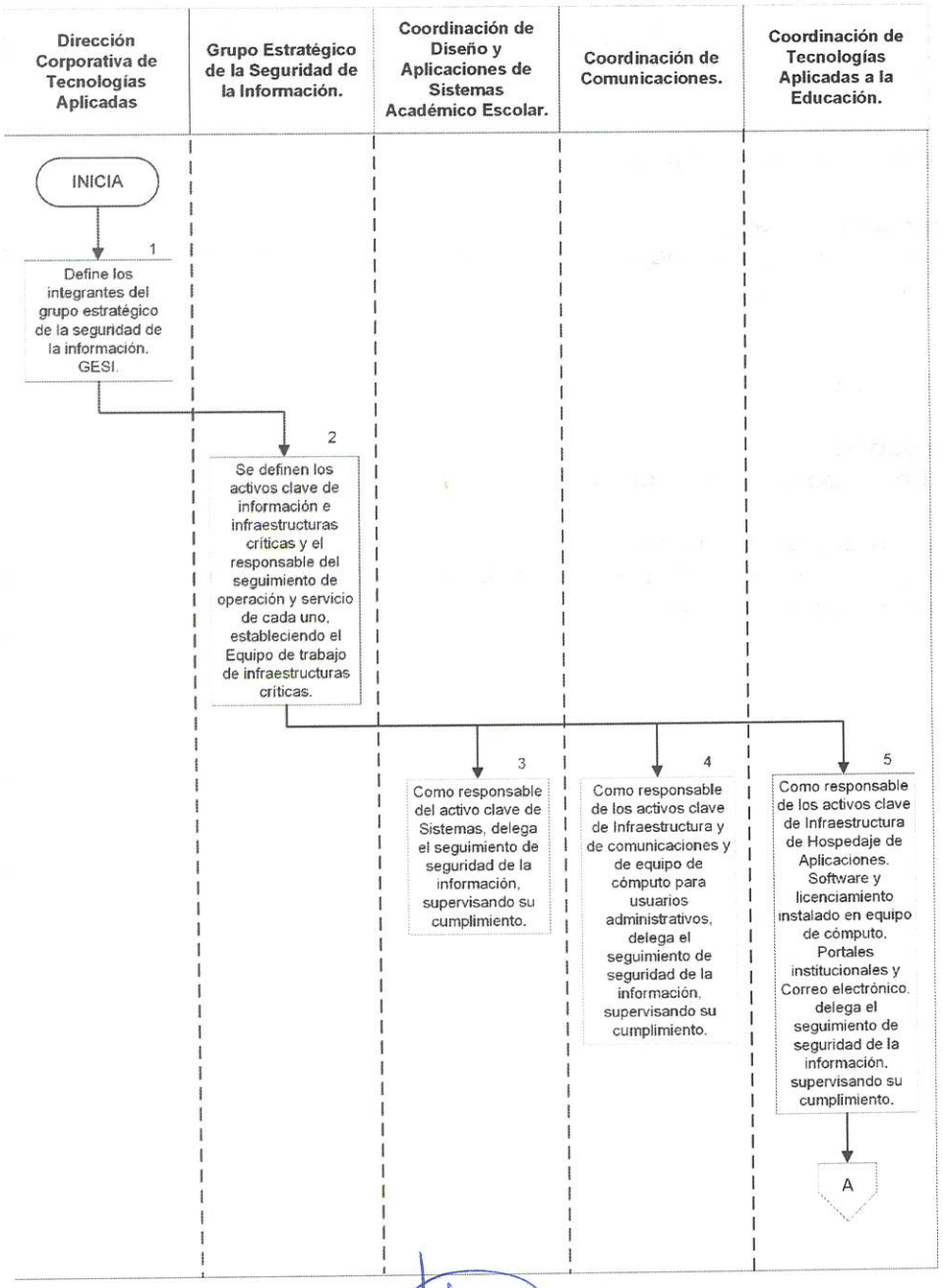
Descripción del Riesgo.
Falta del personal capacitado o con los conocimientos suficientes y pertinentes en un activo de información clave.

Tipo.
Administrativo.

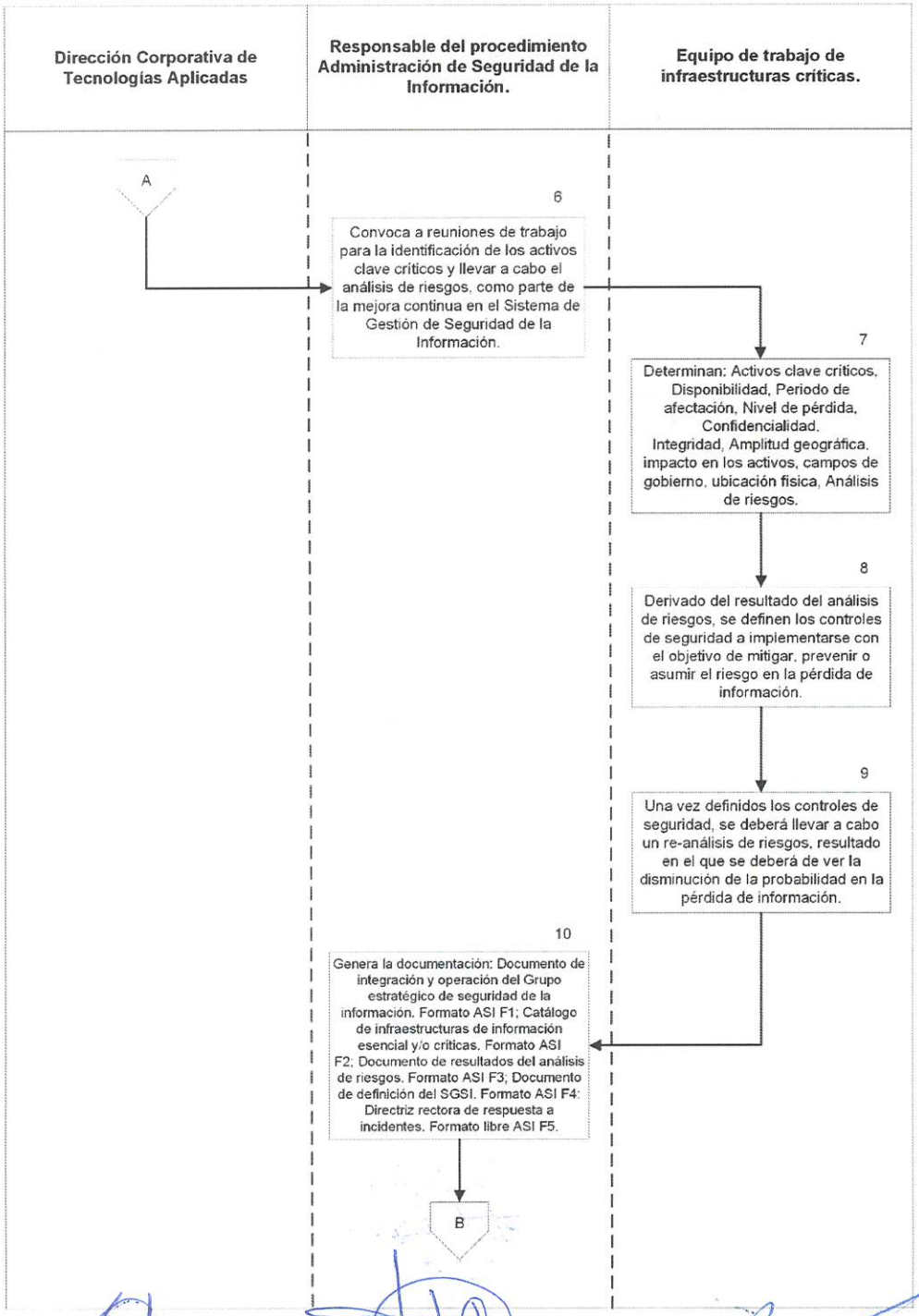
Responsables.
Dirección Corporativa de Tecnologías Aplicadas

