Manual de Normas y Procesos
Tecnología de la Información

Auditoria de Software
Mantenimiento Preventivo
Desarrollo, Mantención y Adquisición de sistemas o Bases de datos
Validación de infraestructura tecnológica

Realizó	***Validó***	***Validó***	***Revisó***	***Autorizó***
Andrés Canto Cáceres / ACAD *Líder de Normatividad*	*Lic. Tania González Segura* *Gerente Corporativo GTHC*	*Ing. Jorge Torres Erosa* *Gerente Corporativo de TI*	*Lic. Jorge Paredes Chi* *Director de Contraloría*	*Lic. Arturo Quirarte Dayarse* *Director General*

Diciembre 2017

GRUPO DICAS

Manual de Tecnología de la información

Control de versiones

Capítulo e inciso al que se aplicó el cambio		Área Responsable del cambio	Versión

Contenido

Introducción

Antecedentes

Grupo Dicas es una de las compañías corporativas más reconocidas y exitosas del sureste mexicano. Nuestra experiencia avala el prestigio y posicionamiento dentro de las principales industrias en las que participa, como lo son la automotriz, inmobiliaria, petrolera y hotelera, además de diversos proyectos e iniciativas de negocio con impacto nacional, operando empresas exitosamente, creando oportunidades de crecimiento para todos nuestros aliados y colaboradores.

Objetivo

El Manual de Tecnología de la Información, presenta las normas, procesos y actividades de las unidades responsables de ejecutar los procesos de Auditoria de Software, Mantenimiento Preventivo, Desarrollo, Mantención y Adquisición de sistemas o Bases de datos y Validación de infraestructura tecnológica con los siguientes propósitos:

- Describir y transmitir en forma ordenada y sistemática, las responsabilidades del Gerente Corporativo de TI, Gerente General de Unidad de Negocio, Director de área, Líder de área y Colaborador que intervienen en estos procesos.
- Promover el desempeño eficiente de las labores, evitar duplicidades y estimular la eficiente toma de decisiones.
- Garantizar que la actuación de cada integrante se apegue a la normatividad y responsabilidad que exige su desempeño laboral.
- Facilitar la capacitación, garantizar la correspondencia entre los requerimientos de cada puesto, la capacidad y habilidades de quienes los atienden.
- Garantizar que las actividades relacionadas con los procesos de Auditoria de Software, Mantenimiento Preventivo, Desarrollo, Mantención y Adquisición de sistemas o Bases de datos y Validación de infraestructura tecnológica, se apeguen a las leyes laborales vigentes.

Presentación

El Manual de Tecnología de la información está estructurado en once capítulos. Los primeros tres describen su contexto general y los siguientes describen las normas, responsabilidades y procesos principalmente junto con su flujo y descriptivo.

Alcance del Manual

Comprende los procesos de Auditoria de Software, Mantenimiento Preventivo, Desarrollo, Mantención y Adquisición de sistemas o Bases de datos y Validación de infraestructura tecnológica, desde que el Gerente Corporativo de TI se encarga del correcto manejo de software en las unidades de negocio, corregir irregularidades en la infraestructura tecnológica, hasta la creación de base de datos en una unidad de negocio, generando un impacto positivo dentro del Grupo.

Normas Generales

Auditoria de Software

1. La planeación de trabajo de auditoria de software debe contener todas las áreas posibles a auditar.
2. El reporte de auditoria de software debe ser debidamente llenado por el Gerente Corporativo de TI.
3. El Líder de área o colaborador en todo momento debe colaborar con el Gerente Corporativo de TI en el proceso de auditoría.
4. Se deberá reportar inmediatamente al Gerente Corporativo de TI cualquier invitación o notificación de una revisión de software.
5. Se realizarán inventarios internos para validar las licencias instalados en el equipo.
6. Los soportes del software instalado en el equipo son factura de origen, fotografías de los COA no de serie, Caja, los números de contrato, si tiene nuevos proyectos adjunte las cotizaciones u órdenes de compra.
7. Está prohibido el uso de software ilegal o sin soporte de su origen.
8. Es responsabilidad del colaborador tener conocimiento de los productos instalados en su equipo de cómputo.
9. Hay que reportar a cualquier usuario no identificado del área de TI que esté haciendo instalaciones en los equipos de oficina.

Mantenimiento Preventivo

1. El Gerente Corporativo de TI elaborara la programación de mantenimiento preventivo de los equipos de cómputo al inicio de cada ejercicio de año, tomando como base el levantamiento y actualización del inventario de equipos de cómputo de la UNE.
2. Las actividades deberán ser programadas en fechas que no afecte el desarrollo normal de las labores de los usuarios.
3. La programación será compartida por los diferentes mecanismos de comunicaciones correos electrónicos, memorandos, mensajería instantánea, etc.
4. El mantenimiento preventivo a los equipos de cómputo e impresoras, se ejecutará una vez por año. Este se realizará en las instalaciones físicas de cada UNE de Grupo Dicas según la programación establecida.

5. En caso de no poder cumplir los mantenimientos programados por cualquier eventualidad, se programa nueva fecha y se informar por escrito y con anterioridad, los cambios a los directamente implicados.
6. El Gerente Corporativo de TI deberá llenar y archivar correctamente los formatos de mantenimiento preventivo para evidenciar los trabajos realizados.

Desarrollo, Mantención y Adquisición de sistemas o Bases de datos

1. El Gerente de TI, es el responsable de la seguridad de los sistemas de información (seguridad informática) de todas las UNEs.
2. El Gerente de TI, en conjunto con el propietario, dueño o responsable del o los sistemas de información, son los responsables de definir el nivel de criticidad del sistema de información, y de identificar los controles de seguridad a aplicar para resguardarlos.
3. Tener normas de programación, versionamiento, documentación y pruebas para cada etapa del ciclo de vida: construcción, pruebas, explotación.
4. Construir los sitios para los procesos de producción, así como los procesos de pruebas, deben efectuarse en ambientes dispuestos para ello.
5. Los sistemas que interoperen o intercambien datos, con otros sistemas o base de datos, pertenecientes al Grupo u otra UNE, deben contar con controles de seguridad en ambos extremos de la comunicación.
6. La responsabilidad del proceso de construcción y/o mantención de sistemas, en particular la programación (codificación), debe tener siempre dos o más responsables de forma que no se detenga el proceso por ninguna circunstancia, es decir, no debe depender una sola persona.
7. El proceso de construcción y/o mantención de sistemas de información tercerizados deben cumplir con estas políticas y con las normas que dicte Grupo Dicas.
8. La documentación de los sistemas de información debe obedecer a los lineamientos de documentación de sistemas. Excepciones a esta política, son la adquisición de software empaquetado.
9. Toda la documentación asociada al ciclo de construcción y/o mantención de sistemas de información debe tener procedimientos de control de versionamiento.
10. El acceso a la documentación de sistemas de información, bibliotecas de códigos fuentes y programas ejecutables, debe estar restringida sólo a personal autorizado. La excepción a esta política, son los manuales de usuario, manuales de capacitación, u otros documentos destinados a los usuarios del o los sistemas de información.
11. La arquitectura de los sistemas de información debe obedecer a los lineamientos de arquitectura de sistemas por Grupo Dicas definidos.

