MARCO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNIDAD GESTIÓN DE SERVICIOS

octubre 2021

MARCO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

INFORMACIÓN DEL DOCUMENTO

ELABORADO POR: *FECHA DE ELABORACIÓN:* *JULIO 2021*	*LIC. LEONARDO BRENES GUADAMUZ* *UNIDAD GESTIÓN DE SERVICIOS*	LEONARDO HUMBERTO BRENES GUADAMUZ (FIRMA) Firmado digitalmente por LEONARDO HUMBERTO BRENES GUADAMUZ (FIRMA) Fecha: 2021.10.28 13:17:06 -06'00'
	LIC. FLORINA ARAYA BONILLA *UNIDAD GESTIÓN DE SERVICIOS*	FLORINA MARIA ARAYA BONILLA (FIRMA) Firmado digitalmente por FLORINA MARIA ARAYA BONILLA (FIRMA) Fecha: 2021.10.28 13:49:29 -06'00'
	LIC. ROBERTO QUIRÓS GARCÍA *UNIDAD GESTIÓN DE SERVICIOS*	JOSE ROBERTO QUIROS GARCIA (FIRMA) Firmado digitalmente por JOSE ROBERTO QUIROS GARCIA (FIRMA) Fecha: 2021.10.28 11:28:48 -06'00'
	MCI. PETRONILA MAIRENA TRAÑA, ING. *JEFA UNIDAD DE GESTIÓN DE SERVICIOS*	PETRONILA DEL CARMEN MAIRENA TRAÑA (FIRMA) Firmado digitalmente por PETRONILA DEL CARMEN MAIRENA TRAÑA (FIRMA) Fecha: 2021.10.28 14:12:47 -06'00'
REVISADO POR: *FECHA DE REVISIÓN:* *AGOSTO 2021*	*LIC. JONATHAN GÓMEZ BENAVIDES* *JEFE UNIDAD DE INFRAESTRUCTURA TECNOLÓGICA*	JOHNNATAN GOMEZ BENAVIDES (FIRMA) Firmado digitalmente por JOHNNATAN GOMEZ BENAVIDES (FIRMA) Fecha: 2021.10.28 11:06:34 -06'00'
	LIC. SHIRLEY ESPINOZA VINDAS *JEFA UNIDAD DE SISTEMAS DE INFORMACIÓN*	SHIRLEY MARIA ESPINOZA VINDAS (FIRMA) Firmado digitalmente por SHIRLEY MARIA ESPINOZA VINDAS (FIRMA) Fecha: 2021.10.27 14:26:19 -06'00'
	LIC. MILAGRO SOMARRIBA MARCHENA *UNIDAD DE SISTEMAS DE INFORMACIÓN*	MILAGRO SOMARRIBA MARCHENA (FIRMA) Firmado digitalmente por MILAGRO SOMARRIBA MARCHENA (FIRMA) Fecha: 2021.10.27 10:01:20 -06'00'
	LIC. MINOR ALI GRANADOS *UNIDAD DE SISTEMAS DE INFORMACIÓN*	MAINOR ALI GRANADOS (FIRMA) Firmado digitalmente por MAINOR ALI GRANADOS (FIRMA) Fecha: 2021.10.26 19:27:03 -06'00'
APROBADO POR: *FECHA DE APROBACIÓN:* *SETIEMBRE 2021*	*LIC. EDGAR MORALES GONZÁLEZ* *DIRECTOR DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN*	EDGAR MORALES GONZALEZ (FIRMA) Firmado digitalmente por EDGAR MORALES GONZALEZ (FIRMA) Fecha: 2021.11.26 16:28:31-06'00'
OFICIALIZADO POR: *FECHA DE OFICIALIZACIÓN:* *DICIEMBRE 2021*	*DRA. PRISCILLA HERRERA GARCÍA* *DIRECTORA GENERAL DE SALUD* *DR. DANIEL SALAS PERAZA* *MINISTRO DE SALUD*	Ministerio de Salud Costa Rica ANA PRISCILLA HERRERA GARCIA (FIRMA) 2021.12.10 15:32:34 -06'00' DANIEL SALAS PERAZA (FIRMA) Firmado digitalmente por DANIEL SALAS PERAZA (FIRMA) Fecha: 2022.01.18 16:51:48 -06'00'

CONTROL DE VERSIONES

VERSIÓN	FECHA	ACTUALIZADO POR	OFICIALIZADO POR
1.0	OCTUBRE 2021	DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	MINISTRO DE SALUD

Contenido

Ilustraciones

1. Introducción

Para el Ministerio de Salud, las tecnologías de información y comunicación constituyen un apoyo imprescindible y estratégico para el buen desempeño de todas las actividades de apoyo logístico y administrativo, así como las funciones rectoras, especialmente en momentos de crisis y amenazas de enfermedades que afectan a la población. De las tecnologías de información y comunicación dependen todos los procesos institucionales para su buen funcionamiento y desempeño; así como para obtener el análisis de la información que soporte la toma de decisiones gerenciales y operacionales.

El desarrollo de un Marco de Gestión de Tecnologías de Información y Comunicación del Ministerio de Salud alineado a la estrategia institucional, mediante un enfoque integrado y global para mejorar los procesos, el desarrollo de estrategias de ejecución y gestión de las TIC y todos los recursos involucrados es de fundamental importancia.

En este punto una buena gobernanza y gestión de las tecnologías de información y comunicación, donde cumple un rol trascendental el director de TI, conocido de forma habitual como CIO (Chief Information Officer), quien está llamado a desempeñar un papel influyente, como responsable de implementar un conjunto de buenas prácticas de gobierno y de gestión de las diferentes áreas relacionadas con la prestación de servicios, infraestructura tecnológica, mantenimiento y desarrollo de software, administración y configuración de la seguridad, entre otros.

Aunado a lo anterior, el equipo que le acompaña en su gestión debe poseer además de las habilidades técnicas y de experiencia adecuadas en gestión del cambio, gestión de equipos de trabajo, resolución asertiva de conflictos, gestión efectiva del tiempo, técnicas de negociación, establecimiento de acuerdos, capacidad de investigación y autoaprendizaje, así como el compromiso, voluntad y proactividad para la innovación y aplicación de las tecnologías disruptivas.