Oportunidades de Atención.
Fortalecer los conocimientos tecnológicos de los colaboradores en cada una de las áreas del activo de información clave.

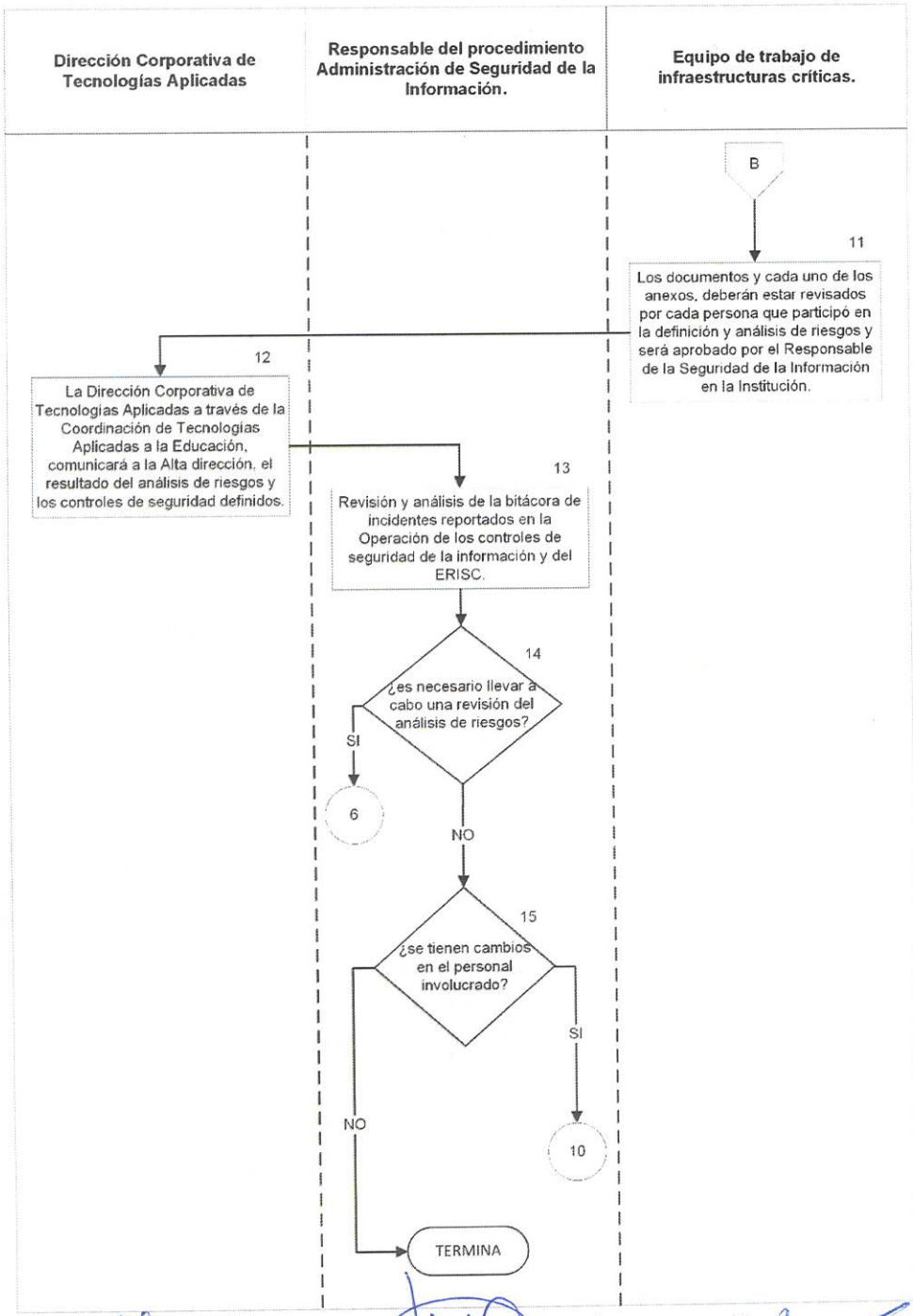
5.4.7 Diagrama de Flujo del Procedimiento Administración de la seguridad de la información.



Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias



Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias



Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

5.4.8 Descripción del Procedimiento.

No.	Unidad Administrativa	Descripción de la actividad
		INICIA
1.	Dirección Corporativa de Tecnologías Aplicadas.	Define los integrantes del grupo estratégico de la seguridad de la información, GESI.
2.	Grupo Estratégico de la Seguridad de la Información.	El Grupo conformado por el Titular de la Dirección Corporativa de Tecnologías Aplicadas, los Coordinadores y un suplente, definen los activos clave de información e infraestructuras críticas y el responsable del seguimiento de operación y servicio de cada uno, estableciendo el Equipo de trabajo de infraestructuras críticas.
3.	Coordinación de Diseño y Aplicaciones de Sistemas Académico Escolar.	Como responsable del activo clave de Sistemas, delega el seguimiento de seguridad de la información, supervisando su cumplimiento.
4.	Coordinación de Comunicaciones.	Como responsable de los activos clave de Infraestructura y de comunicaciones y de equipo de cómputo para usuarios administrativos, delega el seguimiento de seguridad de la información, supervisando su cumplimiento.
5.	Coordinación de Tecnologías Aplicadas a la Educación.	Como responsable de los activos clave de Infraestructura de Hospedaje de Aplicaciones, Software y licenciamiento instalado en equipo de cómputo, Portales institucionales y Correo electrónico, delega el seguimiento de seguridad de la información, supervisando su cumplimiento.
6.	Responsable del procedimiento Administración de Seguridad de la Información.	Convoca a reuniones de trabajo para la identificación de los activos clave críticos y llevar a cabo el análisis de riesgos, como parte de la mejora continua en el Sistema de Gestión de Seguridad de la Información.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

No.	Unidad Administrativa	Descripción de la actividad
7.	Equipo de trabajo de infraestructuras críticas.	Con participación de los responsables de cada activo clave, se determina: • Activos clave críticos. • Disponibilidad, • Periodo de afectación • Nivel de pérdida • Confidencialidad, • Integridad • Amplitud geográfica, impacto en los activos, campos de gobierno, ubicación física • Análisis de riesgos.
8.		Derivado del resultado del análisis de riesgos, se definen los controles de seguridad a implementarse con el objetivo de mitigar, prevenir o asumir el riesgo en la pérdida de información, generando la Tabla de Análisis de Costo - Beneficio
9.		Una vez definidos los controles de seguridad, se deberá llevar a cabo un re-análisis de riesgos, resultado en el que se deberá de ver la disminución de la probabilidad en la pérdida de información.
10.	Responsable del procedimiento Administración de Seguridad de la Información.	Genera la documentación en la que se plasme la definición de: • Documento de integración y operación del Grupo estratégico de seguridad de la información. Formato ASI F1 • Catálogo de infraestructuras de información esencial y/o críticas. Formato ASI F2 • Documento de resultados del análisis de riesgos. Formato ASI F3 • Documento de definición del SGSI. Formato ASI F4 • Directriz rectora de respuesta a incidentes. Formato libre ASI F5
11.		Los documentos y cada uno de los anexos, deberán estar revisados por cada integrante del Equipo de trabajo de infraestructuras críticas, que participó en la definición y análisis de riesgos y será aprobado por el Responsable de la Seguridad de la Información en la Institución.
12.	Dirección Corporativa de Tecnologías Aplicadas.	La Dirección Corporativa de Tecnologías Aplicadas a través de la Coordinación de Tecnologías Aplicadas a la Educación, comunicará a la Alta dirección, el resultado del análisis de riesgos y los controles de seguridad definidos.

No.	Unidad Administrativa	Descripción de la actividad
13.	Responsable del procedimiento Administración de Seguridad de la Información.	Revisión y análisis de la bitácora de incidentes reportados en la Operación de los controles de seguridad de la información y del ERISC.
14.		¿es necesario llevar a cabo una revisión del análisis de riesgos? Si: ir a la actividad 6 No: ir a la actividad 15
15.		¿se tienen cambios en el personal involucrado? Si: ir a la actividad 10 No: fin del procedimiento.
		TERMINA

Total de actividades: 15 **Duración total estimada:** 255 días

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

5.4.9 Formatos que intervienen en el Procedimiento

Formato. Documento de integración y operación del Grupo estratégico de seguridad de la información. Formato ASI F1
Clave: ASI F1
Formulación a cargo de: Responsable del Procedimiento de Administración de Seguridad de la Información.
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: El Responsable del Procedimiento de Administración de Seguridad de la Información proporcionará vía electrónica a los integrantes del Grupo Estratégico de Seguridad de la Información para su revisión y aprobación, de acuerdo a la actividad 10 del procedimiento Administración de la seguridad de la información.

5.4.9.1 Instructivo de llenado del Formato
ASI F1.

Campo	Descripción.
Objetivos.	Listar los objetivos que cumple la conformación del Grupo estratégico de seguridad de la información.
Roles.	Listar los roles que participarán en la conformación del Grupo, así como la descripción del rol y los requerimientos en conocimientos y/o habilidades que se solicita tenga el servidor público.
Responsabilidades.	Listar las responsabilidades que tendrá cada uno de los roles.
Miembros del Grupo.	Listar los integrantes que conformarán el Grupo, identificando Nombre completo, Cargo, Rol y suplente.
Programación de sesiones ordinarias.	Especificar la periodicidad para llevar a cabo las sesiones de trabajo, identificando número de sesiones máximas o mínimas, tiempo para convocar, requisitos para declarar quorum y cancelación o reprogramación de la sesión.
Programación de sesiones extraordinarias.	Especificar la periodicidad para llevar a cabo las sesiones de trabajo, identificando número de sesiones máximas o mínimas, tiempo para convocar, requisitos para declarar quorum y cancelación o reprogramación de la sesión.
Descripción de la forma de operación del Grupo.	Describir las técnicas a aplicar para las sesiones, normas y/o recomendaciones que se deban de aplicar para la administración y operación del Grupo.
Otros aspectos relevantes para la operación del Grupo.	Describir o especificar normas y/o recomendaciones que se deban de llevar a cabo.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Firmas y fechas de firma, revisión y autorización	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Formato. Catálogo de infraestructuras de información esencial y/o críticas. Formato ASI F2
Clave: ASI F2
Formulación a cargo de: Responsable del Procedimiento de Administración de Seguridad de la Información.
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: El Responsable del Procedimiento de Administración de Seguridad de la Información proporcionará vía electrónica a los integrantes del Grupo Estratégico de Seguridad de la Información para su revisión y aprobación, de acuerdo a la actividad 10 del procedimiento Administración de la seguridad de la información.