12. Para la construcción de nuevos sistemas de información o mejoras a los existentes, se debe especificar los controles de seguridad desde la etapa de levantamiento de requerimientos, tales como encriptación de claves, de mensajes, de configuración, auditoria de trazabilidad, entre otros.
13. En la identificación de controles de seguridad deben participar las áreas de negocio que serán usuarios del sistema de información en construcción o proceso de mantención.
14. El diseño e implementación de controles de seguridad, deben ser preferentemente de tipo automático, evitando procesos o intervención manuales. Las excepciones deben ser aprobadas por el Gerente de TI.
15. En la etapa de diseño, debe considerarse los procedimientos necesarios para realizar revisiones periódicas de contenidos de campos, registros, tablas (de datos), o archivos considerados sensibles, frecuencia de los respaldos y tiempos de retención de estos, y procesos de depuración (limpieza de datos, indexaciones, u otros procesos relacionados con optimización y rendimiento)
16. Se puede emplear datos de prueba extraídos desde las bases de datos de los sistemas en producción, pero sólo deben ser empleadas dentro de las instalaciones de Grupo dicas y UNEs. Excepciones a esta política, deben ser autorizadas por el dueño de la información, o en su defecto por el Director General y se deberá elaborar y formalizar un Convenio de Confidencialidad por parte de terceros.
17. El acceso a las bases de datos de construcción, prueba y producción, deben contar con controles de acceso (autenticación y autorización). Debe definirse quiénes (roles) tienen acceso a las bases de datos en sus diferentes ambientes y qué tipo de acceso (consulta, actualización, eliminación). Jamás en la etapa de construcción y/o prueba se debe dar acceso a los datos de producción.
18. En términos generales, todo sistema que considere transformación de datos de entrada debe ser diseñada y construida considerando controles de integridad de éstos.
19. Los sistemas que se construyan en Grupo Dicas o por proveedores, y aquellos sistemas “paquetizados” que se adquieran, deben contemplar funcionalidades que permita acceder tanto a los registros de auditoría como a los registros de trazabilidad.
20. Cuando un sistema tenga previsto el envío de datos (interoperabilidad) que contengan información clasificada como reservada, se debe implementar mecanismos de cifrado de los datos.

21. El dueño o propietario de la Información, en conjunto el gerente de TI, evaluarán la necesidad de usar y aplicar tecnologías de encriptación para proteger información, o de tecnologías de firma digital para firmar documentos electrónicos.
22. Se usará firma digital avanzada, sólo cuando se trate de documentos con carácter de instrumento público.
23. El proveedor de firma electrónica avanzada deberá ser una Entidad Certificadora con registro vigente
24. El mecanismo de autenticación de usuarios del Grupo debe estar basado en una estructura de árboles jerárquicos. Excepciones a esta política deben estar autorizadas el gerente de TI.
25. La generación de códigos de cuentas y contraseñas de acceso de los usuarios a los sistemas de información, deben asegurar, a lo menos:
    - Que los códigos de cuentas sean únicos.
    - Que la generación de contraseñas cumpla al menos con atributos tales como: largo mínimo, sean alfanuméricas, no repetibles, renovables periódicamente, y que permita su cambio por el involucrado (usuario) cuando se use por primera vez.
26. El mecanismo o procedimiento de creación de grupos de usuarios, perfiles o privilegios, entre otros aspectos, deben preferentemente ser administrado en cada sistema de información. Excepciones a esta política deben ser autorizadas el Gerente de TI.
27. La solicitud de códigos de cuentas de acceso a los sistemas de información debe efectuarse según se establece en la Política de Control de Acceso.
28. Toda la documentación, archivos ejecutables, códigos fuente y librerías de software de los sistemas construidos, script de bases de datos, así como la documentación de paquetes de software adquiridos, debe estar bajo procedimientos de control de cambios y de versionamiento.
29. La Unidad de Operaciones debe mantener un registro actualizado de todos los sistemas en explotación, con datos respecto de versión, fecha de última compilación, responsable(s) de su mantención y soporte.
30. Previo a cualquier cambio, actualización, o reconfiguración, planificada, en los servidores de aplicaciones, de bases de datos, u otros equipos asociados a la operación de sistemas de información, se debe efectuar un análisis y emitir un informe técnico que evalué los impactos y riesgos que puedan generar estos cambios.
31. En el proceso de análisis y adquisición de paquetes de software a terceros, deben considerarse aspectos y atributos de seguridad de la información, y el impacto en la

seguridad frente eventuales cambios o modificaciones para su implantación en Cualquier UNE de Grupo Dicas.

32. Las modificaciones a los paquetes de software o sistemas adquiridos a terceros, que surjan producto de su explotación y tengan relación con la seguridad de la información, deben ser aprobados el Gerente de TI.
33. Se prohíbe el uso y/o copia de cualquier paquete de software, por parte de los usuarios de cualquier UNE de Grupo Dicas, del cual no se disponga de su respectiva licencia que lo autorice.
34. La instalación de paquetes de software que son denominados "OPEN" deben ser autorizados por el gerente de TI con el objeto de validar si están dentro de los lineamentos de herramientas de software utilizados por Grupo Dicas.
35. La puesta en producción de los Sistemas de Información, sean éstos construidos internamente o adquiridos a terceros, deben siempre considerar la realización de actividades de capacitación dirigida a Usuarios Finales, Administradores de Plataforma y de la Mesa de Ayuda.

Validación de la Infraestructura Tecnológica

El departamento de TI tiene la facultad para construir, delimitar o definir las instalaciones, los equipos y programas existentes y a ser adquiridos que conforman los activos informáticos adecuados, para la ejecución de los procesos.