El marco de gestión de las tecnologías de información y comunicación del Ministerio de Salud de Costa Rica es un documento de consulta y aplicación obligatoria que establece y define una serie de componentes que orientan el desarrollo e impulsan estrategias para la utilización eficiente de los recursos tecnológicos e informáticos de la institución en sus tres niveles de gestión a través de políticas, procedimientos y lineamientos con el objetivo de generar valor mediante la gestión de la infraestructura tecnológica, los sistemas de información y mejorar la calidad y transparencia de los servicios que se ofrecen a los usuarios internos y la ciudadanía en general.

Con el auge tecnológico y el uso vertiginoso de las TIC en todos los campos de la vida diaria, la Institución debe estar preparada para enfrentar la sustracción o manipulación de información, sabotaje, suplantación de identidad, redireccionamiento de dominios, entre otras acciones delictivas cibernéticas que deben contrarrestarse; asimismo se

considera de vital importancia elaborar esquemas preventivos en materia de gestión de tecnologías de información y comunicación, identificar los riesgos de los recursos tecnológicos críticos, definir mecanismos de control de esos riesgos, proyectar y planificar las inversiones en tecnología de información, priorizar y ejecutar proyectos que generen valor e interoperen para toma de decisiones basadas en evidencia e inteligencia de datos, sin dejar de lado el salvaguardar los equipos y proteger el acceso a los datos almacenados en ellos, con el fin de garantizar la seguridad de la información.

Este documento debe ser revisado y actualizado en todos sus componentes una vez cada cuatro años, con la conducción y apoyo del máximo jerarca y sus titulares subordinados, a fin de garantizar que la gestión de las tecnologías de información y comunicación permanezca alineada con los objetivos estratégicos institucionales.

Ante un eventual incumplimiento de lo establecido en cada uno de los componentes del presente documento, se actuará de conformidad con el régimen disciplinario vigente, el Reglamento Autónomo de Servicios del Ministerio de Salud y las leyes correspondientes.

2. Objetivo General

Determinar los componentes del marco de gestión de tecnologías de información y comunicación del Ministerio de Salud, mediante la implementación de un conjunto de buenas prácticas de gestión de las TIC para garantizar la mejora continua en los servicios, infraestructura tecnológica y sistemas de información acorde con los objetivos institucionales.

2.1 Objetivos Específicos

- Identificar y actualizar los componentes del marco de gestión de tecnologías de información y comunicación a fin de que permanezcan vigentes, operativos, alineados a la normativa institucional y nacional.
- Garantizar la eficiencia y la utilización adecuada de los recursos, mediante el desarrollo y establecimiento de las pautas necesarias a los usuarios internos y externos del Ministerio de Salud en el uso de las tecnologías de información y comunicación,
- Velar que los sistemas de información sean eficientes, interoperables, funcionales, flexibles y que proporcionen seguridad, integridad, disponibilidad y oportunidad de la información.
- Procurar que la infraestructura tecnológica institucional cumpla con los requerimientos de rendimiento y desempeño para facilitar el acceso a los servicios de manera confiable, oportuna y segura.
- Coordinar y proponer oportunamente la adquisición y distribución de los recursos

de tecnologías de información y comunicación, acorde con diagnósticos de necesidades detectadas y el cumplimiento de buenas prácticas administrativas, legales y técnicas.

- Establecer las consideraciones generales de calidad que permitan la evaluación, control y seguimiento durante las diferentes etapas de los proyectos en materia de tecnologías de información y comunicación, con el fin de asegurar la mejora continua.
- Definir e implementar medidas de seguridad informática, seguridad de la información y ciberseguridad que involucre la detección, corrección y mitigación del riesgo sobre la disponibilidad, integridad y confidencialidad de la información, así como evitar la modificación o divulgación no autorizada, posible pérdida de información o de activos.
- Identificar y administrar los riesgos asociados a los recursos de tecnologías de información y comunicación, para tomar las medidas necesarias y lograr minimizar riesgos.

3. Alcance

Este marco de gestión debe ser de consulta y acatamiento obligatorio para todos los usuarios y funcionarios, que hagan uso de las tecnologías de información y comunicación del Ministerio de Salud.

4. Estructura y organización de las Tecnologías de Información y Comunicación

El 13 de octubre del 2014, mediante el oficio DM-379-14, se aprueba la supresión de la Unidad de Gestión Integral de la Información (UGII) y la creación de una nueva unidad organizacional con rango de Departamento denominada “Departamento de Tecnologías de Información y Comunicación” en adelante DTIC, con dependencia jerárquica del Despacho Ministerial y con una desagregación de tres unidades organizacionales, a saber: Unidad de Gestión de Servicios, Unidad de Sistemas de Información y Unidad de Infraestructura Tecnológica.

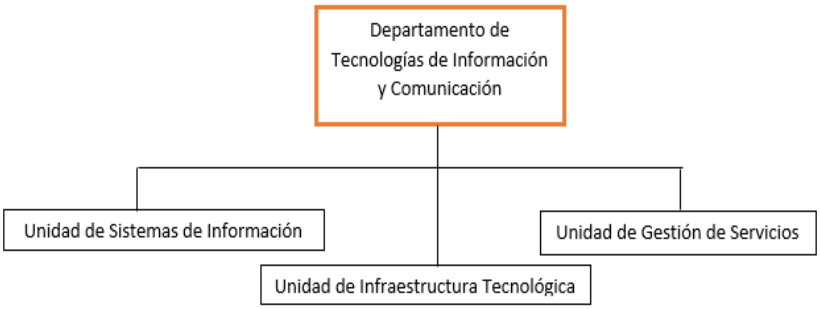

Ilustración 1. Organigrama del DTIC

Posteriormente, mediante el decreto 41999-S de la Gaceta N°209 del 4 noviembre 2019, correspondiente a la Reforma del Reglamento Orgánico del Ministerio de Salud, pasa a depender de la Dirección General de Salud.

Ilustración 2. Dependencia jerárquica del DTIC

El objetivo del DTIC, es garantizar que las tecnologías de información y comunicación respondan a las necesidades institucionales mediante el desarrollo y mejoramiento continuo de la seguridad, disponibilidad, integridad y oportunidad de los sistemas de información, la infraestructura y los servicios, a fin de fortalecer la Rectoría y la toma de decisiones.