5.4.9.2 Instructivo de llenado del Formato
ASI F2.

Campo	Descripción.
Objetivos.	Establecer con los servidores públicos que administren Activos de Información, los objetivos y mecanismos para garantizar la protección de las infraestructuras críticas que éstos tengan bajo su responsabilidad.
Activos clave definidos.	Especificar el nombre del Activo clave, descripción y el responsable del seguimiento de la operación para la seguridad de la información.
Valoración de las matrices de infraestructuras esenciales de información y, en su caso, críticas, así como de activos clave	Para cada uno de los activo clave definidos, determinar: la valoración de la pérdida de información tomando en cuenta la confidencialidad, integridad y disponibilidad de la misma.
Parámetros de influencia para determinar una infraestructura esencial de información y/o crítica	Identificar para cada uno de los activo clave, la influencia en Amplitud geográfica, Período de afectación, Cantidad de IC afectadas y Campos de gobierno.
Elaboración de matrices	En esta sección se efectúa la construcción de las matrices que integran los parámetros de influencia de una infraestructura esencial de información y/o crítica. Matrix de Impacto: número de activos afectados, Matriz de interdependencia: niveles de gobierno afectados y de acuerdo a estos dos valores, determinar la Matriz de Criticidad.

Campo	Descripción.
Identificación de las infraestructuras de información esenciales y/o críticas:	De acuerdo a la obtención de la Matriz de Criticidad, se identifican aquellos activos clave que son críticos para la Institución.
Elaboración del catálogo de infraestructuras de información esenciales y/o críticas	Para cada una de los activos clave identificados como infraestructuras críticas, especificar: Identificador / clave, nombre, descripción, sector / subsector, institución y ubicación física y, si es de impacto en la Información de Seguridad Nacional.
Firmas y fechas de firma, revisión y autorización	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Formato: Documento de resultados del análisis de riesgos. Formato ASI F3
Clave: ASI F3
Formulación a cargo de: Responsable del Procedimiento de Administración de Seguridad de la Información.
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: El Responsable del Procedimiento de Administración de Seguridad de la Información proporcionará vía electrónica a los integrantes del Grupo Estratégico de Seguridad de la Información para su revisión y aprobación, de acuerdo a la actividad 10 del procedimiento Administración de la seguridad de la información.

5.4.9.3 Instructivo de llenado del Formato
ASI F3

Campo	Descripción.
Objetivo del análisis de riesgos.	Establecer el objetivo del proceso de análisis, impacto y beneficios.
Lista de controles recomendados.	Generar la Tabla 1 con la relación de los controles recomendados para su implantación que apliquen para la prevención, mitigación de riesgos en la pérdida de información, estableciendo la Prioridad, Control recomendado, Amenazas a mitigar, Activos a proteger, Riesgos residuales, Requerimientos especiales y la Inversión requerida.
Riesgos aceptados.	Generar la Tabla 2 con la relación de los riesgos aceptados que fueron determinados durante el análisis, definiendo la Secuencia, Amenazas, Activos de información, Riesgos y Observaciones.
Firmas y fechas de firma, revisión y autorización de la sección de Controles definidos.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.
Objetivo y alcance de la directriz de administración de riesgos.	Establecer el objetivo y el alcance en la gestión de riesgos en la pérdida de información.
Justificación.	Indicar la justificación de establecer la gestión de la administración de riesgos.
Requerimientos regulatorios.	Listar los requerimientos, normas, estándares que respalde o

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Elementos para la administración de riesgos	Listar los elementos, el Grupo de riesgos sobre los que incide y el Escenario en el que podrá presentarse el riesgo: • Umbrales de tolerancia al riesgo. • Mecanismos que se utilizarán para medir la correcta administración de riesgos. • Estrategias de mitigación. • Periodicidad con la que se informará a los involucrados en el proceso.
Directrices de administración de riesgos	Listar las directrices para su administración, estableciendo la Necesidad, Directriz de Administración de riesgos, Escenario y el Impacto: • Mantener la confidencialidad, integridad y disponibilidad de la información mediante el uso adecuado de la Seguridad Informática, reaccionando de forma inmediata y oportuna a los incidentes de seguridad de la Institución. • Establecer los mecanismos que permitan la administración de la Seguridad de la información de la Institución, disminuyendo el impacto de eventos adversos que comprometan la seguridad de la Información. • Implantar y operar los controles de seguridad de la información de acuerdo al Programa de implantación del SGSI, así como los correspondientes a la capacidad de respuesta a Incidentes. • Creación de políticas y procedimientos que permitan establecer la Seguridad de la Información e integrarlas en el SGSI implementado.
Firmas y fechas de firma, revisión y autorización de la sección de Directrices de administración de riesgos.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.
Objetivo y alcance del Análisis de costo-beneficio de controles de seguridad.	Establecer el objetivo y el alcance de la evaluación derivado del análisis del costo-beneficio.
Análisis de Costo – Beneficio.	Generar la Tabla 3 con el Análisis de Costo – Beneficio, de acuerdo a la Instrucción de trabajo para tal efecto.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Tabla de Reproceso de análisis Costo – Beneficio.	Derivado del resultado en la Instrucción de trabajo, generar la Tabla 4 con el resultado del reanálisis de riesgos, indicando la siguiente información: Código escenario; Prioridad original; Riesgo residual; Nueva prioridad; Nuevos controles presupuestos.
Firmas y fechas de firma, revisión y autorización de la sección de Análisis de costo-beneficio de controles de seguridad.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.
Declaraciones de aplicabilidad.	Identificar de la Declaración de aplicabilidad, estableciéndolo con la clave SGSI-CONALEP-001:AAAA. En donde AAAA será el año de la determinación de Análisis de riesgos.
Análisis Determinación de Riesgos.	Generar la Tabla 5 con el análisis en la determinación de riesgos, que contendrá la siguiente información: número de riesgo, amenaza, agente de amenaza, activos clave involucrados, Existencia de un agente amenaza desde la perspectiva de un activo de información particular "e" (existir), Interés del agente amenaza para atacar al activo de información "i" (querer), Capacidad del agente amenaza para atacar al activo de información "c" (poder), Vulnerabilidad del activo de información "v", Existencia del agente amenaza "P" =(e+i+c+v)/4, Nivel de impacto humano "ih", Nivel de impacto material "im", Nivel de impacto financiero "if", Nivel de impacto operativo "io", Nivel de impacto en la imagen de la Institución "ii", Impacto "I" (valor más alto que se haya obtenido de los niveles de impacto), Nivel de Riesgo determinado por el producto del valor de la Existencia del agente de amenaza por el Impacto en materializarse R=PI.
Controles implantados.	Generar la tabla 6 con la información del nombre del control; responsable para su implantación (puede aplicar por activo); descripción del control, tipo de control: prevención, mitigación; frecuencia de aplicación y justificación de su implantación.
Controles a implantar para la mitigación del riesgo.	Listar los controles que se identifican como pendientes para su implementación, indicando la siguiente información: nombre del control; responsable para su implantación (puede aplicar por activo); descripción del control, tipo de control: prevención, mitigación; frecuencia de aplicación y justificación de su implantación.
Documentación de soporte de las Declaraciones de aplicabilidad.	Listar los anexos que soporta el análisis de los riesgos y los controles propuestos para la contención de información.

