



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

PERÍODO ACADÉMICO: 2023-B

ASIGNATURA: TIC'S.

PROFESOR: Ing. Carlos Montenegro.

TIPO DE INSTRUMENTO: Alineamiento Estratégico y Varios

NOMBRE: Marlon Pachacama

FECHA DE ENTREGA: 14/12/2023

GESTION DE TIC

Una institución pública Caso de Estudio tiene definida los siguientes ítems: Misión, Visión y Objetivos Estratégicos Institucionales. Adicionalmente, la Institución tiene aprobado la cadena de valor, mapa de procesos y la estructura organizativa

En el Estatuto institucional debe constar la siguiente información acerca de TICs:

- Atribuciones y Responsabilidades del Proceso y subprocesos de TICs
- Productos y Servicios (Opcional)

Sobre la base de esta información:

- a) Demuestre el grado de alineamiento de la Unidad de TICs con la misión y los Objetivos Institucionales. Para el efecto, corra el proceso para dos escenarios diferentes que se pueden desprender de la Misión, y concluya.
- b) Defina una estructura de la Unidad de Tecnologías de la Información y Comunicación, debidamente justificada, de acuerdo al alineamiento estratégico escogido. Tome en cuenta las directivas del sector público para la Seguridad de la Información. Compare con la estructura actual y concluya.
- c) Suponga que la CGE decide realizar una auditoria integral de la estructura funcional de TICs. Elabore una matriz que le permita identificar el alcance de dicha auditoria, de acuerdo a las Normas de Control interno

ESTATUTO ORGÁNICO REGISTRO CIVIL

Misión: Proveer servicios relacionados con la gestión de la identidad y de los hechos y actos relativos al estado civil de las personas, resguardando y administrando la información y datos personales de manera integral a través de canales físicos y electrónicos con calidad, seguridad, eficiencia y transparencia.

Visión: Convertirnos al 2025 en el referente nacional y regional en la prestación e innovación de servicios públicos, garantizando el derecho a la identidad y protección de datos de nuestros usuarios.

Objetivos estratégicos:

- OE1.- Incrementar los niveles de satisfacción de los usuarios.
- OE2.- Incrementar la oportunidad y calidad en el registro de hechos y actos civiles.
- OE3.- Incrementar la oportunidad y calidad en la identificación de los ecuatorianos y extranjeros que residen legalmente en el país.
- OE4.- Incrementar la oferta y provisión de servicios electrónicos.
- OE5.- Incrementar la seguridad, integridad y confiabilidad de la información registral física y electrónica con estándares de seguridad y protección de datos.
- OE6.- Fortalecer las capacidades institucionales

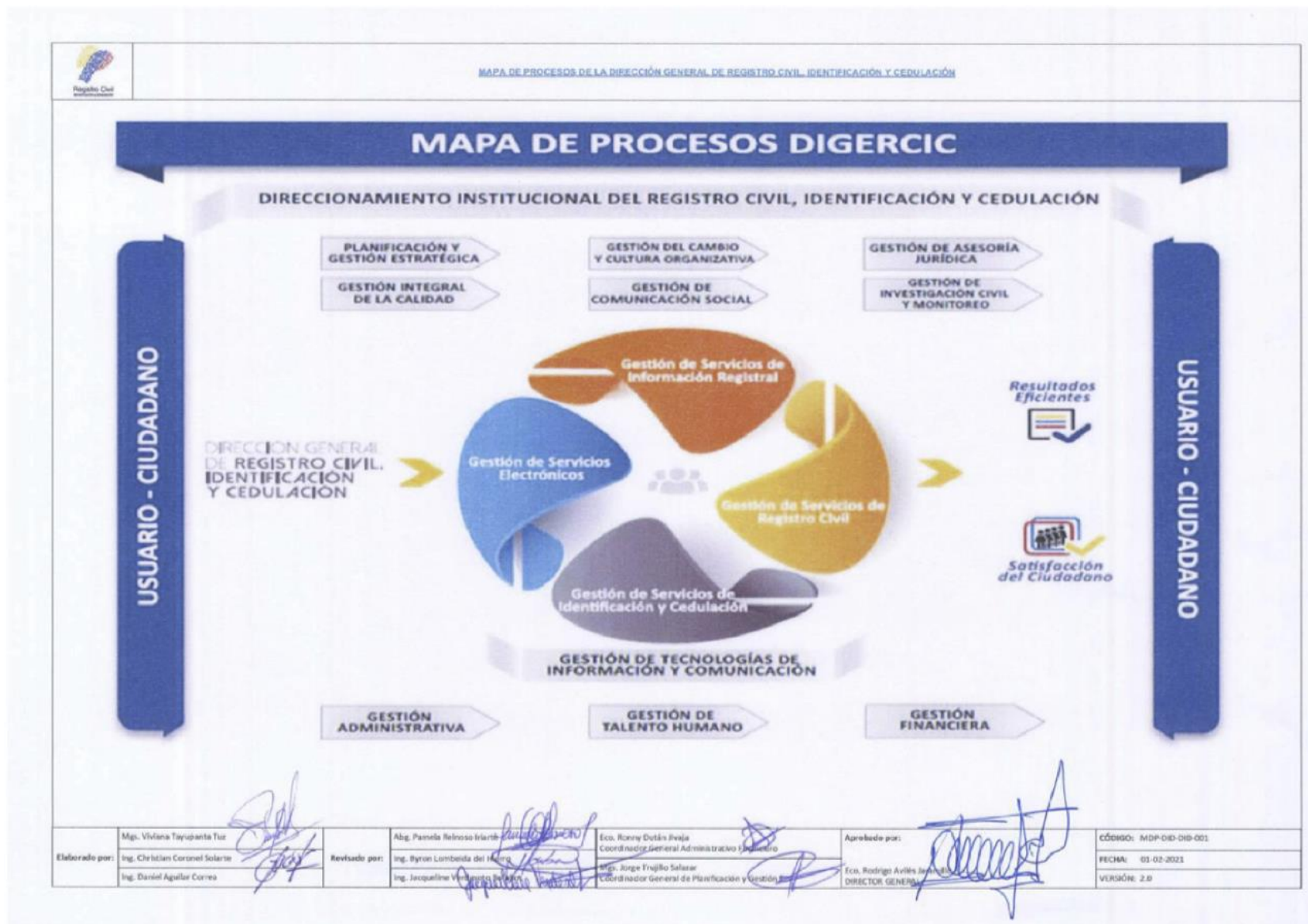
Objetivos Institucionales:

- a) Incrementar los niveles de satisfacción de los usuarios.
- b) Incrementar la inscripción y registro de hechos y actos civiles oportunos y con calidad.
- c) Incrementar la identificación de los ecuatorianos y extranjeros que residen legalmente en el país.
- d) Incrementar la oferta y provisión de servicios electrónicos.
- e) Incrementar la integridad y confiabilidad de la información registral física y electrónica.
- f) Incrementar la eficiencia institucional de la DIGERCIC.
- g) Incrementar el desarrollo del Talento Humano de la DIGERCIC.
- h) Incrementar el uso eficiente del presupuesto de la DIGERCIC.

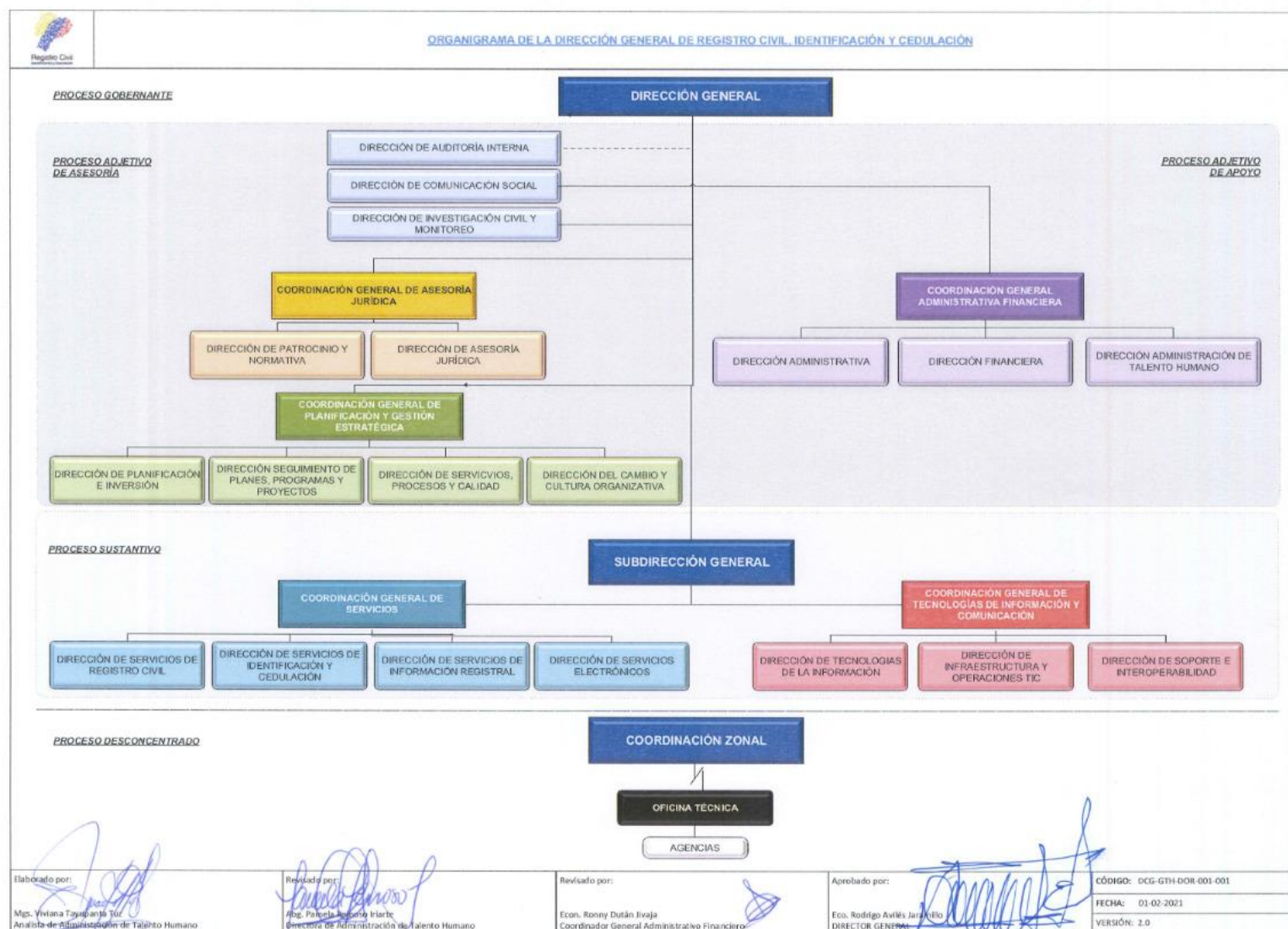
Cadena de Valor:



Mapa de Procesos:



Estructura Organizativa:



Atribuciones y Responsabilidades del Proceso y subprocesos de TICs

1.2.3. Gestión General de Tecnologías de la Información y Comunicación TIC

Misión: Coordinar la prestación de los servicios tecnológicos de la información y comunicación a los usuarios y la gestión interna por medio de la planificación, implementación y control, con el fin de contribuir a la gestión y mejoramiento continuo.

Responsable: Coordinador/a General de Tecnologías de Información y Comunicación TIC

ATRIBUCIONES Y RESPONSABILIDADES:

- a) Asesorar a las autoridades institucionales en materia de TIC;
- b) Articular la Planificación Operativa anual de las Direcciones a su cargo;
- c) Liderar la formulación de los planes: estratégico, operativo y de contratación de bienes y servicios
- d) Gestionar el portafolio de proyectos de TIC;
- e) Monitorear la ejecución de proyectos de TIC;
- f) Coordinar la disponibilidad, continuidad y capacidad de los sistemas, infraestructura y servicios tecnológicos;
- g) Controlar la operación de los sistemas y servicios tecnológicos;
- h) Gestionar los recursos tecnológicos, humanos y presupuestarios de la Coordinación;
- i) Liderar la gestión de la calidad, seguridad y riesgos de TIC;
- j) Liderar la implementación de sistemas y servicios tecnológicos para los usuarios;
- k) Evaluar el desempeño de las TIC en la Institución;
- l) Gestionar el cumplimiento de la normativa gubernamental en materia de TIC;
- m) Controlar la aplicación de políticas, procesos, normas y estándares de TIC para la institución;
- n) Controlar el uso racional de la TIC en la Institución;
- o) Gestionar la innovación tecnológica conforme tendencias y buenas prácticas;
- p) Coordinar las acciones para soporte de usuarios y aplicaciones;
- q) Controlar la gestión de la seguridad informática;
- r) Establecer lineamientos para el cumplimiento de niveles de servicio internos y externos;
- s) Liderar la definición de la arquitectura de referencia de sistemas;
- t) Gestionar los riesgos del uso de TIC;
- u) Articular a la organización con el uso de las TIC;
- v) Evaluar informes de gestión y de resultados del área;
- w) Monitorear el cumplimiento de indicadores de gestión a su cargo;
- x) Controlar y evaluar los reportes y actualización de la herramienta de Gobierno por Resultados de las direcciones a su cargo; y,
- y) Las demás que le sean asignadas por autoridad competente.

1.2.3.1. Gestión de Tecnologías de la Información TI

Misión: Planificar, diseñar, construir y mantener sistemas y servicios informáticos seguros que, a través de una adecuada gestión, satisfagan los requerimientos de los usuarios y de la Institución.

Responsable: Director/a de Gestión de Tecnologías de la Información TI

ATRIBUCIONES Y RESPONSABILIDADES:

- a) Asesorar a las autoridades institucionales en materia de su competencia;
- b) Planificar la gestión operativa de la coordinación;
- c) Gestionar proyectos informáticos que satisfagan los requerimientos de los usuarios;
- d) Analizar, diseñar, desarrollar y probar nuevas aplicaciones y/o cambios a las existentes;
- e) Asegurar la calidad de las nuevas aplicaciones y/o cambios a las existentes, de acuerdo a los procedimientos establecidos;
- f) Gestionar la elaboración de manuales e instructivos técnicos, de capacitación, operación, usuario, administración y paso a producción de las aplicaciones;
- g) Implementar y mantener un repositorio del código fuente e información relacionada con el software de las aplicaciones;
- h) Elaborar normas, procedimientos y estándares en lo referente a arquitectura, desarrollo y mantenimiento de aplicaciones;
- i) Diseñar, mantener y actualizar la arquitectura de sistemas institucionales;
- j) Gestionar el cambio de las aplicaciones institucionales escaladas por los niveles de soporte establecidos;
- k) Analizar y evaluar nuevas tecnologías, estándares y herramientas existentes en el mercado para desarrollo y mantenimiento de aplicaciones;
- l) Aplicar políticas de seguridad informática a nivel de aplicaciones;
- m) Preparar y presentar especificaciones técnicas para contratación de servicios de desarrollo,
- n) Gestionar y mantener actualizada la base de datos de proveedores de aplicaciones;
- o) Gestionar el cumplimiento de niveles de servicio y garantías técnicas contratadas;
- p) Administrar los contratos de desarrollo y/o mantenimiento de aplicaciones de software;
- q) Planificar y controlar los niveles de calidad para el desarrollo y mantenimiento de aplicaciones de software;
- r) Cumplir los niveles de servicio internos establecidos por la Coordinación de TIC;
- s) Establecer métricas de productividad de la dirección;
- t) Controlar la aplicación de las normas oficiales para gestión de la seguridad informática;
- u) Evaluar riesgos asociados a vulnerabilidades y amenazas informáticas internas y externas;
- v) Supervisar y controlar a nivel nacional equipos, sistemas, redes y servicios informáticos contra amenazas a la seguridad;
- w) Gestionar incidentes de seguridad informática internos y externos;
- x) Administrar herramientas y tecnologías para seguridad informática;
- y) Gestionar cuentas de usuario de equipos, sistemas, redes y servicios informáticos;
- z) Gestionar o ejecutar pruebas de intrusión a equipos, sistemas, redes y servicios informáticos;
- aa) Gestionar riesgos de seguridad informática;
- bb) Clasificar los activos informáticos críticos;