4.1 Gestión de las Tecnologías de Información y Comunicación

Las funciones del proceso de nivel cero correspondiente a la gestión de las tecnologías de Información y Comunicación, llevadas a cabo por el DTIC y sus unidades organizativas; están definidas en el Manual de Organización y Funciones del Ministerio de Salud, publicado en enero 2020.

Cada una de estas funciones son convertidas en servicios, los cuales se identifican y detallan en el Catálogo de Servicios TIC y su ejecución se rige mediante procedimientos y lineamientos.

4.2 Comité Gerencial de TIC

El Comité Gerencial de TIC es el órgano asesor consultivo del máximo Jerarca del Ministerio de Salud en materia de tecnologías de información y comunicación, encargado de la administración de los recursos humanos, materiales y financieros, basado en el Plan Estratégico Institucional (PEI) y Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) para la priorización de proyectos informáticos según los requerimientos de automatización de las actividades administrativas y operativas institucionales, formulación de políticas, estándares y directrices relativas a la gestión del DTIC y toma de decisiones estratégicas de tecnologías de Información y comunicación.

Mediante el Decreto Ejecutivo Nº 32564-S del 20 de junio de 2005 publicado en La Gaceta Nº 167 del 31 de agosto de 2005, se creó el Comité Gerencial de Informática del Ministerio de Salud.

Posteriormente con el Decreto Ejecutivo Nº 38727-S del 30 de setiembre de 2014 publicado en La Gaceta Nº 29 del 11 de febrero de 2015, se deroga el Decreto Ejecutivo Nº 32564-S, que menciona en el Considerando V “que sea el Consejo Ministerial quién asuma las responsabilidades indicadas en el punto 1.6. de las normas N-22007-CO-DFOE "Normas Técnicas Para La Gestión y El Control De Las Tecnologías de Información de la Contraloría General de la República"

Posteriormente, mediante la Resolución R-DC-17-2020 emitida por la Contraloría General de la República, sugiere a las instituciones la conformación de un Comité Gerencial de Tecnologías de Información.

El Comité Gerencial de Tecnologías de Información y Comunicación del Ministerio de Salud (CGTICMS) debe estar debidamente conformado por:

- Dirección General de Salud, quien lidera y representa a todas las direcciones del nivel central y el nivel regional
- Departamento de Tecnologías de Información y Comunicación, quien coordina, ejecuta y operativiza las decisiones del CGTICMS
- Dirección Administrativa, quien determina los recursos para priorizar y atender las necesidades institucionales
- Dirección Jurídica, quien asesora en materia legal la ejecución de los proyectos tecnológicos
- Dirección de Planificación, alinea los proyectos tecnológicos a los objetivos estratégicos de la institución

Este CGTICMS debe ser oficializado por el máximo Jerarca de la institución, sesiona mensualmente y comunica de previo la agenda.

5. Componentes del Marco de Gestión TIC

5.1 Gestión del procesamiento y almacenamiento de datos e información

Este componente cobra relevancia histórica en la terminología computacional, desde el surgimiento del concepto de dato e información, un dato es cualquier número o caracter que puede representar los valores de una medición o fenómeno observable y la información es el conjunto de esos datos agrupados por características determinadas por la misma observación.

El procesamiento de datos es la acción de analizar los datos y convertirlos en información valiosa para la toma de decisiones, el almacenamiento de datos se refiere a las herramientas que se emplean para almacenar los datos.

Actualmente, se puede realizar el procesamiento de forma automatizada, gracias a sistemas basados en algoritmos cada vez más sofisticados, que se van autoperfeccionando con la información extraída de las tres fases principales en el procesamiento de datos:

a) Selección de datos

No todos los datos tienen valor (o al menos, no el mismo valor), depende de su veracidad calidad y fiabilidad, pero también de su finalidad y de la estrategia particular utilizada.

Por eso, es importante trabajar con herramientas que hagan la selección de los datos a tratar, de forma automática, dados los volúmenes y la velocidad con que se reciben. Buscar la forma de capturar el dato mediante las tecnologías disponibles, para mitigar el mínimo error en esa captura.

b) Agrupación de datos

Una vez con los datos de valor, estos deben agruparse para que tengan sentido. Un dato suelto no provee información de calidad, pero un conjunto de datos sí brinda información relevante sobre muchos aspectos. Es aquí donde importa la selección de un buen sistema administrador de bases de datos que proporcione la tecnología y robustez para modelar, codificar y transformar esos datos.

c) Análisis de datos

Con los datos ya agrupados, se genera información, mediante el análisis de esos grupos se obtiene significado de esa información, y se consigue conocer aspectos fundamentales, tales como perfiles de usuarios, notificaciones, sexo, lugares geográficos, descripción de enfermedades, resultados de laboratorio, identificar algunas oportunidades y opciones de mejora, así como conocer los puntos fuertes o débiles en los procesos institucionales.

Para este análisis deben considerarse tecnologías como el “big data” o datos masivos, el “machine learning” o aprendizaje automático y el “business intelligence” o inteligencia de

negocios en sus distintas formas de implementarla según la información y las necesidades institucionales.

Estos datos convertidos en información relevante necesitan almacenarse para poder disponer de estos en algún momento, aquí la importancia del “bit” y el “byte” como unidades básicas de almacenamiento de datos en una base de datos y en un medio físico o lógico haciendo uso de diferentes tecnologías emergentes, disruptivas e innovadoras para generar valor a la institución.

Para conocer esos volúmenes de datos y trabajar en su agrupación y velocidad de procesamiento se requiere el establecimiento de un modelo de arquitectura de información que le permita al Ministerio de Salud conocer y disponer de un conjunto de datos e información procesada y almacenada agrupada y gestionada por los procesos y subprocesos institucionales.

Con un modelo de arquitectura de información establecido y actualizado constantemente según los cambios organizacionales y del entorno tecnológico, se pueden tener mapeadas todas las entradas, procesamiento y salidas de información por distintos medios y formatos, cumpliendo con la normativa vigente de apertura de datos, accesibilidad y experiencia de usuario; así como planificar los escenarios de captura, depuración, integridad, modelado, análisis de datos, disposición y recuperación de estos, que posibilite a los sistemas de información e infraestructura tecnológica, generar valor para las distintas unidades organizativas en su quehacer y toma de decisiones. Asimismo, identificar servicios nuevos o mejorar los existentes, establecer estándares y metodologías ágiles de trabajo para capturar, procesar y almacenar esos datos.