Campo	Descripción.
5. Programa de mitigación de riesgos.	Especificar la clave del programa que identifica la implementación de los controles de seguridad: CONALEP-DCTA-NNN Donde NNN es el número de programa.
Número de riesgo y descripción.	Esta información, deberá ser de acuerdo a lo plasmado en la Tabla 5 Análisis Determinación de Riesgos.
Impacto.	Indicar la afectación de la pérdida de información: Local, Nacional, Mundial.
Controles asociados.	Generar la Tabla 7 Información de Controles, misma que contendrá la información: nombre del control; responsable para su implantación (puede aplicar por activo); descripción del control, tipo de control: prevención, mitigación; frecuencia de aplicación y justificación de su implantación.
Fecha de implementación.	Indicar por cada control la fecha compromiso para su implantación.
Responsable de la implantación.	Esta información se encuentra definida en la Tabla 7 Información de Controles, por lo que se puede hacer referencia a dicho anexo.
Responsable de verificar el cumplimiento.	Responsable de la Operación de los controles de seguridad de la información y del ERISC.
Actividades a realizar.	Esta información se encuentra definida en la Tabla 7 Información de Controles, por lo que se puede hacer referencia a dicho anexo.
Firmas y fechas de firma, revisión y autorización de la sección Programa de mitigación de riesgos.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.
6. Programa de contingencia de riesgos – Objetivo.	Indicar el objetivo del programa para la contingencia de riesgos.
Eventos generadores.	Indicar los eventos que pueden propiciar el despliegue del Programa de Contingencia y las Acciones o mecanismos de activación del programa de contingencia.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Definición del Programa de contingencia y pruebas de viabilidad.	Elaborar la matriz de pruebas que aplicará para todos los riesgos identificados, indicando el número de actividad, descripción y responsable. Precisar las actividades que se deberán tomar en cuenta para el caso de suceder el evento en horario no laborable o laborable, procedimiento de respaldo / acciones de respaldo, configuraciones de infraestructura de comunicaciones, para equipos de cómputo, procedimiento para la operación temporal del servicio, procedimiento para la recuperación del servicio, tiempos de ejecución, requerimientos mínimos para mantener un nivel adecuado de operación y de niveles de servicio con recursos disminuidos, activos clave identificados como críticos, Instalaciones alternativas, proveedores alternativos para recursos críticos y demás punto que pueda ser referente para al plan de contingencia.
Definición de la estructura del equipo de respuesta a la contingencia por el riesgo.	Para cada uno de los riesgos identificados, establecer la estructura del equipo de respuesta a la contingencia por el riesgo, indicando Áreas participantes y los Responsables del seguimiento y aseguramiento de la ejecución del Programa de contingencia.
Responsabilidades de cada integrante.	Indicar para cada uno de los riesgos identificados, las responsabilidades de cada integrante.
Aseguramiento de respuesta a la contingencia.	De acuerdo a los riesgos identificados, describir cómo es que se asegura la respuesta de contingencia.
Control de versiones del Programa de contingencia.	Indicar la cronología de las versiones en la actualización del Programa de contingencia, que se ha actualizado derivado de la mejora continua, indicando Fecha de la revisión / modificación, Versión, Sección modificada, Descripción del cambio, Nombre y cargo de quien realizó el cambio y Nombre y cargo de quien autorizó y validó la nueva versión.
Evaluación preliminar del daño.	De acuerdo a los riesgos identificados, describir los diferentes niveles de severidad (Interrupción, Contingencia, Desastre), indicando Nivel de severidad, Descripción y Ejemplos.
Informar a los usuarios afectados por la contingencia.	Describir el procedimiento a seguir para informar a los usuarios afectados por la contingencia.
Procedimiento de respuesta.	Describir el procedimiento a seguir para proceder con la respuesta describiendo las medidas técnicas, organizativas y humanas a realizar para la solución del incidente de manera pronta y eficiente: apartado Definición del Programa de contingencia y prueba de viabilidad.
Ejecución.	Describir las tareas necesarias a realizar por cada una de las áreas involucradas para la solución de la contingencia: apartado Definición del Programa de contingencia y prueba de viabilidad.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Evaluación.	Describir la forma en que se evaluará el Programa de contingencia tomando en cuenta el análisis de los resultados de la aplicación.
Lista de contactos externos.	Indicar el Nombre de la empresa o área involucrada en el Programa de contingencia y que sea externa a CONALEP, personal de contacto y los medios de contacto.
Firmas y fechas de firma, revisión y autorización de la sección Programa de contingencia de riesgos.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.
7. Programa de implantación para el manejo de riesgos.	Indicar la clave de Identificación del Programa, Número de Riesgo y Descripción de acuerdo a la Tabla 5 Análisis Determinación de Riesgos, por lo que se puede hacer referencia a dicho anexo.
Impacto.	Indicar la afectación de la pérdida de información: Local, Nacional, Mundial.
Controles asociados.	Generar la Tabla 7 Información de Controles, misma que contendrá la información: nombre del control; responsable para su implantación (puede aplicar por activo); descripción del control, tipo de control: prevención, mitigación; frecuencia de aplicación y justificación de su implantación.
Fecha de implementación.	Indicar por cada control la fecha compromiso para su implantación.
Responsable de la implantación.	Esta información se encuentra definida en la Tabla 7 Información de Controles, por lo que se puede hacer referencia a dicho anexo.
Responsable de verificar el cumplimiento.	Responsable de la Operación de los controles de seguridad de la información y del ERISC.
Actividades a realizar.	Esta información se encuentra definida en la Tabla 7 Información de Controles, por lo que se puede hacer referencia a dicho anexo.
Firmas y fechas de firma, revisión y autorización de la sección Programa de implantación para el manejo de riesgos.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.
8. Lista de amenazas a activos de información.	Establecer el catálogo de amenazas base mediante el cual se hará el análisis de riesgos, indicando Número referencia, Amenaza y Agente amenaza.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
9. Guía de identificación y evaluación de escenarios de riesgo.	Indicar el objetivo y el alcance de la guía para la identificación y evaluación de escenarios de riesgo.
Tabla Nivel de impacto	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar el Nivel de impacto aplicar los siguientes parámetros: Valor Impacto 100 Alto 50 Medio 10 Bajo
Tabla Existencia del agente amenaza para el cálculo de P.	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar la Existencia del agente amenaza aplicar los siguientes parámetros: Valor Probabilidad de existencia del agente amenaza 0.9 Es casi seguro que existe 0.7 Es muy posible que exista 0.5 Es probable que exista 0.3 Es poco probable que exista 0.1 Es casi imposible que exista
Tabla Niveles de Interés del agente amenaza para el cálculo de P.	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar los Niveles de Interés del agente amenaza aplicar los siguientes parámetros: Valor Nivel de interés del agente amenaza 0.9 El interés es incontrolable 0.7 Se genera mucho interés 0.5 Se genera regular interés 0.3 Se genera poco interés 0.1 Casi no se genera interés
Tabla Capacidad del agente amenaza para el cálculo de P.	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar la Capacidad del agente amenaza aplicar los siguientes parámetros: Valor Nivel de capacidad del agente amenaza 0.9 Los recursos son superiores 0.7 Cuenta con muchos recursos 0.5 Los recursos son regulares 0.3 Cuenta con muy pocos recursos 0.1 Los recursos son casi nulos