- cc) Realizar la creación, seguimiento y actualización de la información en la herramienta Gobierno por Resultados;
- dd) Evaluar el cumplimiento de indicadores de gestión a su cargo; y,
- ee) Las demás que le sean asignadas por autoridad competente.

Gestiones internas:

- Arquitectura y Proyectos.
- Desarrollo y Mantenimiento.
- Seguridad Informática.
- Gobierno de TIC

Entregables:

- Gestión interna de Arquitectura y Proyectos:
 1. Especificaciones técnicas y términos de referencia para contratación de bienes y servicios;
 2. Especificaciones de requerimientos para desarrollo de sistemas internos;
 3. Diseños arquitectónicos de sistemas, plataformas y redes institucionales;
 4. Informes de evaluación de nuevas tecnologías y productos;
 5. Proyectos para implementación de sistemas institucionales;
 6. Estudios de factibilidad y costo/beneficio de proyectos;
 7. Informes de avance de proyectos; y,
 8. Informes de análisis de solicitudes de cambio de sistemas.
- Gestión interna de Desarrollo y Mantenimiento:
 1. Sistemas/aplicaciones institucionales;
 2. Reporte de portales/ páginas Web institucionales actualizadas;
 3. Reporte de servicios Web para intercambio de datos;
 4. Manuales técnicos y de usuarios de sistemas/ aplicaciones;
 5. Instructivos de capacitación de sistemas/aplicaciones;
 6. Informe de programas fuentes inventariados;
 7. Informe de requerimientos de cambio de sistemas/aplicaciones implementadas;
 8. Reportes de control de desarrollo y mantenimiento de sistemas / aplicaciones;
 9. Estándares actualizados para desarrollo de sistemas / aplicaciones; y,
 10. Reporte de bugs/errores de sistemas/aplicaciones corregidas.
- Gestión interna de Seguridad Informática:
 1. Plan actualizado de gestión de la seguridad informática;
 2. Reporte de activos de información inventariados;
 3. Reportes de monitoreo de la seguridad de programas, hardware, redes y servicios;
 4. Base de datos de usuarios y permisos de acceso a sistemas, aplicaciones y servicios informáticos;
 5. Propuestas de políticas, procedimientos y normas para gestión de la seguridad informática;
 6. Reportes de auditoría de seguridad informática;
 7. Reportes de análisis de incidentes informáticos;

8. Informes de gestión de incidentes de seguridad informática;
 9. Reporte de controles de seguridad informática implementados; y,
 10. Reportes de pruebas de intrusión a plataformas de hardware, software y redes de datos,
- Gestión interna de Gobierno de TIC:
 1. Plan operativo anual, plan anual de compras y necesidades de personal de la coordinación;
 2. Plan estratégico institucional de tecnologías de la información actualizada;
 3. Reportes de control y seguimiento de planes y proyectos de la coordinación;
 4. Informes de gestión de la dirección e indicadores de medición de la coordinación;
 5. Presupuesto anual de la coordinación;
 6. Plan institucional de riesgos de tecnologías de la información actualizada;
 7. Procedimiento control de calidad de TIC;
 8. Reporte de sets de pruebas de proyectos y cambios de sistemas;
 9. Informes de control de calidad proyectos y cambios;
 10. Informe de procesos estándares y buenas prácticas de gestión TI implementados;
 11. Reporte de pruebas de proyectos y cambios;
 12. Catálogo actualizado de servicios informáticos; y,
 13. Reportes actualizados de la información en la Herramienta de Gobierno por Resultados.

1.2.3.2. Gestión de Infraestructura y Operaciones TIC

Misión: Implementar y administrar plataformas de hardware, software y redes de datos que por medio de la provisión oportuna garanticen la continuidad, disponibilidad, rendimiento, seguridad y capacidad óptima de los sistemas y servicios informáticos.