Este modelo de arquitectura de información del Ministerio de Salud facilita la planificación operativa de actividades que generen valor en el cumplimiento de los objetivos estratégicos institucionales (PEI), derivados de los objetivos del desarrollo sostenible (ODS) y los objetivos del Plan Nacional de Desarrollo (PND), asimismo en con el plan estratégico de TIC (PETIC) y el Plan Operativo Institucional (POI) del DTIC.

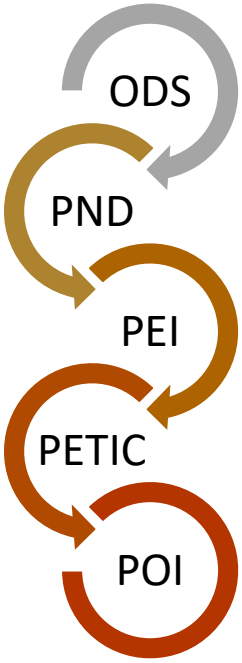

Ilustración 3. Planes estratégicos institucionales

Una vez establecido el modelo y mediante su implementación gradual es importante considerar el aseguramiento de la seguridad o ciberseguridad de esos datos e información almacenados.

5.2 Modelo de Arquitectura de Información

El Modelo de Arquitectura de Información es la esquematización completa y detallada de los datos e indicadores en los sistemas institucionales y el flujo de información que opera sobre la infraestructura tecnológica, es decir, comprende el modelo de los datos institucionales que proporcionan información, considerando la información como un todo, un elemento integral donde confluyen la información por distintos medios para proveer evidencia del quehacer organizacional y apoyar la toma de decisiones oportunas y confiables.

El modelo de arquitectura de información está ligado a la gestión de la calidad de la información, a la planificación y organización estratégica de las tecnologías de la información, al enfoque y mapeo de procesos, la gestión documental y la gestión archivística de la institución.

Este concepto de Información como un componente integral dentro de la institución, es

lo que da una visión global del flujo de información que apoya la toma de decisiones gerenciales.

El modelo de arquitectura de información debe contar con el apoyo de las autoridades institucionales para asignación de los recursos financieros, humanos, logísticos y funcionales para su elaboración, implementación, mantenimiento y actualización permanente.

El establecimiento de un modelo de arquitectura de información le permite al Ministerio de Salud contar con una herramienta orientada a la obtención de información acerca de sus procesos actuales y futuros, así como las aplicaciones y bases de datos que soportan la información de dichos procesos; todo ello como un insumo para la planificación y toma de decisiones tanto estratégicas como tecnológicas, que le permitan contribuir con el desarrollo y cumplimiento de los objetivos institucionales.

En resumen, el modelo de arquitectura de Información institucional constituye una caracterización de todos los datos relevantes de la institución para cumplir con su misión y visión. Es de utilidad para planificar y dimensionar los proyectos de desarrollo de software y aplicaciones interoperables, por lo que es una función donde el proceso de gestión de tecnologías de información y comunicación coordina con otras unidades organizativas de la institución, para su elaboración, análisis y actualización permanente.

5.2.1 Fases del Modelo de Arquitectura de Información

Para la elaboración, implementación y mantenimiento de un modelo de arquitectura de información, se deben considerar una serie de fases:

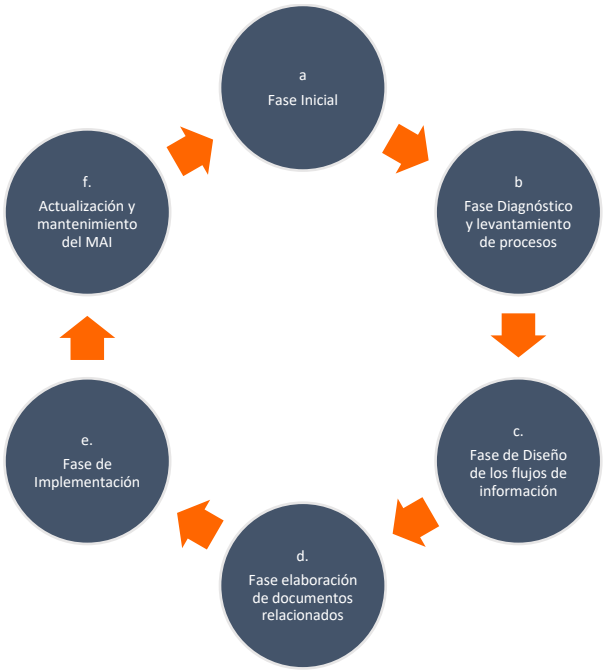

Ilustración 4. Fases de Modelo de Arquitectura de Información

a) Fase Inicial

1. Definir y nombrar un equipo de trabajo responsable de la planificación, elaboración, mantenimiento y actualización permanente del modelo de arquitectura de información institucional.
2. Revisar el marco regulatorio interno y nacional vigente
3. Definir un plan de trabajo, con actividades y fechas de ejecución propuestas.
4. Incluir en el Plan Estratégico de Tecnologías de la Información y Comunicación del Ministerio de Salud vigente y el Plan Operativo Institucional, las actividades que corresponden al establecimiento de un Modelo de Arquitectura de Información y gestión de la calidad de la información, para definir recursos y contar con el apoyo conjunto de las otras unidades organizativas si se requiere.

b) Fase Diagnóstico y levantamiento de procesos

1. Identificar los procesos y subprocesos institucionales con los datos relevantes.

2. Crear plantillas y herramientas de trabajo para el levantamiento y diagnóstico de los datos relevantes por proceso.
3. Solicitar el llenado de las plantillas y herramientas de trabajo a las distintas unidades organizativas
4. Recopilar y consolidar la información de las plantillas y herramientas de trabajo para dar inicio al mapeo de los datos según procesos.
5. Analizar cada uno de los procesos y subprocesos.

c) Fase de Diseño de los flujos de información

1. Elaborar, documentar y diseñar el flujo de información según el mapeo y análisis de los datos de los procesos y subprocesos institucionales
2. Revisar y actualizar los flujos de información.
3. Diseñar el diagrama completo

d) Fase elaboración de documentos relacionados

1. Elaborar criterios sobre estructuras de datos y flujo de información para sistemas institucionales automatizados y no automatizados según el mapeo de datos.
2. Crear los documentos relacionados que se requieran, políticas o lineamientos para adaptar los sistemas institucionales y corregir o mejorarlos según el flujo de información del modelo respecto al mapeo de datos de los procesos y subprocesos institucionales.