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Tabla Vulnerabilidad del Activo de información para el cálculo de P.	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar la Vulnerabilidad del Activo de información del agente amenaza aplicar los siguientes parámetros: Valor Vulnerabilidad del activo de información 0.9 Sin ningún tipo de protección 0.7 Muy poca protección 0.5 Medianamente protegido 0.3 Protección normal 0.1 Protección reforzada
Probabilidad de ocurrencia.	Con base en lo anterior, la fórmula para obtener la Probabilidad de ocurrencia, se establece como: P=(e+i+c+v)/4 para aquellos casos en que participe el elemento humano como agente perpetrador. En otros casos no se considera el interés (i), al tratarse de amenazas naturales (medio ambiente), o materiales (incendio), por lo que la fórmula a emplearse se reduce a la siguiente: P= (e+c+v)/3 Valor Probabilidad de ocurrencia de la amenaza Homologación al Manual de Control Interno 0.9 Alta 6-10 0.5 Media 2-5 0.1 Baja 1
Nivel de impacto humano ih	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar el Nivel de impacto humano con la pérdida de información en el agente amenaza aplicar los siguientes parámetros: Valor Impacto Humano 10 Desastroso Muertes 8 Gran impacto Heridos 6 Regular impacto Lesiones que producen una incapacidad 4 Mínimo impacto Lesiones leves 2 Insignificante Sin lesiones
Nivel de impacto material im	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar el Nivel de impacto material con la pérdida de información en el agente amenaza aplicar los siguientes parámetros: Valor Impacto Material 10 Desastroso Pérdidas graves no recuperables 8 Gran impacto Pérdidas graves recuperables a largo plazo 6 Regular impacto Pérdidas leves no recuperables 4 Mínimo impacto Pérdidas leves recuperables 2 Insignificante Sin pérdidas materiales

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Nivel de impacto financiero if	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar el Nivel de impacto financiero con la pérdida de información en el agente amenaza aplicar los siguientes parámetros: Valor Impacto Financiero 10 Desastroso Más de $1,000,000.00 8 Gran impacto Entre $100,000.00 y $1,000,000.00 6 Regular impacto Entre $50,000.00 y $100,000.00 4 Mínimo impacto Entre $10,000.00 y $50,000.00 2 Insignificante Menor de $10,000.00
Nivel de impacto operativo io	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar el Nivel de impacto operativo con la pérdida de información en el agente amenaza aplicar los siguientes parámetros: Valor Impacto Operativo 10 Desastroso Afectación de procesos críticos que no pueden restablecerse en menos de dos días 8 Gran impacto Afectación de procesos críticos, que pueden restablecerse en menos de dos días 6 Regular impacto Afectación de varios procesos no críticos 4 Mínimo impacto Afectación de un proceso no crítico 2 Insignificante Sin afectación de procesos
Nivel de impacto en la imagen ii	Para cada activo clave y de acuerdo a los agentes de amenaza, para determinar el Nivel de impacto en la imagen de la Institución con la pérdida de información en el agente amenaza aplicar los siguientes parámetros: Valor Impacto Imagen 10 Desastroso Difusión a nivel internacional 8 Gran impacto Difusión a nivel nacional 6 Regular impacto Difusión a nivel local 4 Mínimo impacto Difusión dentro de la dependencia o entidad 2 Insignificante Difusión dentro de la unidad
Determinar el valor de R, riesgo.	Una vez evaluado cada uno de los cincos tipos de impacto, se utilizará el valor más alto que se haya obtenido para cada agente de amenaza, a fin de sustituirlo en la fórmula principal R= PI.
Consensuar valores.	Describir las actividades que se llevaron a cabo para el análisis de los resultados obtenidos.
Tabla de Análisis y Determinación de Riesgos – Tabla 5	Derivado del resultado obtenido en el análisis y determinación de riesgos, el resultado se podrá consultar en la Tabla 5 Análisis y Determinación de Riesgos.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Establecer prioridad de atención del riesgo.	Para determinar la Probabilidad de Ocurrencia, analizar los resultados de R, en los que aquellos riesgos cuyo valor sea igual o menor a 1.8, no requieren de llevar a cabo acción alguna por parte de la dependencia o entidad. Aquellos riesgos cuyo valor sea mayor a 1.8, si tienen que ser atendidos, siendo necesario entonces establecer un nivel de prioridad para su atención. El nivel de prioridad de cada riesgo está basado en su valor relativo, esto es, al escenario de riesgo cuyo valor relativo es el más alto, le corresponde la prioridad de 1, al riesgo con el segundo valor más alto, le corresponde la prioridad 2 y así sucesivamente hasta completar todos los escenarios y determinar la estrategia de seguridad a seguir para enfrentar el riesgo: evitar, prevenir, mitigar, financiar o asumir.
Tabla Evaluación de Riesgos	Integrar la Tabla 8 Evaluación de Riesgos con la siguiente información: Código de escenario, Probabilidad, Impacto, Riesgo, Criterio de aceptación, ¿Requiere control?, prioridad, estrategia y controles propuestos.
Fecha de elaboración.	Indicar la fecha de elaboración y/o actualización del formato.
Firmas y fechas de firma, revisión y autorización.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Formato: Documento de definición del SGSI. Formato ASI F4
Clave: ASI F4
Formulación a cargo de: Responsable del Procedimiento de Administración de Seguridad de la Información.
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: El Responsable del Procedimiento de Administración de Seguridad de la Información proporcionará vía electrónica a los integrantes del Grupo Estratégico de Seguridad de la Información para su revisión y aprobación, de acuerdo a la actividad 10 del procedimiento Administración de la seguridad de la información.