Responsable: Director/a de Infraestructura y Operaciones TIC

ATRIBUCIONES Y RESPONSABILIDADES:

- a. Asesorar a las autoridades institucionales en materia de su competencia;
- b. Gestionar la capacidad de la infraestructura para un rendimiento adecuado del procesamiento de datos;
- c. Gestionar la continuidad de las operaciones de TIC que evite suspensión del servicio a los usuarios;
- d. Gestionar la disponibilidad de los sistemas y servicios informáticos institucionales;
- e. Elaborar y establecer normas, procedimientos, estándares de operación y de monitoreo de plataformas de hardware, software y redes de datos;
- f. Inventariar equipos y parámetros de configuración de plataformas de hardware, software y redes de datos;
- g. Dirigir, instalar, configurar, administrar y monitorear plataformas de hardware, software y redes de datos;
- h. Administrar la arquitectura de plataformas de hardware, software y redes de datos;
- i. Gestionar cambios de plataformas de hardware, software y redes de datos en coordinación con las Direcciones que conforman la Coordinación de TIC;
- j. Administrar y configurar plataformas de hardware, software y redes de datos para ambientes de pruebas, desarrollo, producción, capacitación y proyectos;

- k. Administrar, controlar y operar los centros de datos de la Institución;
- l. Elaborar y establecer planes para recuperación de desastres y de continuidad de las actividades de TIC de la Institución;
- m. Solucionar incidentes y problemas de plataformas de hardware, software y redes de datos escalados por los niveles de soporte establecidos;
- n. Ejecutar pasos a producción de nuevas plataformas de hardware, software, redes de datos y aplicaciones o cambios a las existentes;
- o. Administrar bitácoras de operaciones del centro de datos y de redes de datos;
- p. Analizar y evaluar nuevas tecnologías para plataformas de hardware, software y redes de datos;
- q. Establecer políticas de seguridad informática para plataformas de hardware, software y redes de datos;
- r. Presentar especificaciones técnicas para contratación de plataformas de hardware, software y redes de datos;
- s. Administrar la base de datos de proveedores de plataformas de hardware, software y redes de datos;
- t. Gestionar el cumplimiento de niveles de servicio y garantías técnicas contratadas;
- u. Cumplir los niveles de servicio internos establecidos por la Coordinación de TIC;
- v. Gestionar mantenimientos de plataformas de hardware, software y redes de datos en coordinación con las demás Direcciones de la Coordinación de TIC;
- w. Gestionar con la dirección a cargo la ejecución de obras civiles o de otra índole que puedan afectar las redes y los centros de datos;
- x. Gestionar servicios de telefonía IP y comunicaciones unificadas para la Institución;
- y. Realizar la creación, seguimiento y actualización de la información en la herramienta Gobierno por Resultados;
- z. Evaluar el cumplimiento de indicadores de gestión a su cargo; y,
- aa. Las demás que le sean asignadas por autoridad competente.

Gestiones internas:

- Infraestructura.
- Plataformas de Software.
- Redes y Comunicaciones.

Entregables:

- Gestión interna de Infraestructura;
 - 1. Plan de capacidad de hardware, actualizado;
 - 2. Plan de continuidad de TIC institucional, actualizado;
 - 3. Plan de recuperación de desastres, actualizado;
 - 4. Informe de equipos físicos y virtuales instalados y en operación;
 - 5. Reportes de disponibilidad de plataformas de hardware;
 - 6. Reportes de monitoreo de equipos de hardware;
 - 7. Reportes de resolución de incidentes y problemas de equipos;
 - 8. Reporte de pruebas de contingencia de centros de datos;
 - 9. Bitácora de operaciones, actualizada;
 - 10. Plan de respaldos, actualizado;

11. Reporte de Respaldos de datos e información;
12. Informes de restauración de respaldos;
13. Plan mantenimiento preventivo de equipos, actualizado;
14. Informes de cumplimiento de niveles de operación;
15. Informes de control de contratos de soporte y mantenimiento de equipos;
16. Informe de equipos físicos y virtuales inventariados;
17. Informes de cambios y mantenimientos de infraestructura;
18. Reportes de control de proyectos asignados;
19. Especificaciones técnicas para contratación de equipos; y,
20. Reportes de mantenimiento de centros de datos.

- Gestión interna de Plataformas de Software:

1. Reporte de software base en operación (sistemas operativos, bases de datos, middleware, virtualización, otros);
2. Reportes de monitoreo de software base;
3. Reportes de solución de incidentes y problemas de software base;
4. Plataformas institucionales de gestión en operación (email gestión documental, AFIS, HSM, otros);
5. Informes de cumplimiento de niveles de operación;
6. Informes de control de contratos de software base;
7. Reporte de inventario actualizado de software base;
8. Reporte de cambios y mantenimientos de software base;
9. Bases de datos en operación en ambientes de producción, test y desarrollo;
10. Reportes de configuración y afinamiento de bases de datos;
11. Reportes de disponibilidad de bases de datos (ORACLE, DB2, MS SQL Server, MYSQL,QLIKVIEW, otras);
12. Reportes de capacidad de bases de datos;
13. Reportes de respaldos, recuperación y réplicas de bases de datos;
14. Reportes de transacciones almacenadas en las bases de datos (número de transacciones ejecutadas por tipo de usuarios, clientes, agencias, etc.);
15. Informes de procesos de validación de información entregada por instituciones externas;
16. Informes de anomalías y depuración de información registral;
17. Informes de minería de datos;
18. Plan de contingencia de base de datos;
19. Reportes de control de proyectos;
20. Especificaciones técnicas para contratación de software base;
21. Reportes de disponibilidad de plataformas de software;
22. Procedimientos de estándares de operación; y,
23. Reportes actualizados de la información en la Herramienta de Gobierno por Resultados.