1. Definir y dictar las políticas, estándares en tecnologías, seguridad de la información (integridad y confidencialidad) y su soporte tecnológico, velando por el cumplimiento de la normativa legal.
2. Evaluar el área física donde se instalará un nuevo hardware informático, confirmando que el área este óptima para la instalación de los mismos.
3. Asegurar que los equipos tecnológicos tengan: disponibilidad de energía eléctrica, cableado estructurado y mantengan las condiciones físicas aceptables y adecuadas de temperatura, entre otros.
4. Solicitar al Departamento Administrativo y Financiero los recursos para la adquisición de las infraestructuras o servicios que garanticen la continuidad de cualquier UNE de grupo Dicas.

5. Construir, seleccionar, instalar y mantener el buen funcionamiento de las instalaciones y la infraestructura de TI.
6. Supervisar los proyectos de construcción, destrucción o remodelación de instalaciones físicas relacionadas con la infraestructura tecnológica.

7. Participar en los comités de adquisición de bienes y/o servicios, donde se incluyan equipos informáticos como parte integrante o complementaria de otros.
8. Vigilar y llevar un inventario detallado de la infraestructura tecnológica de la cada UNE, acorde con las necesidades existentes de la misma.
9. Coordinar la adquisición o reemplazo de los activos informáticos que hayan sido proyectados, según las necesidades que se presenten en cada área de trabajo.
10. Prolongar la vida útil de los equipos de la infraestructura tecnológica.
11. Validar el cumplimiento de las especificaciones del hardware de TI indicadas en las solicitudes de compra, de no ser así se encargará de la devolución de los mismos.
12. Validar la ejecución de mantenimiento preventivo de todo el hardware como equipos informáticos de las UNEs de Grupo Dicas.
13. Instalar toda la infraestructura tecnológica utilizada en la cualquier UNE de grupo Dicas.
14. Verificar el inventario de los equipos de TI que sean instalados, con la finalidad de llevar un control de los mismos.
15. Instruir al Usuario sobre el uso y manejo adecuado de la infraestructura de TI.
16. Los usuarios solo podrán utilizar los equipos asignados para ejecutar las actividades o tareas correspondientes a sus funciones asignadas por el puesto que desempeña.
17. Informar a TI, en caso de presentarse cualquier problema de infraestructura de TI
18. Los encargados deberán informar a TI cuales empleados de su área están autorizados para mover su equipo asignado fuera de la oficina.
19. Todo el inventario de activos fijos estará resguardado dentro del depto. de TI
20. Custodiar todos los activos informáticos de cualquier UNE de Grupo Dicas.
21. El responsable de TI custodia los equipos informáticos asignados (PC´s, monitores, teclados, impresoras, USB, etc.)
22. Firmar responsiva de activo fijo (equipo de cómputo) e información almacenada. Validar y firmar la recepción de activo descrito en el *Formulario Préstamo de activos (Equipos).*

Responsabilidades

Auditoria de Software

Gerente Corporativo de TI:

1. Identificar área a auditar.
2. Escoger equipos a auditar en la unidad de negocio.

3. Elaborar reporte de irregularidades en caso de ser necesario.
4. Realizar las correcciones necesarias.
5. Archivar reportes de auditoria de software digitalmente.

Líder de área:

1. Colaborar en la auditoria de software de acuerdo al proceso.

Mantenimiento Preventivo

Colaborador:

1. Firmar formato de mantenimiento preventivo.

Gerente Corporativo de TI:

1. Revisar la planeación de mantenimiento preventivo
2. Realizar mantenimiento preventivo
3. Llenar de manera correcta el formato de mantenimiento preventivo.

Desarrollo, Mantención y Adquisición de sistemas o Bases de datos

Gerente General:

1. Solicitar sistema tecnológico al Gerente Corporativo de TI.

Gerente Corporativo de TI:

1. Realizar evaluaciones de viabilidad de proyecto.
2. Elaborar una presentación para la demostración de un sistema.
3. Archivar documentos digitalmente.

Director de área:

1. Validar o rechazar la presentación del proyecto.

Validación de infraestructura tecnológica

Director de área:

1. Solicitar propuesta de infraestructura tecnológica al Gerente Corporativo de TI.
2. Verificar la propuesta realizada por el Gerente Corporativo de TI.
3. Integrar información de propuesta a su proyecto.

Gerente Corporativo de TI:

1. Analizar el proyecto e identificar necesidades tecnológicas adecuadas.
2. Realizar propuesta de infraestructura tecnológica.
3. Archivar propuestas tecnológicas digitalmente.

Procedimientos / Actividades

Auditoria de Software

Gerente Corporativo de TI:

- Identifica el área a revisar con base a la planeación de trabajando, revisando las fechas determinadas de cada área, para prevenir irregularidades en los equipos tecnológicos de las unidades de negocio.
- Informa fecha de auditoria de software al Líder de área, para asegurar su confirmación.

Líder de área:

- Recibe la información de la fecha de auditoria y confirma de asistencia.

Gerente Corporativo de TI:

- Escoge aleatoriamente equipos tecnológicos a auditar del área para la correcta auditoria de software.
- Realiza auditoria de software con el procedimiento adecuado, en caso de existir una irregularidad elabora un reporte de seguimiento de irregularidades (Anexo 1) con base a los resultados de auditoria y realiza las modificaciones tecnológicas para las correcciones necesarias.
- Elabora un reporte satisfactorio de cierre de auditoria de software (Anexo 2), en caso de no encontrar una irregularidad en los resultados de la auditoria de software.
- Envía reporte de cierre al Líder de área para su verificación.

Líder de área:

- Recibe reporte de cierre de auditoria de software y firma dicho reporte.
- Envía reporte al Gerente Corporativo de TI.

Gerente Corporativo de TI:

- Recibe y archiva reporte de auditoria de software digitalmente y físico.

Mantenimiento Preventivo

Gerente Corporativo de TI:

- Identifica área a revisar con base a la planeación de trabajo (Anexo 1), revisando las fechas determinadas en la planeación de mantenimiento preventivo, para prevenir irregularidades en los equipos tecnológicos de las unidades de negocio.
- Informa fecha de mantenimiento preventivo al Líder de área vía correo electrónico.

Líder de área:

- Recibe información de fecha de mantenimiento preventivo para su preparación.

Gerente Corporativo de TI:

- Escoge equipos para aplicar mantenimiento preventivo con base a su planeación.
- Realiza mantenimiento preventivo de manera satisfactoria.
- Llena y firma correctamente el formato de mantenimiento preventivo (Anexo 2) para el correcto control del proceso.
- Solicita al Líder de área firma de realizado en el formato de mantenimiento preventivo.