e) Fase de Implementación

1. Publicar y divulgar en intranet, el modelo de arquitectura de información.
2. Elaborar un plan de revisión del modelo y estructuras de datos de los sistemas institucionales actuales para que generen valor a la toma de decisiones.
3. Realizar revisiones del flujo de información en sistemas institucionales en producción y desarrollo para emitir criterios de realizar mejora o modificación según el modelo de arquitectura de información.
4. Describir la forma en que los datos son creados, almacenados, transportados y entregados por los procesos y servicios de la institución.
5. Describir la recepción y entrega de datos por parte de terceros.
6. Identificar el nivel de confidencialidad y tipo de acceso según los roles (o tipos de personas) que los utilizan.

7. Elaborar las políticas de privacidad para los sistemas de información o bases de datos que sean sensibles de confidencialidad y protección de datos personales.
8. Establecer los mecanismos para asegurar y garantizar la seguridad o ciberseguridad de los datos e información, tema que se ampliará en el componente de seguridad y ciberseguridad.

f) Actualización y mantenimiento del MAI

1. Dar seguimiento a la ejecución del plan de trabajo con el fin de reorientar esfuerzos o incorporar otras actividades que surjan del análisis
2. Realizar mejora continua y actualización permanente del Modelo de Arquitectura de Información Institucional.
3. Hacer revisiones periódicas o auditorías de control al flujo de información de los procesos institucionales y validarlo con los sistemas de información en producción.

5.3 Gestión de la calidad

La gestión de la calidad es un compromiso con los usuarios, donde los bienes y servicios en materia de TIC deben ser de conformidad con los requerimientos y planes estratégicos basados en un enfoque de eficiencia y de mejoramiento continuo.

Los funcionarios internos, proveedores externos y personal del DTIC deben aplicar las siguientes recomendaciones para lograr estándares en la calidad de los bienes y servicios TIC:

Para los funcionarios del Ministerio de Salud

a)Comprometerse con el personal del DTIC en la realización de proyectos.
b)Aplicar la normativa interna vigente en materia TIC.
c)Responder a encuestas de satisfacción de forma objetiva.
d)Utilizar los medios oficiales de comunicación: soporte@misalud.go.cr y teams para la atención de incidentes o solicitudes.
e)Utilizar los bienes y servicios TIC únicamente para labores institucionales

Para proveedores de servicios

a)Mantener una comunicación eficiente y transparente con el personal del DTIC.
b)Apegarse a las buenas prácticas internacionales y normativa interna vigente en materia de TIC.
c)Implementar, mantener y seguir medidas técnicas y organizativas de seguridad institucionales.

Para el personal del DTIC

a)Crear un compromiso con la calidad.
b)Ejecutar las funciones apegados a la normativa vigente.
c)Asegurar los recursos tecnológicos necesarios para brindar productos y servicios de calidad.
d)Capacitar a los usuarios internos con el objetivo de optimizar el uso de los bienes y servicios de TIC.
e)Investigar nuevas tecnologías de punta.
f)Implementar oportunidades de mejora, como resultado de la aplicación de herramientas de opinión a los usuarios de los servicios que se brindan.
g)Atender tiquetes emitidos por el Centro de Servicios según los acuerdos de nivel de servicio (SLA) definidos.
h)Dar seguimiento exhaustivo de todas las contrataciones externas.
i)Garantizar los atributos que aseguran la calidad de la información.

Ilustración 5. Aspectos para la gestión de la calidad

El control de la calidad se realiza por medio de mecanismos y herramientas para evaluar y detectar errores, riesgos u oportunidades de mejora, con el fin de asegurar el seguimiento efectivo de indicadores, cumplimiento de objetivos y planes institucionales.

5.4 Seguridad y Ciberseguridad

La seguridad es un componente fundamental en la gestión TIC, el cual ha llegado a especializarse en seguridad informática, seguridad de la información y ciberseguridad, apoyada en metodologías y principios básicos, que son los siguientes:

Minimizar el riesgo de ataque	*Establecer valores predeterminados seguros*	*Principio de privilegio mínimo*	*Desconfiar en los servicios adquiridos*	*Principio de defensa en profundidad*	*Separación de tareas*
• Reducir la cantidad de elementos que convergen en una misma aplicación.	• Considerar experiencia de seguridad para los usuarios.	• Definir privilegios (derechos y permisos) según los recursos que requiera el usuario.	• Elaborar estándares para la administración de los servicios contratados a terceros.	• Implementar mecanismos de control en diferentes niveles que contribuyan a evitar un riesgo.	• Realizar la asignación de roles según el perfil de cada usuario.

Ilustración 6. Principios básicos para la gestión de la seguridad

Además de los principios básicos, se considera la transversalidad de las TIC, la cual se refiere a aquella colaboración de la tecnología con las diversas ramas del conocimiento, de forma tal que es posible crear soluciones y propuestas de valor mediante una colaboración en conjunto.

La seguridad de la información contempla los siguientes aspectos:

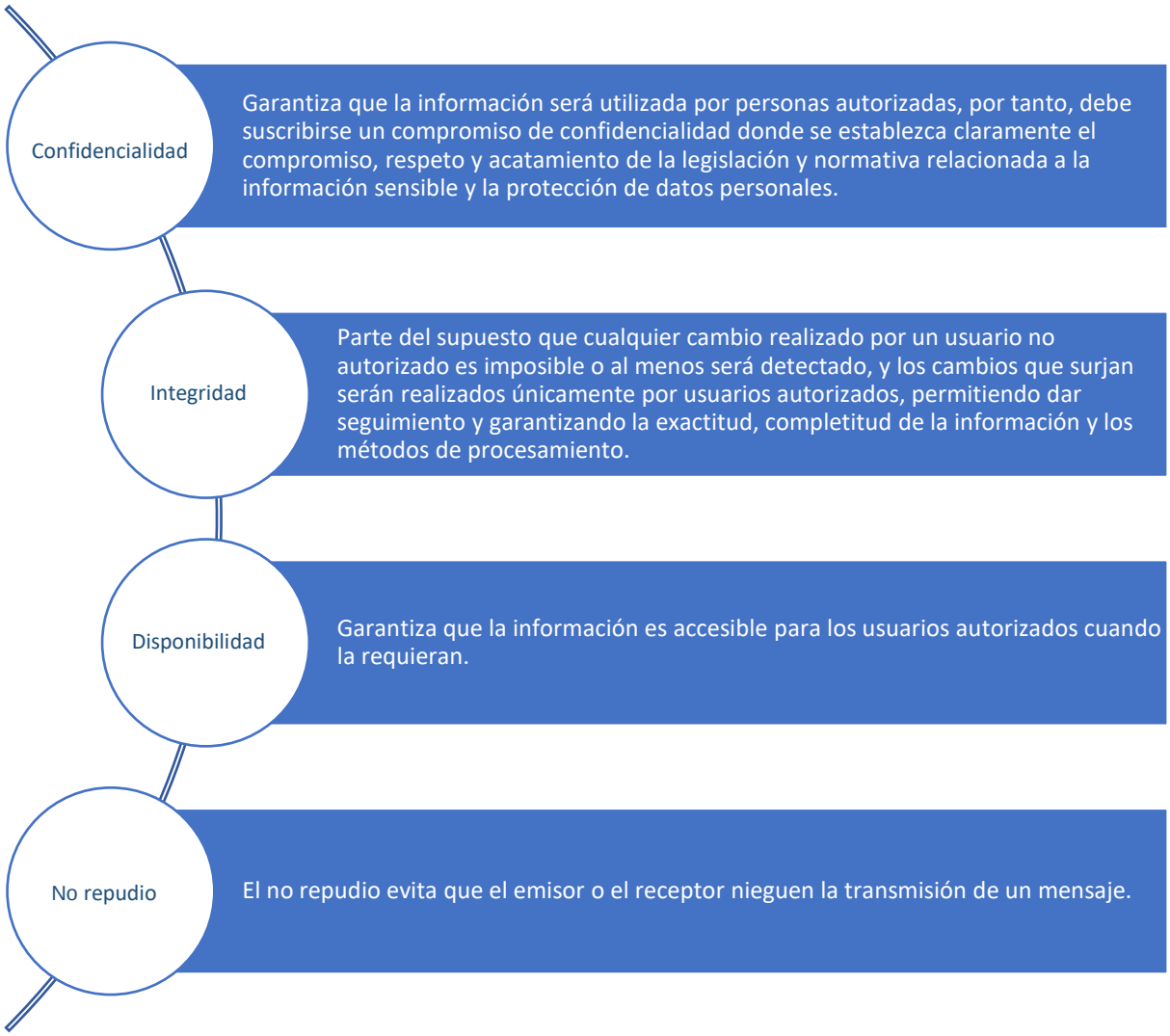

Ilustración 7. Principios de la seguridad de la información

La seguridad informática y la seguridad de la información contemplan los siguientes elementos:

Organización de la seguridad de la información	•Se deben definir los roles y responsabilidades para la gestión del riesgo basados en los objetivos del proyecto e institucionales
Seguridad en recursos humanos	•Se debe contar con planes de capacitación e inducción, orientados a aspectos de seguridad de las TIC
Gestionar los activos	•Todos aquellos recursos como: sistemas, infraestructura, bases de datos y recurso humano se deben identificar y administrar según los objetivos institucionales.
Gestión de la autenticación y control de acceso	•Se debe mantener un control de acceso a todos los activos físicos y lógicos, así como de las instalaciones conforme al rol definido a cada usuario
Criptografía	•Toda aquella información de acceso restringido requiere la utilización de usuario y contraseña y utilizar el cifrado no reversible para garantizar la integridad y confidencialidad de la información.
Seguridad de sitios y equipos de la organización	•Se deben establecer las medidas de control físicas y lógicas las cuales garanticen la protección de los activos e información
Comunicaciones seguras	•Se deben implementar los controles que aseguren la infraestructura de la red con el fin de la protección de la información que viaja mediante ella.
Adquisición, desarrollo y soporte de sistemas de información	•Los proyectos de software que se realizan o que se les brinda mantenimiento deben mantener las mejores prácticas de seguridad aplicables
Protección de datos	•Toda aquella información que se encuentra bajo el amparo de la ley de protección de datos se debe resguardar en apego a lo establecido en la normativa vigente
Protección ante código malicioso	•Implementar medidas que permitan el correcto uso de las aplicaciones o plataformas para mitigar la inclusión de código o software malicioso

Ilustración 8. Aspectos de la seguridad informática y la seguridad de la información

La ciberseguridad, por su parte es la implementación de una serie de buenas prácticas con el fin de proteger las computadoras, servidores, sistemas, dispositivos móviles, redes y los datos en tránsito de cualquier tipo de ataque. Para logra una robusta seguridad se

deben incorporar los siguientes elementos:

Controles a nivel de aplicación	•Implementar el inventario del software oficial, el cual debe ser actualizado periódicamente para garantizar que el mismo aún es soportado por el fabricante
Protección de servidores	•Mantener una actualización frecuente en los controladores, sistemas operativos, firmware, aplicaciones y dispositivos con el fin de reducir las vulnerabilidades
Listas de software autorizado	•Contar con un listado del software autorizado para la instalación y uso, el cual incentive la seguridad de la información, así como la plataforma tecnológica
Gestión continua de riesgos de ciberseguridad	•Realizar una verificación periódica de vulnerabilidades, principalmente en la plataforma web para la minimización de riesgos externos
Privilegios administrativos	•Aplicación de políticas para la creación de contraseñas de acuerdo a los perfiles de cada usuario
Protecciones de correo electrónico y navegadores Web	•Contar con herramientas que permitan el filtrado de: contenidos, de nombres, dirección IP, DNS, palabras clave que permita regular el acceso a sitios.
Protección contra software malicioso	•Todos los sistemas y hardware deben de contar con sistemas de protección de amenazas los cuales garanticen la mitigación de las vulnerabilidades.
Control y limitación de puertos de red, protocolos y servicios	•Implementar la protección perimetral en todos los dispositivos y la red de datos como: inactivación de puertos no usados entre otros
Configuración segura de dispositivos de red	•Estandarización de las configuraciones de los equipos de red, como elemento minimizador del riesgo
Defensa perimetral	•Contar con sistemas para la detección y la prevención de intrusos para mantener un monitoreo constante del tráfico y detectar condiciones irregulares en la red organizacional
Controles de acceso para redes inalámbricas	•Establecer elementos de seguridad para el acceso a la red institucional, que garantice a cada usuario conectado, acceso a la información según sus permisos

Ilustración 9. Elementos de la ciberseguridad

Corresponde al DTIC elaborar las políticas, procedimientos y lineamientos que involucren los mecanismos de control para afirmar la seguridad y ciberseguridad de la información.