5.4.9.4 Instructivo de llenado del Formato
ASI F4

Campo	Descripción.
1. Definición del SGSI.	Indicar la situación actual que existe en la Administración de la seguridad de la información.
Análisis de riesgos.	Describir el resultado y conclusión derivado del análisis de riesgos, de los requerimientos de seguridad de la información de la Institución.
Requerimientos.	Describir los requerimientos que se han identificado para la implantación de los controles en la seguridad de la información.
Estrategias a corto, mediano y largo plazo.	Describir las estrategias que se adoptaron en el tratamiento de los riesgos identificados, estableciendo aquellas que deberán ser adoptadas o implantadas en el corto, mediano y largo plazo.
Estrategias, directrices y mecanismos.	Genera la tabla 1 Estrategias y mecanismos que contendrá la información: Secuencia o número de riesgo, Amenaza, Probabilidad, Impacto, Riesgo, Criterio de aceptación, ¿Requiere control?, prioridad, Estrategia, Controles propuestos.
Controles de seguridad.	Describir los controles de seguridad definidos para contrarrestar el riesgo identificado, indicando el Objetivo de control de la seguridad y el o los controles para su cumplimiento.
2. Programa de implantación del SGSI.	Describir las Datos generales del programa de implantación del Sistema de gestión de seguridad de la información.
Cronograma para la implantación.	Establecer las actividades que se llevarán a cabo para su implantación, indicando las Actividades (alto nivel), el responsable y el periodo para llevarse a cabo.
Métricas de desempeño.	El desempeño de la implementación será medido conforme a las siguientes métricas: Métrica para medición de desempeño del programa = (# de actividades cumplidos en tiempo / # de actividades programados) x 100.

Campo	Descripción.
3. Programa de evaluaciones del SGSI.	De acuerdo al cronograma establecido para la implantación del Sistema de gestión de seguridad de la información, indicar el avance obtenido que se ha tenido hasta el momento.
Reporte y análisis de desviaciones.	Describir las desviaciones que se han tenido para su implantación y las acciones de control determinadas para su atención.
Acciones correctivas y contingentes.	De acuerdo a las desviaciones identificadas, describir la acciones correctivas y contingentes que se han programado al respecto.
Informe de cambios.	Describir los cambios que se han llevado a cabo derivado del proceso de la implantación.
Acciones de mejora continua.	Indicar las acciones y razones de mejora que se han llevado a cabo o que se han programado.
4. Implantación de la mejora al SGSI.	Para el informe de evaluaciones al SGSI, describir los incidentes y acciones de mejora llevadas a cabo o que fueron programadas como parte del proceso de mejora.
Análisis de incidentes y acciones de mejora	Listar los incidentes presentados durante el periodo y que no se encuentra contemplado su mitigación con los controles de seguridad definidos, indicando la siguiente información: Incidente, Acciones de mejora preventivas / correctivas y Responsable.
Conclusiones y lecciones aprendidas.	Derivado de los incidentes presentados, describir las conclusiones a las que se llegó y cuáles fueron las lecciones aprendidas al respecto.
Documentación de referencia.	Indicar los anexos como documentación de referencia para el informe de las evaluaciones llevadas a cabo o programadas para el Sistema de Gestión de Seguridad de la Información, SGSI.
Seguimiento de las acciones de mejora.	Listar las acciones de mejora de acuerdo a los incidentes presentados, indicando lo siguiente: Acciones de mejora preventivas / correctivas, Nivel de cumplimiento, Hallazgos o áreas de oportunidad, Impacto y mejora de la eficiencia, Nueva fecha compromiso para revisión.
Implantación del programa.	Establecer la clave del programa para la implantación del SGSI, Descripción, Impacto, Controles asociados (hacer referencia a la Tabla 7 Información de Controles obtenido en el Formato ASI F3), Fecha de implantación, Responsable de la implantación, Responsable de verificar el cumplimiento (Responsable de la Operación de los Controles de Seguridad de la Información y del ERISC).
Actividades a realizar.	Describir las actividades programadas para la implantación: Número de actividad, Responsable, Descripción, Fecha de inicio, Fecha final, Justificación.
5. Informe de revisión del SGSI.	En la elaboración del informe de revisión, indicar la Documentación de referencia para tal efecto: Formato ASI F2 Catálogo de Infraestructuras críticas y el Formato ASI F3 Documento de Resultados del Análisis de Riesgos.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Incidentes y evaluación.	De acuerdo a los incidentes presentados y su evaluación, indicar Descripción del Incidente / Violación de seguridad, Resultado del intento, Control aplicado para restablecer la seguridad y Análisis y Evaluación del cumplimiento.
Conclusiones.	Describir las conclusiones que se han tenido en el proceso de revisión del Sistema de gestión de seguridad de la información, SGSI.
Fecha de elaboración.	Indicar la fecha de elaboración y/o actualización del formato.
Firmas y fechas de firma, revisión y autorización.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Formato: Directriz rectora de respuesta a incidentes. Formato ASI F5
Clave: ASI F5
Formulación a cargo de: Responsable del Procedimiento de Administración de Seguridad de la Información.
Medio de Elaboración: Computarizado
No. de Ejemplares: Original
Distribución: El Responsable del Procedimiento de Administración de Seguridad de la Información proporcionará vía electrónica a los integrantes del Grupo Estratégico de Seguridad de la Información para su revisión y aprobación, de acuerdo a la actividad 10 del procedimiento Administración de la seguridad de la información.