Líder de área:

- Recibe solicitud y firma correctamente de realizado.
- Entrega formato de mantenimiento preventivo correctamente al Gerente Corporativo de TI

Gerente Corporativo de TI

- Recibe y archiva formato de mantenimiento preventivo de manera digital o física.

Desarrollo, Mantención y Adquisición de sistemas o Bases de datos

Gerente General:

- Identifica necesidad de un sistema tecnológico para la simplificación de actividades en la unidad de negocio.
- Solicita sistema tecnológico a Gerente Corporativo de TI vía correo electrónico.

Gerente Corporativo de TI:

- Recibe solicitud de sistema tecnológico para la realización oportuna de un análisis de viabilidad.
- Realiza análisis de viabilidad, contemplado las necesidades solicitadas, en caso de rechazar la solicitud, justifica dicho rechazo e informa al Gerente General de Unidad de Negocio.
- Elabora una presentación para el director de área, determinando la proyección de la base de datos solicitada, en caso de que el análisis de viabilidad haya sido positivo.
- Envía presentación correctamente realizada al Director de área vía correo electrónico.

Director de área:

- Recibe presentación para la validación de la información anexada, en caso de rechazo, informa al Gerente Corporativo de TI que su solicitud fue rechazada.
- Informa de aprobación al Gerente Corporativo de TI vía correo electrónico, para la iniciación del proyecto.

Gerente Corporativo de TI:

- Recibe aprobación y archiva documentos digitalmente.
- Inicia el proyecto de la creación de base de datos.

Validación de infraestructura tecnológica

Director de área:

- Determina necesidad de infraestructura tecnológica en un proyecto, analizando las necesidades del dicho proyecto.
- Solicita propuesta de infraestructura tecnológica y envía proyecto a Gerente Corporativo de TI vía correo electrónico o documento en físico.

Gerente Corporativo de TI:

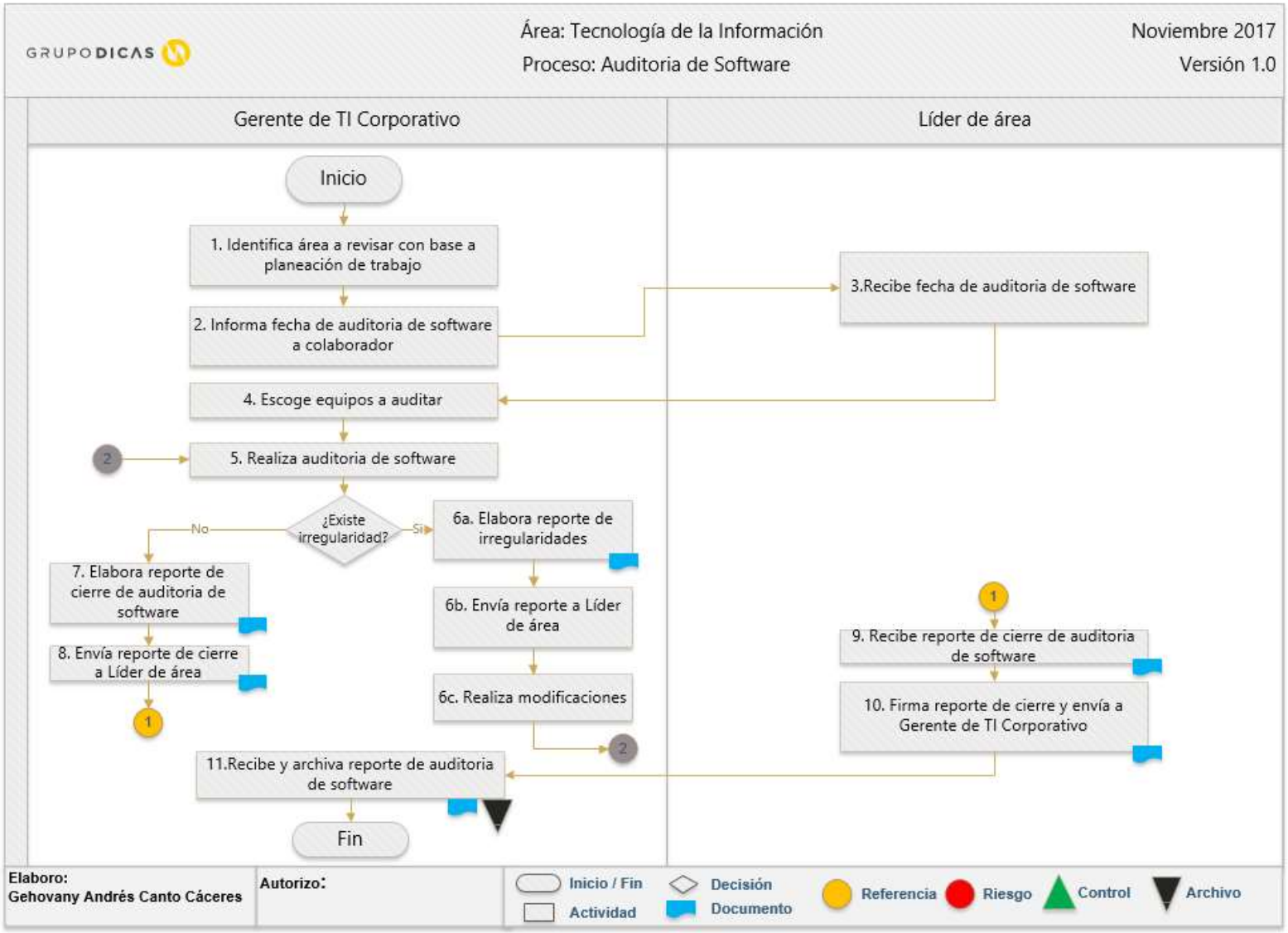
- Recibe solicitud de infraestructura y el proyecto enviado por el Director de área.
- Analiza proyecto e identifica necesidades tecnológicas necesarias de acuerdo a las expectativas de dicho proyecto para su correcta realización.
- Realiza propuesta de infraestructura tecnológica (Anexo 1) con base a los resultados del análisis previamente realizado.
- Archiva documentos digitalmente e igual manera de manera física si es necesario.
- Envía información al Director de área vía correo electrónico o documento en físico si es necesario.