- Gestión interna de Redes y Comunicaciones:

1. Diseños de redes físicas y virtuales (LAN/WAN alámbricas e inalámbricas);
2. Reporte de redes físicas y virtuales en operación;
3. Informe de equipos de red y seguridad de red en operación;

4. Reportes de monitoreo de redes;
5. Reportes de solución de incidentes y problemas de redes;
6. Reportes de disponibilidad de enlaces de datos de terceros;
7. Informes de control de contratos de redes con terceros;
8. Reportes de utilización efectiva de redes;
9. Informe sobre respaldos de configuración de redes;
10. Plan de mantenimiento de equipos de redes actualizado;
11. Manuales técnicos de redes;
12. Informe sobre inventario de enlace de datos;
13. Informe sobre inventario de equipos y software de redes a nivel nacional;
14. Reporte de configuraciones de centrales telefónicas IP;
15. Reportes de monitoreo de tráfico de centrales telefónicas;
16. Informes de cambios y mantenimientos de redes; y,
17. Informe sobre pruebas de seguridad de redes.

1.3.2.3.3. Gestión de Soporte e Interoperabilidad TI

Misión: Gestionar la interoperabilidad con entidades externas y facilitar soporte técnico oportuno a requerimientos de usuarios por medio de una gestión adecuada de incidentes y problemas informáticos que permita garantizar la prestación de los servicios a la ciudadanía.

Responsable: Director/a de Soporte e Interoperabilidad TI

ATRIBUCIONES Y RESPONSABILIDADES:

- a. Asesorar a las autoridades institucionales en materia de su competencia;
- b. Gestionar el centro de atención a usuarios a nivel nacional (soporte nivel 0);
- c. Controlar, clasificar, priorizar y asignar solicitudes de soporte de usuarios, de aplicaciones/servicios, redes o infraestructura;
- d. Supervisar el seguimiento y atención oportuna de las solicitudes escaladas a otros niveles de soporte de aplicaciones/servicios, redes, infraestructura;
- e. Gestionar incidentes, problemas y mantenimientos de aplicaciones / servicios, redes o infraestructura;
- f. Gestionar y medir los niveles de servicios internos de TIC;
- g. Gestionar el soporte de aplicaciones institucionales;
- h. Inventariar equipos, aplicaciones, servicios a disposición de los usuarios;
- i. Gestionar el mantenimiento periódico de equipos de usuarios o de uso común para asegurar su óptimo funcionamiento;
- j. Elaborar, controlar y aplicar políticas, estándares y procedimientos para soporte tecnológico;
- k. Dirigir la instalación, configuración y controlar equipos y aplicaciones ofimáticas e institucionales para los usuarios;
- l. Elaborar reportes de actividad y productividad de la dirección;
- m. Analizar necesidades de entrenamiento/capacitación informática para reducir las solicitudes de soporte;
- n. Diseñar servicios tecnológicos para interoperabilidad con entidades externas;

- o. Administrar la asistencia tecnológica para la entrega de servicios de interoperabilidad con entidades externas;
- p. Administrar el sistema de gestión de eventos de seguridad informática;
- q. Elaborar acuerdos de niveles de servicio y uso de los servicios de interoperabilidad;
- r. Facilitar información a las áreas respectivas para provisión y facturación de servicios de interoperabilidad;
- s. Realizar la creación, seguimiento y actualización de la información en la herramienta Gobierno por Resultados;
- t. Apoyar, supervisar y evaluar la gestión de los procesos desconcentrados en el ámbito de Soporte e Interoperabilidad;
- u. Evaluar el cumplimiento de indicadores de gestión a su cargo; y,
- v. Las demás que le sean asignadas por autoridad competente.

Gestiones internas:

- Soporte de Usuarios.
- Soporte de Aplicaciones.
- Interoperabilidad.

Entregables:

- Gestión interna de Soporte de Usuarios:
 - 1. Reporte de tickets atendidos de soporte a requerimientos de usuarios;
 - 2. Reportes de gestión de atención de requerimientos;
 - 3. Reporte de notificaciones de incidentes y problemas;
 - 4. Reporte de notificaciones de mantenimientos planificados y no planificados;
 - 5. Informe sobre inventario actualizado de equipos y software de usuarios finales;
 - 6. Base de datos de conocimientos de incidentes y problemas, actualizada;
 - 7. Reportes de incidentes de seguridad informática;
 - 8. Procedimientos estándares de operación;
 - 9. Reportes de escalamiento de tickets de soporte;
 - 10. Informes de mantenimiento de equipos y software de usuario;
 - 11. Instructivos para uso de equipos y software de usuarios;
 - 12. Informe sobre pruebas de sistemas y equipos informáticas;
 - 13. Reportes de comisiones técnicas a otras dependencias.
- Gestión interna de Soporte de Aplicaciones:
 - 1. Informe sobre inventario de aplicaciones, actualizado;
 - 2. Reportes de monitoreo de aplicaciones;
 - 3. Reportes de atención de solicitudes de soporte de aplicaciones;
 - 4. Reportes de solución de incidentes y problemas de aplicaciones;
 - 5. Informes de control de contratos de soporte de aplicaciones;
 - 6. Informes de cambios y mantenimientos de aplicaciones;
 - 7. Reportes de disponibilidad de aplicaciones;
 - 8. Manuales de soporte de aplicaciones;

9. Programas de software de monitoreo y operación de aplicaciones;
10. Reportes de pasos a producción nuevas o cambios de aplicaciones;
11. Reportes de gestión de incidentes y problemas;
12. Reportes de gestión de mantenimiento de infraestructura y sistemas;
13. Acuerdos de niveles de servicios de TIC;
14. Encuestas de satisfacción de usuarios;
15. Base de datos de ítems tecnológicos (CMDDB);
16. Reporte de solicitudes de cambios de sistemas; y,
17. Reportes de medición de niveles de servicios.