5.4.1 Privacidad de la información

La protección de datos, también llamada privacidad de información es el aspecto de las TIC que se ocupa de la capacidad que tiene la institución o usuario, para determinar qué datos en un sistema de información pueden ser o no compartidos con terceros.

Actualmente la tecnología permite medidas para garantizar la privacidad y el acceso seguro a la información, como la autenticación en dos pasos o factores, en la cual se utilizan dos elementos: contraseña y una notificación por un medio electrónico.

Corresponde al DTIC, elaborar las políticas, procedimientos y lineamientos que involucren los mecanismos de control para asegurar la privacidad y protección de los datos.

5.4.2 Seguridad de documentos electrónicos

El Ministerio de Salud cuenta con tres tipos de documentos: papel, digitalizado y el digital. El primero corresponde a los documentos físicos, el segundo se refiere a los documentos que nacen en papel y luego son digitalizados y el último cuyo origen es digital.

Cualquier esquema de seguridad de información que trabaje con documentos electrónicos, sean digitales o digitalizados, deben estar en la capacidad de proteger tanto sus dimensiones como sus propiedades. Los aspectos más importantes a considerar en la protección de documentos electrónicos son:

Ilustración 10. Aspectos para la protección de documentos electrónicos

Los aspectos que se deben considerar como mecanismos de control son:

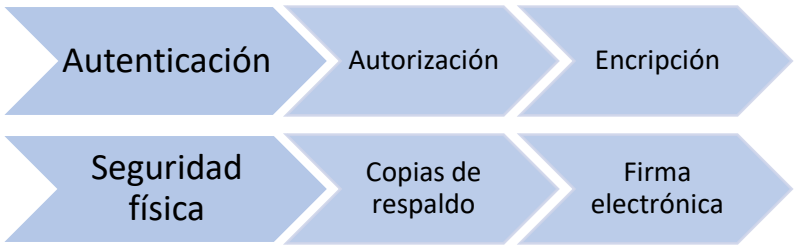

Ilustración 11. Mecanismos de control para documentos electrónicos

5.4.3 Firmas y certificados digitales

La firma digital es un método que asocia la identidad de una persona o equipo, con un mensaje o documento electrónico, para asegurar la autoría y la integridad de este.

Para verificar la firma se tiene que validar la vigencia del Certificado Digital del firmante, el estado del certificado digital (si está revocado) y que el uso del certificado digital sea el apropiado para la operación realizada (firma y no repudio) mediante una Entidad Certificadora Autorizada.

Los funcionarios del Ministerio de Salud deben aplicar las siguientes medidas de seguridad para el uso de la firma digital:

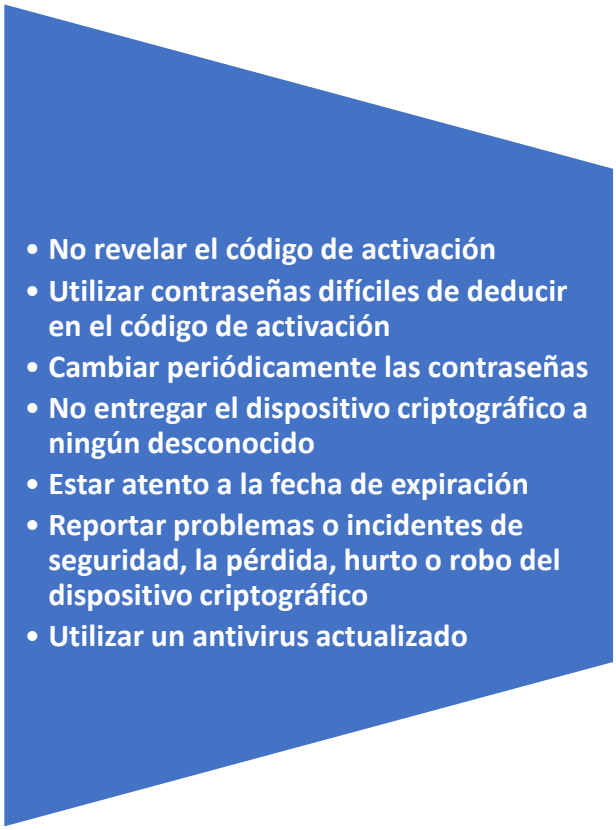

Ilustración 12. Buenas prácticas para uso de firma digital

El Ministerio de Salud debe apegarse a la normativa nacional vigente en materia de firmas y certificados digitales, a través de la entidad certificadora nacional y sus medios de soporte.

5.4.4 Portal web

El portal web institucional es el punto de acceso central amigable a una serie de servicios, una sección de noticias de actualidad e información general y de interés primordial, además de enlaces para que los distintos usuarios y funcionarios puedan interactuar con las páginas, sitios, subsitios y secciones de contenido web sobre temas específicos de interés nacional y de las funciones rectoras del Ministerio, así mismo en todo momento se consideran aspectos de transparencia, datos abiertos, usabilidad y accesibilidad.

Los funcionarios tienen acceso desde el portal al correo institucional, espacio de información sobre el teletrabajo, la intranet, las encuestas electrónicas y al campus virtual del Ministerio de Salud.

El portal institucional es responsivo, puede ser visto desde cualquier dispositivo electrónico inteligente como: tableta, teléfono, microcomputadora u ordenador personal.

Corresponde al DTIC, elaborar los procedimientos y lineamientos que involucren los mecanismos de control para asegurar la disponibilidad, accesibilidad y usabilidad del Portal Web Institucional.