Director de área:

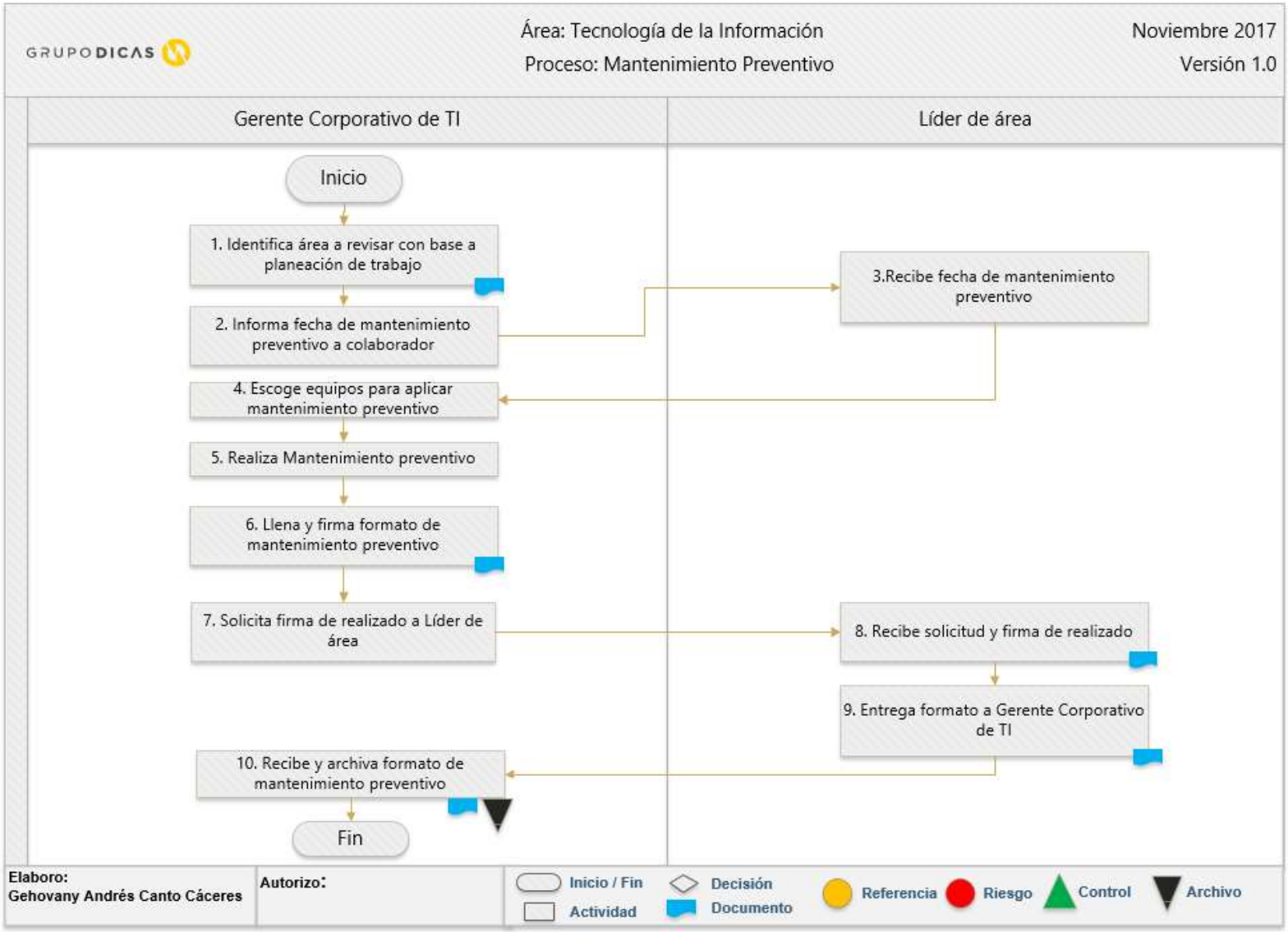
- Recibe información y verifica si necesita alternativas, en caso de necesitarlas, las solicita la Gerente Corporativo de TI.
- Integra información al proyecto de manera satisfactoria, en caso de estar de acuerdo a la propuesta realizada por el Gerente Corporativo de TI.