- **Gestión interna de Interoperabilidad:**

1. Informes técnicos para implementación de servicios de interoperabilidad;
2. Reporte de pruebas de interoperabilidad con entidades externas;
3. Reporte de servicios de interoperabilidad implementados;
4. Acuerdos de confidencialidad para uso de servicios de interoperabilidad;
5. Catálogo de servicios Web para interoperabilidad;
6. Reportes estadísticos de servicios de interoperabilidad para facturación;
7. Manuales técnicos y de usuarios de servicios de interoperabilidad;
8. Reportes de entrega-recepción de servicios de interoperabilidad con entidades externas;
9. Informes de cumplimiento de niveles de servicio para interoperabilidad;
10. Informes de gestión de incidentes de interoperabilidad;
11. Propuestas de políticas, procedimientos y normas tecnológicas para implementación de servicios de interoperabilidad; y,
12. Reportes actualizados de la información en la Herramienta de Gobierno por Resultados.

Sobre la base de esta información:

- a) **Demuestre el grado de alineamiento de la Unidad de TICs con la misión y los Objetivos Institucionales. Para el efecto, corra el proceso para dos escenarios diferentes que se pueden desprender de la Misión, y concluya.**

Escenario 1

Mejora en Servicios Electrónicos (Objetivo d):

Análisis:

- La Unidad de TICs debe centrarse en fortalecer y expandir los servicios electrónicos para alinearse con el objetivo institucional "d".
- Debería garantizar la eficiencia, seguridad y calidad en la provisión de servicios electrónicos relacionados con el estado civil.

Contribución:

- Desarrollo de plataformas electrónicas para facilitar la inscripción y consulta de hechos civiles.
- Implementación de medidas de seguridad para proteger la información personal.

Conclusión:

- La Unidad de TICs contribuye directamente al logro del objetivo "d", mejorando la oferta de servicios electrónicos de manera eficiente y segura.

Escenario 2

Eficiencia Institucional (Objetivo f):

Análisis:

- La eficiencia institucional (Objetivo f) implica mejorar procesos internos para una gestión más efectiva.
- La Unidad de TICs puede desempeñar un papel clave en la optimización de sistemas y procesos tecnológicos.

Contribución:

- Implementación de sistemas de información que agilicen los procesos internos.
- Desarrollo de herramientas para la gestión eficiente de la información registral.

Conclusión:

- La Unidad de TICs contribuye significativamente al objetivo "f", mejorando la eficiencia institucional mediante soluciones tecnológicas.

Conclusión General:

La Unidad de TICs muestra un alto grado de alineamiento con la misión y objetivos institucionales, ya que contribuye directamente a mejorar la oferta de servicios electrónicos y a optimizar la eficiencia interna. Sus esfuerzos se alinean estrechamente con la misión de proveer servicios de identidad y estado civil de manera integral, segura y eficiente.

- b) Defina una estructura de la Unidad de Tecnologías de la Información y Comunicación, debidamente justificada, de acuerdo con el alineamiento estratégico escogido. Tome en cuenta las directivas del sector público para la Seguridad de la Información. Compare con la estructura actual y concluya.**

1. Director de TICs:
 - Responsable de liderar la estrategia y alineación de la Unidad con los objetivos institucionales.
 - Supervisión de las operaciones diarias y la implementación de proyectos tecnológicos.
2. Subdirección de Desarrollo de Sistemas:
 - Encargada de diseñar, desarrollar e implementar sistemas y aplicaciones que respalden la oferta de servicios electrónicos y optimicen los procesos internos.
3. Subdirección de Seguridad de la Información:
 - Responsable de implementar y mantener políticas y prácticas de seguridad de la información.

- Monitoreo constante de las amenazas de ciberseguridad y garantía de la protección de datos personales.
- 4. Subdirección de Infraestructura Tecnológica:
 - Encargada de la gestión y mantenimiento de la infraestructura tecnológica, incluyendo servidores, redes y hardware.
 - Asegura la disponibilidad y confiabilidad de los sistemas críticos.
- 5. Subdirección de Innovación Tecnológica:
 - Enfocada en la investigación y adopción de nuevas tecnologías para mejorar la eficiencia y calidad de los servicios.
 - Evaluación de tendencias tecnológicas y su aplicabilidad en la institución.

Justificación:

- La subdivisión permite una gestión más enfocada y especializada, abordando áreas clave para el cumplimiento de la misión y objetivos institucionales.
- La seguridad de la información se coloca como una prioridad, reflejando el compromiso con la protección de datos personales y el cumplimiento de las directivas del sector público.