5.4.9.5 Instructivo de llenado del Formato
ASI F5

Campo	Descripción.
Objetivo.	Establecer el objetivo de la directriz rectora de respuesta a incidentes.
Alcance.	Establecer el alcance de la directriz rectora de respuesta a incidentes.
Justificación.	Indicar la justificación en la definición de la directriz rectora de respuesta a incidentes.
Roles y responsabilidades para la aplicación y cumplimiento de la Directriz.	En la definición de la Directriz, indicar los roles, descripción y responsabilidades de cada actor que tendrá en la definición de la Directriz: Responsable de la seguridad de la información en la Institución o RSII, Grupo de estratégico de seguridad de la información o GESI, Equipo de trabajo de infraestructuras críticas, Equipo de trabajo de análisis de riesgos, Equipo de respuesta a incidentes de seguridad o ERISC, Responsable de la supervisión de la implementación de los controles de seguridad de información y de manejo de riesgos, Responsables de la implementación de los controles de seguridad de información y de manejo de riesgos, Responsable de la Administración de servicios.
Directrices de administración de riesgos.	Describir las necesidades o actividades en la Directriz de administración de riesgos, indicando la Necesidad, Directriz de respuesta a incidentes, Escenario, Impacto.
Mecanismo de difusión de la Directriz.	Describir el mecanismo que se adoptará para la difusión de la Directriz.
Mecanismo de revisión del cumplimiento de la Directriz.	Describir el mecanismo que se adoptará para la revisión del cumplimiento de la Directriz.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias

Campo	Descripción.
Mecanismo de revisión periódica de la Directriz con respecto de las necesidades de la Institución	Describir el mecanismo que se adoptará para la revisión periódica de la Directriz tomando en cuenta las necesidades de la Institución en Seguridad de la información.
Fecha de elaboración.	Indicar la fecha de elaboración y/o actualización del formato.
Firmas y fechas de firma, revisión y autorización.	Indicar el nombre y cargo del servidor público, firma, fecha de firma y el rol que tiene en el llenado del formato, tomando en cuenta que la aprobación deberá ser por el Responsable de la Seguridad de la Información en la Institución. El documento deberá ser rubricado en todas las hojas, por todos los servidores públicos especificados en esta sección.

5.4.9.3.1 Instrucción de Trabajo Tabla de Análisis de Costo - Beneficio

Nombre: Tabla de Análisis de Costo - Beneficio

Clave: **Código: Pr-ADMVO-CONALEP-006-Pd-004-IT-01** **No. de Revisión:** 01

Propósito: Mediante un análisis de los agentes de amenaza para cada uno de los activos clave definidos, generar la tabla del impacto en su costo - beneficio.

Alcance: De acuerdo a la tabla de amenazas y cada uno de los agentes definidos y su impacto en la pérdida de información en los activos clave.

Etapa / Actividad	Tarea	Responsable
I. Análisis de Costo – Beneficio.		
1	Tabla para el análisis definiendo las columnas: Código Escenario; Prioridad; Riesgo; Control; Costo; Probabilidad de ocurrencia; Impacto en recursos económicos; Valor económico del riesgo; ¿control aceptable?; Probabilidad de ocurrencia después de implementar el control; Impacto después de implementar el control; Riesgo residual (después de implementar el control); ¿control conveniente?; ¿se recomienda?; Inversión necesaria.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.1.	Anotar en la primera fila el código de escenario de riesgo de máxima prioridad, junto con sus valores de "prioridad", "R", y "P", así como el "Control" propuesto de mayor valor.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.2.	Anotar, en las filas siguientes, los mismos datos para aquellos escenarios a los que les aplica el mismo Control de la primera fila.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.3.	Continuar con el escenario de mayor prioridad de entre los que aún no se han considerado.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de

Etapa / Actividad	Tarea	Responsable
		trabajo de infraestructuras críticas.
1.4.	Ejecutar los pasos 1, 2 y 3, hasta agotar todos los escenarios.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.5.	Para cada escenario, investigar el Costo del control (B), considerando para ello costos de adquisición o desarrollo, instalación, mantenimiento, capacitación, soporte técnico, etc.).	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.6.	Investigar y consensuar el impacto "I$", desde un punto de vista exclusivamente financiero y con la mayor precisión posible (considerar costos de inventario, pérdidas por procesos interrumpidos, costos de recuperación de imagen, datos, hardware, software, etc.).	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.7.	Calcular "R$" (riesgo en función de costos) mediante el producto de "P" por "I$".	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.8.	Comparar costos entre "B" y "R$"; a. Si "B" es menor o igual a "R$", el control es aceptable. b. Si "B" es mayor a "R$", rechazar el control y reiniciar el proceso al mismo escenario, con un control diferente, incluyendo aquellos escenarios a los que le aplique el nuevo control.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
II. Reanálisis.		
1.9.	Recalcular "P" (ahora P'), pero tomando en cuenta la influencia del control ya aceptado.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.10.	Recalcular I' para estar en posibilidades de obtener el valor de R', al multiplicar P' por I'.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de

Etapa / Actividad	Tarea	Responsable
		trabajo de infraestructuras críticas.
1.11.	Verificar si R es ahora menor que R', en cuyo caso se considera que el control es conveniente y se recomienda. En caso contrario, deberá reiniciar el cálculo.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.12.	Registrar los costos de todos los controles recomendados y obtener el total a invertir.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.13.	Continuar con el llenado de la Tabla de Reproceso de análisis Costo - Beneficio, capturando los códigos de los escenarios en el orden de su prioridad original.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.14.	Asignar a cada escenario el valor de su riesgo residual (R').	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.15.	De acuerdo a su nuevo riesgo residual, asignar nuevamente prioridades.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
1.16.	Proponer nuevos controles para aquellas prioridades elevadas, y, de ser el caso, reiniciar el análisis costo beneficio.	Responsable del Procedimiento Administración de Seguridad de la Información y el Equipo de trabajo de infraestructuras críticas.
	Termina	
	Total de Actividades: 16	**Duración Estimada:** 15 días.

Elaboró	Revisó	Autorizó
Eudaldo Rivera Melgarejo	Joel Olvera Velázquez	José Cartagena Subdias