Diagramas de Flujo

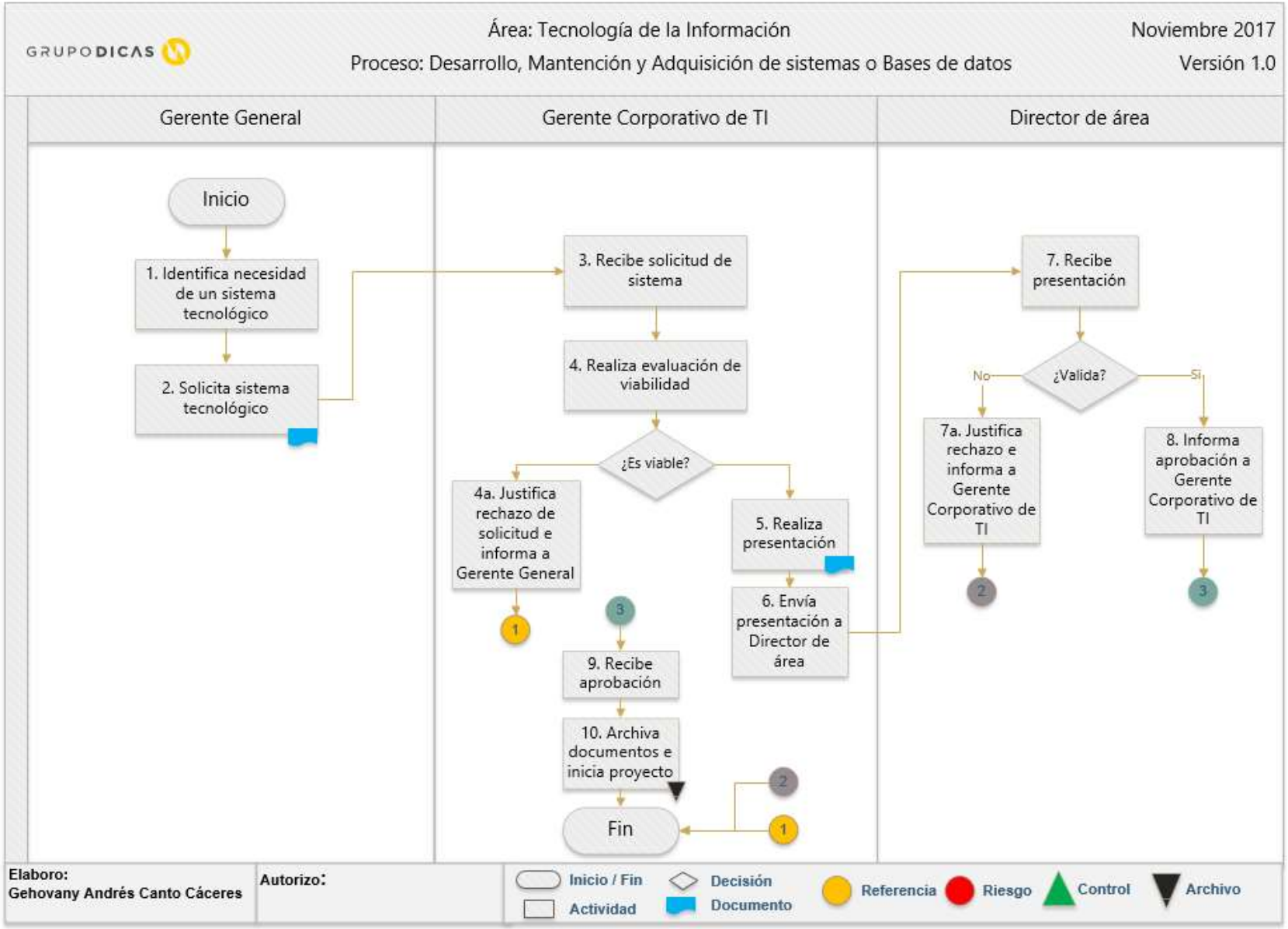
Auditoria de Software



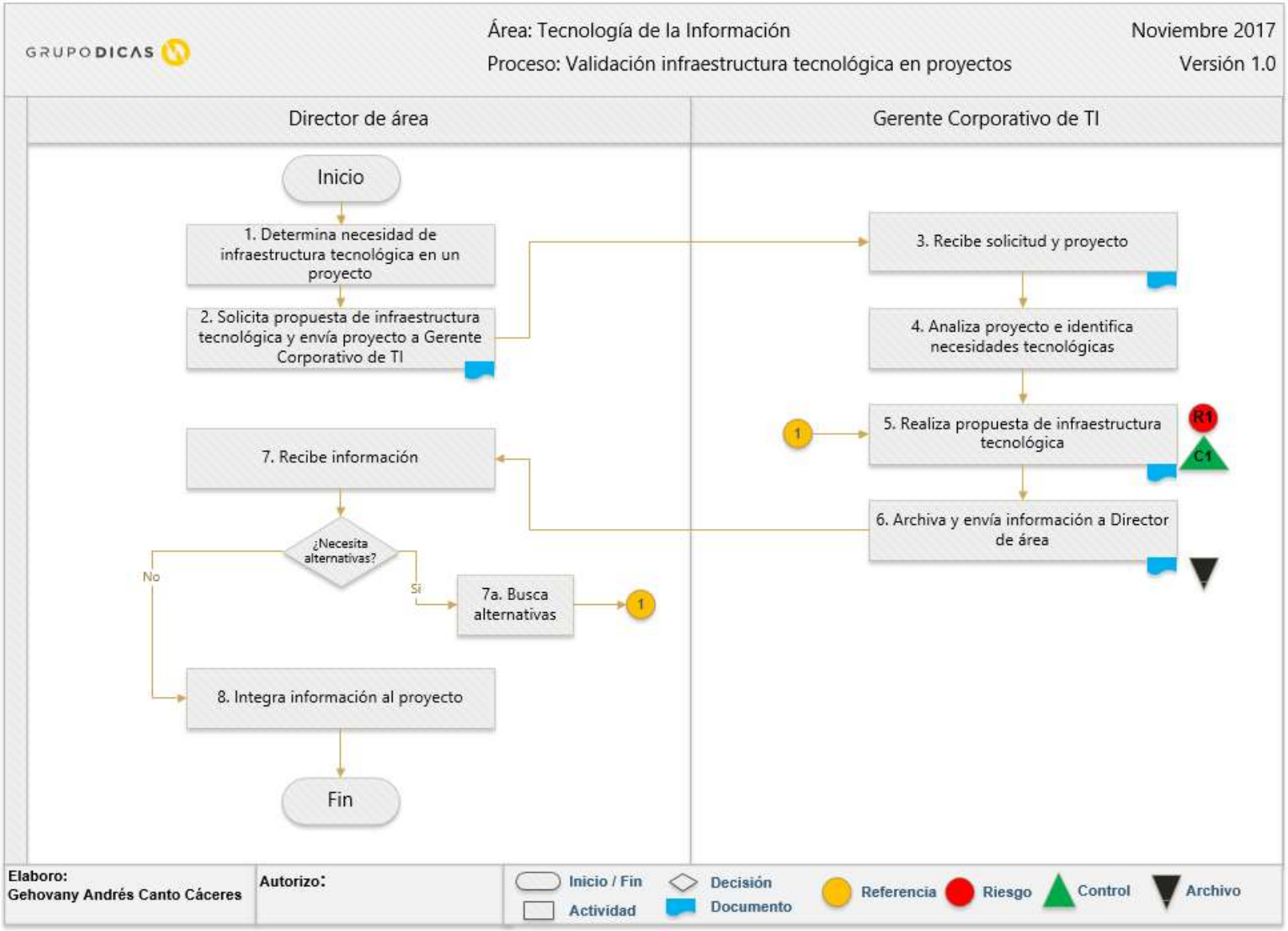
Mantenimiento Preventivo:



Desarrollo, Mantención y Adquisición de sistemas o Bases de datos:



Validación de infraestructura tecnológica en proyectos:



GRUPO DICAS

Descriptivo de Actividades

Auditoria de software:

GRUPO DICAS	Área: Tecnología de la Información Proceso: Auditoría de Software			Noviembre 2017 Versión 1.0
RESPONSABLE	**ACTIVIDAD**	**DOCUMENTOS**	**RIESGOS**	**CONTROLES**
Gerente Corporativo de TI	1. Identifica área a revisar con base a planeación de trabajo ¿Cómo? Revisando las fechas determinadas en la planeación de auditoria de software ¿Para que? Para prevenir irregularidades en los equipos tecnológicos de las unidades de negocio.			
Gerente Corporativo de TI	2. Informa fecha de auditoria de software al Líder de área ¿Cómo? Vía correo electrónico.			
Líder de área	3.Recibe fecha de auditoria de software ¿Cómo? Vía correo electrónico.			
Gerente Corporativo de TI	4. Escoge equipos a auditar del área ¿Cómo? Aleatoriamente			
Gerente Corporativo de TI	5. Realiza auditoria de software ¿Cómo? Con el programas especializado.			
	¿Existe irregularidad?			
	En caso de ser negativo:			
Gerente Corporativo de TI	6a. Elabora reporte de irregularidades. ¿Cómo? Con base a los resultados de la auditoria de software ¿Para que? Para el seguimiento y prevención de futuras irregularidades	Reporte de irregularidades		
Gerente Corporativo de TI	6b. Envía reporte a Líder de área ¿Cómo? Vía correo electrónico y documento en físico.			
Gerente Corporativo de TI	6c. Realiza modificaciones (Continua en actividad 5)			
	En caso de ser positivo continua en la actividad 7			
Gerente Corporativo de TI	7. Elabora reporte de cierre de auditoria de software ¿Cómo? Con base a los resultados de la auditoria de software ¿Para que? Para la finalización y elaboración del reporte del cierre.	Reporte de cierre		
Gerente Corporativo de TI	8. Envía reporte de cierre a Líder de área	Reporte de cierre		
Líder de área	9. Recibe reporte de cierre de auditoria de software	Reporte de cierre		
Líder de área	10. Firma reporte de cierre y envía a Gerente de TI Corporativo	Reporte de cierre		
Gerente Corporativo de TI	11.Recibe y archiva reporte de auditoria de software digitalmente y físico.			
	Fin del proceso			

Mantenimiento Preventivo:

GRUPO DICAS	Área: Tecnología de la Información Proceso: Mantenimiento Preventivo TI		Noviembre 2017 Versión 1.0	
RESPONSABLE	**ACTIVIDAD**	**DOCUMENTOS**	**RIESGOS**	**CONTROLES**
Gerente Corporativo de TI	1. Identifica área a revisar con base a planeación de trabajo ¿Cómo? Revisando las fechas determinadas en la planeación de mantenimiento preventivo ¿Para que? Para prevenir irregularidades en los equipos tecnológicos de las unidades de negocio.	Planeación de mantenimiento Preventivo		
Gerente Corporativo de TI	2. Informa fecha de mantenimiento preventivo al Líder de área ¿Cómo? Vía correo electrónico.			
Líder de área	3.Recibe fecha de mantenimiento preventivo ¿Cómo? Vía correo electrónico.			
Gerente Corporativo de TI	4. Escoge equipos para aplicar mantenimiento preventivo ¿Cómo? Con base a su planeación			
Gerente Corporativo de TI	5. Realiza Mantenimiento Preventivo ¿Cómo? Con base a la planeación.			
Gerente Corporativo de TI	6. Llena y firma correctamente el formato de mantenimiento preventivo ¿Para que? Para el correcto control del proceso.	Formato de Mantenimiento preventivo		
Gerente Corporativo de TI	7. Solicita firma de realizado a Líder de área.			
Líder de área	8. Recibe solicitud y firma correctamente de realizado.	Formato de Mantenimiento preventivo		
Líder de área	9. Entrega formato a Gerente Corporativo de TI			
Gerente Corporativo de TI	10. Recibe y archiva formato de mantenimiento preventivo ¿Cómo? De manera digital o física.	Formato de Mantenimiento preventivo		
	Fin del proceso			

Desarrollo, Mantención y Adquisición de sistemas o Bases de datos:

GRUPO DICAS	Área: Tecnología de la Información Proceso: Desarrollo, Mantención y Adquisición de sistemas o Bases de datos			Noviembre 2017 Versión 1.0
RESPONSABLE	**ACTIVIDAD**	**DOCUMENTOS**	**RIESGOS**	**CONTROLES**
Gerente General	1. Identifica necesidad de un sistema tecnológico ¿Para qué? para la simplificación de actividades en la unidad de negocio.			
Gerente General	2. Solicita sistema tecnológico ¿A quién? A Gerente Corporativo de TI ¿Cómo? Vía correo electrónico.			
Gerente Corporativo de TI	3. Recibe solicitud de sistema tecnológico ¿Cómo? Vía correo electrónico ¿Para que? Para analizar la viabilidad			
Gerente Corporativo de TI	4. Realiza evaluación de viabilidad ¿Cómo? Analizando las variables de la solicitud.			
	¿Es viable?			
	En caso de ser negativo:			
Gerente Corporativo de TI	4a. Justifica rechazo de solicitud e informa a Gerente General ¿Cómo? Vía correo electrónico (Fin del proceso).			
	En caso de ser positivo continúa en la actividad 5			
Gerente Corporativo de TI	5. Elabora una presentación correctamente realizada ¿A quien? Al Director de área¿Para qué? Para ejecutar una demostración del sistema	Presentación de demostración		
Director de área	6. Recibe presentación ¿Cómo? Vía Correo electrónico ¿Para qué? Para la validación de dicha presentación.			
	¿Válida?			
	En caso de ser negativo:			
Director de área	6a. Justifica rechazo e informa a Gerente Corporativo de TI ¿Cómo? Vía correo electrónico.			
	En caso de ser positivo continúa en la actividad 8			
Director de área	7. Informa aprobación a Gerente Corporativo de TI ¿Cómo? Vía correo electrónico ¿Para qué? Para la iniciación del proyecto.			
Gerente Corporativo de TI	8. Recibe aprobación ¿Cómo? Vía correo electrónico.			
Gerente Corporativo de TI	9. Archiva documentos digitalmente e inicia proyecto.			
	Fin del proceso			

Validación de infraestructura tecnológica:

GRUPO DICAS	Área: Tecnología de la Información Proceso: Validación infraestructura tecnológica			Noviembre 2017 Versión 1.0
RESPONSABLE	**ACTIVIDAD**	**DOCUMENTOS**	**RIESGOS**	**CONTROLES**
Director de área	1. Determina necesidad de infraestructura tecnológica en un proyecto ¿Cómo? Analizando lo necesario del dicho proyecto.			
Director de área	2. Solicita propuesta de infraestructura tecnológica y envía proyecto a Gerente Corporativo de TI ¿Cómo? Vía correo electrónico y documento en físico	Proyecto y Solicitud de herramienta de trabajo		
Gerente Corporativo de TI	3. Recibe solicitud y proyecto en vía correo electrónico y de igual manera documento en físico.	Proyecto		
Gerente Corporativo de TI	4. Analiza proyecto e identifica necesidades tecnológicas necesarias de acuerdo a las expectativas de dicho proyecto ¿Para qué? Para su correcta realización.			
Gerente Corporativo de TI	5. Realiza propuesta de infraestructura tecnológica ¿Cómo? Con los resultados del análisis de necesidades realizado anteriormente.	Propuesta de infraestructura	R1. Proveedor no cumple con las especificaciones	C1. Realizar una tabla comparativa de proveedores
Gerente Corporativo de TI	6. Archiva documentos digitalmente e igualmente de manera física y envía información a Director de área ¿Cómo? Vía correo electrónico y documento en físico.	Propuesta de infraestructura		
Director de área	7. Recibe información vía correo electrónico ¿Para que? Para verificar si necesita alternativas.			
	¿Necesita alternativas?			
	En caso de ser positivo:			
	7a. Busca alternativas. (Continua en la actividad 5)			
	En caso de ser negativo continua en la actividad 8			
Director de área	8. Integra información al proyecto			
	Fin del proceso			

Formatos

Auditoria de Software

Anexo 1 – Reporte de irregularidades y Anexo 2 – Cierre de Auditoria

ITEM	Archivo	Usuario	Modelo	Serie	Windows	Instalado	Licencia	Office	Licencia	SQL	Licencia	Otros	Licencia	Otros	Licencia		Windows	Office	Visual Studio	SQL SERVER	SQL CAL
RSD14	(osescobe-HP)	osescobe-HP	Hewlett-Packard HP ProDi	MXL4411TY0	Windows 10 Professional (x64) Version 1607	01/09/2016	00330-80000-00000-AA002 (Key: VK7JG-NPHTM-C9	Microsoft - Office Hogar y Empre	00196-13330-03253-AAOEM (Key: ends with VQTKC)	f				Nero - Nero11	Corel - CorelDRAW		REVSAR CONTRATO	CAJA JUSTIFICAR			
RSD04	(CajaGral)	CajaGral	LENOVO F0BB00GULD L	MP1SAMM7	Windows 10 Home Single Language (x64) V	01/03/2017	00327-30463-22041-AAOEM (Key: TCN4Q-DR4B6-X	Microsoft - Office Hogar y Empre	00196-13330-03255-AAOEM (Key: ends with 29VGP)	g							ICAGE222744	CAJA JUSTIFICAR			
RSD26	(Sistemas-HP)	Sistemas-HP	Hewlett-Packard HP ProBo	CNU234895W9	Windows 10 Professional (x64) Version 1607	24/01/2017	00330-80000-00000-AA581 (Key: VK7JG-NPHTM-C9	Microsoft - Office Hogar y Empre	00333-56303-47008-AA926 (Key: ends with 3PFD9)	fg							REVSAR CONTRATO	CAJA JUSTIFICAR			

Mantenimiento Preventivo:

Anexo 1 – Planeación de mantenimiento preventivo

Sistema de Check List Posicion de TI

						Trimestre 1									Trimestre 2									Trimestre 3								
Plan	Clasificaci	Tipo	o Estándar por	Responsab	Periodicid	Enero				Febrer				Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiem			
Actualizacion	Computo	Software	Dicas	RLL	trimestral					p														p												p			
Actualizacion	Computo	Hardware	Dicas	RLL	trimestral										p																								
Actualizacion	Computo	Software	Promotora	RLL	trimestral	p								p								p														p			
Actualizacion	Computo	Hardware	Promotora	RLL	semestral						p																												
Actualizacion	Computo	Software	Servimid	RLL	trimestral				p										p												p								
Actualizacion	Computo	Hardware	Servimid	RLL	semestral							p																										p	
Actualizacion	Computo	Software	Premier motors Me	RLL	trimestral		p																					p											
Actualizacion	Computo	Hardware	Premier motors Meric	RLL	semestral									p																									
Inventario	Computo	Hardware	Dicas	RLL	trimestral									p												p										p			
Inventario	Computo	Software	Dicas	RLL	semestral																							p											
Inventario	Computo	Hardware	Promotora	RLL	semestral	p																																	
Inventario	Computo	Software	Promotora	RLL	semestral																	p																	
Inventario	Computo	Hardware	Servimid	RLL	semestral				p																														

Anexo 2 – Formato de mantenimiento preventivo

GRUPO DICAS

Datos del mantenimiento preventivo

Fecha		**Unidad de negocio**	
Nombre del responsable de mantenimiento			
Hora de inicio		**Hora de finalización**	

Descripción de lo realizado

Evidencias de lo realizado \| OPCIONAL Fotografías

NOTAS	

_____
Responsable de área
Valida

_____
Firma de realización

Validación de infraestructura tecnológica:

Anexo 1 – Propuesta de infraestructura

LABORATORIOS ITPE												
LABORATORIO	**PISO**	**ubicación**	**Categoria**	**voz**		**datos**	**HDMI**	**contacto**	**ubicación**	**descripcion**	**ubicación**	**descripcion**
GEOFISICA	PB	Escritorio Mtro.	Computo			1	1	2	Trayectoria al proyector para el hdmi			
GEOFISICA	PB	Mesa de trabajo	Computo			19		19				
GEOFISICA	PB	Techo	Proyector					1	pared norte	pantalla		
GEOFISICA	PB	Centro del techo	AP			1		1				
GEOFISICA	PB	Centro del techo	Bocina						solo ducteria			
GEOLOGIA	PB	Escritorio Mtro.	Computo			1	1	2	Trayectoria al proyector para el hdmi			
GEOLOGIA	PB	Mesa de trabajo	Computo			1		1				
GEOLOGIA	PB	Techo	Proyector					1	pared norte	pantalla		
GEOLOGIA	PB	Centro del techo	AP			1		1				
GEOLOGIA	PB	Centro del techo	Bocina						solo ducteria			
PETROLERA	PB	Escritorio Mtro.				1	1	1	Trayectoria al proyector para el hdmi			
PETROLERA	PB	Mesa de trabajo				2		2	Uno por cada mesa			
PETROLERA	PB	Techo	Proyector					1	pared sur	pantalla		
PETROLERA	PB	Centro del techo	AP			1						
PETROLERA	PB	Centro del techo	Bocina						solo ducteria			
ELECTRICA	PA	Escritorio Mtro.				1	1	2	Trayectoria al proyector para el hdmi			
ELECTRICA	PA	Techo	Proyector					1	pared norte	pantalla		