Comparación con la Estructura Actual:

1. Fortalezas:
 - La estructura propuesta refleja una mayor especialización y enfoque en áreas críticas como seguridad de la información y desarrollo de sistemas.
 - La subdivisión permite una gestión más eficiente y orientada a resultados.
2. Desafíos:
 - Puede requerir ajustes en la actual estructura para implementar los cambios propuestos.
 - Podría implicar la necesidad de capacitación o contratación de personal especializado en las nuevas áreas.

Conclusión: La estructura propuesta mejora la alineación estratégica de la Unidad de TICs con los objetivos institucionales al enfocarse en áreas clave. Aunque podría requerir ajustes y cambios en la estructura actual, se espera que conduzca a una gestión más eficiente y efectiva de las tecnologías de la información y la comunicación en la institución. Además, el enfoque en la seguridad de la información asegura el cumplimiento de las directivas del sector público y protege la integridad de los datos gestionados por la institución.

- c) Suponga que la CGE decide realizar una auditoría integral de la estructura funcional de TICs. Elabore una matriz que le permita identificar el alcance de dicha auditoría, de acuerdo con las Normas de Control interno

La siguiente matriz proporciona una guía para identificar el alcance de la auditoría integral de la Unidad de TICs, de acuerdo con las Normas de Control Interno:

Área de Auditoría	Objetivos de Auditoría	Criterios de Auditoría	Fuentes de Evidencia
Gestión Estratégica	1. Alineación de la estrategia TICs con los objetivos institucionales.	- Revisión de documentos estratégicos y planes.	Documentos estratégicos, planes TICs.
	2. Evaluación de la contribución de TICs a la misión.	- Entrevistas con la alta dirección y personal clave.	Entrevistas, comunicaciones oficiales.
Desarrollo de Sistemas	3. Calidad y eficiencia en el desarrollo de sistemas.	- Revisiones de código, pruebas y proyectos recientes.	Revisiones de código, informes de pruebas.
	4. Cumplimiento de plazos y presupuesto en proyectos.	- Análisis de proyectos en términos de tiempo y costos.	Informes de proyectos, presupuestos.
Seguridad de la Información	5. Efectividad de las políticas de seguridad de la información.	- Evaluación de políticas y procedimientos de seguridad.	Documentación de políticas, registros de seguridad.
	6. Resiliencia frente a amenazas y gestión de incidentes.	- Análisis de incidentes anteriores y protocolos de respuesta.	Informes de incidentes, protocolos.
Infraestructura Tecnológica	7. Disponibilidad y rendimiento de la infraestructura.	- Monitoreo de sistemas, historial de tiempos de inactividad.	Registros de monitoreo, informes de rendimiento.
	8. Mantenimiento preventivo y correctivo de hardware y redes.	- Registro de mantenimiento y actualizaciones.	Registros de mantenimiento, informes de actualizaciones.
Innovación Tecnológica	9. Evaluación de la adopción de nuevas tecnologías.	- Registro de proyectos de innovación y adopción.	Informes de proyectos, registros de adopción.

Justificación:

- **Gestión Estratégica:** Evaluar la alineación estratégica y la contribución de TICs a la misión garantiza que las iniciativas tecnológicas respalden los objetivos institucionales.
- **Desarrollo de Sistemas:** Evaluar la calidad y eficiencia del desarrollo de sistemas asegura la entrega oportuna de soluciones tecnológicas efectivas.
- **Seguridad de la Información:** Auditar la seguridad garantiza la protección de datos y el cumplimiento de normativas de seguridad.
- **Infraestructura Tecnológica:** Evaluar la disponibilidad y rendimiento de la infraestructura garantiza la continuidad de los servicios.
- **Innovación Tecnológica:** Evaluar la adopción de nuevas tecnologías asegura la relevancia y eficacia de los sistemas y procesos.

Conclusión: La auditoría integral propuesta permite evaluar de manera exhaustiva la gestión de la Unidad de TICs, garantizando el cumplimiento de las normas de control interno y la eficacia en la contribución al logro de los objetivos institucionales. Los criterios de auditoría proporcionan una guía clara para la recopilación de evidencia y la identificación de áreas de mejora.

Bibliografía:

Visión / Misión / Valores – Registro Civil. (s/f). Gob.ec. Recuperado el 11 de diciembre de 2023, de <https://www.registrocivil.gob.ec/valores-mision-valores/>

Objetivos Estratégicos – Registro Civil. (s/f). Gob.ec. Recuperado el 11 de diciembre de 2023, de <https://www.registrocivil.gob.ec/objetivos-estrategicos/>

Cadena de Valor – Registro Civil. (s/f). Gob.ec. Recuperado el 11 de diciembre de 2023, de <https://www.registrocivil.gob.ec/cadena-de-valor/>

Mapa de Procesos DIGERCIC – Registro Civil. (s/f). Gob.ec. Recuperado el 11 de diciembre de 2023, de <https://www.registrocivil.gob.ec/mapa-de-procesos-digercic/>

Organigrama – Registro Civil. (s/f). Gob.ec. Recuperado el 11 de diciembre de 2023, de <https://www.registrocivil.gob.ec/organigrama/>

De, R. del R. C. 14 R. O. E. E. 822. (s/f). ESTATUTO ORGANICO POR PROCESOS DIRECCION GENERAL DE REGISTRO CIVIL. Gob.ec. Recuperado el 11 de diciembre de 2023, de https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2019/08/Estatuto_digercic_2019.pdf