5.5 Gestión del riesgo

La gestión del riesgo es fundamental para asegurar la continuidad de las operaciones, la protección de la información, los bienes institucionales y el valor de los servicios brindados. Para la gestión efectiva de los riesgos en los servicios, infraestructura y sistemas de información se debe proceder con su identificación, evaluación o diagnóstico y la forma de gestionarse para determinar planes de acción y seguimiento.

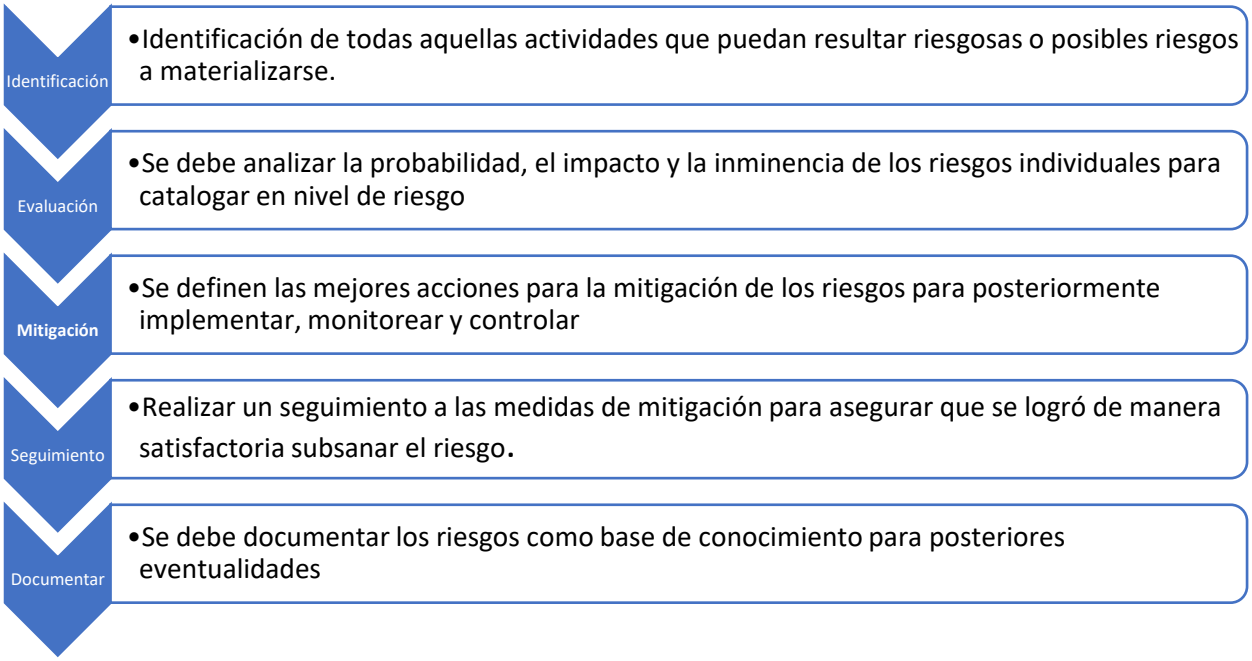

Ilustración 13. Gestión del riesgo

El Ministerio de Salud cuenta con el procedimiento **MS.UO.LI.06.04 Administración de Riesgos,** el cual establece la transparencia y claridad de las actividades, roles, responsabilidades y rendición de cuentas de los funcionarios a cargo, además del seguimiento respectivo.

Los riesgos deben ser vistos como oportunidades de mejora, principalmente en el fomento del aprendizaje, innovación, logro de objetivos y el apoyo en la gestión de incidentes.

5.6 Administración y gestión de proyectos

La administración de proyectos es una responsabilidad compartida entre el DTIC y las unidades organizativas dueñas o solicitantes de un proyecto, para garantizar un seguimiento efectivo, mediante la organización y estandarización de las actividades llevadas a cabo y el cumplimiento de tiempos de entrega, la calidad del servicio brindado y la mitigación oportuna de riesgos de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo óptimo, además del presupuesto preestablecido.

Para una auténtica y objetiva administración y gestión de los proyectos, se deben establecer un conjunto de buenas prácticas que indican el papel de los responsables y las actividades que deben llevarse a cabo.

Corresponde al Comité Gerencial TIC, girar instrucciones y priorizar los proyectos institucionales relacionados con las tecnologías de información y comunicación. Al DTIC le corresponde ejecutar los proyectos en conjunto con las unidades organizativas solicitantes, a fin de incorporar los mecanismos de control necesarios para asegurar el éxito de cada proyecto.

5.6.1 Gestión de proyectos

Es la función o enfoque gerencial que permite tener un mayor control sobre los riesgos asociados y el cumplimiento de los objetivos de los proyectos, para lo cual se debe definir una metodología con base en mejores prácticas, con el objetivo de lograr los productos esperados, en términos de alcance, tiempo, costo y calidad.

Desde el punto de vista del proyecto, se debe identificar, definir, combinar y coordinar apropiadamente aspectos como experiencia, lógica y dinámica relacionada a la naturaleza del proyecto para poder concluirlo satisfactoriamente.

Fases para considerar en la realización de proyectos:

- **Iniciación:** Se define y autorizan el proyecto o una fase de un proyecto.
- **Planificación:** Definición de los objetivos, el alcance y el curso de acción.
- **Ejecución:** Desarrollo de las acciones para el cumplimiento de los objetivos planificados del proyecto.
- **Seguimiento y Control:** Evaluación y supervisión del avance, con el objetivo de identificar variaciones, riesgos y tomar las medidas correctivas y preventivas a tiempo.
- **Cierre:** Este proceso verifica que se hayan finalizado formalmente todas las etapas del proyecto.

Ilustración 14. Fases de la realización de proyectos

5.7 Gestión de infraestructura tecnológica

La infraestructura tecnológica se rige por los planes estratégicos institucionales, además por los principios de integración y de estandarización para lograr la satisfacción de los requerimientos institucionales, mediante la planificación, adquisición y administración de los recursos TIC.

El DTIC asesora, emite y ejecuta recomendaciones técnicas, con el propósito de garantizar el adecuado funcionamiento de las comunicaciones, la protección de equipos y de la información en ellos contenida, basado en las normas de salud ocupacional, seguridad física y normas internacionales aplicables.

La gestión de la infraestructura de TIC es la coordinación de todos los recursos, los sistemas, las plataformas, las personas y los entornos de TI, que debe considerar los siguientes temas:

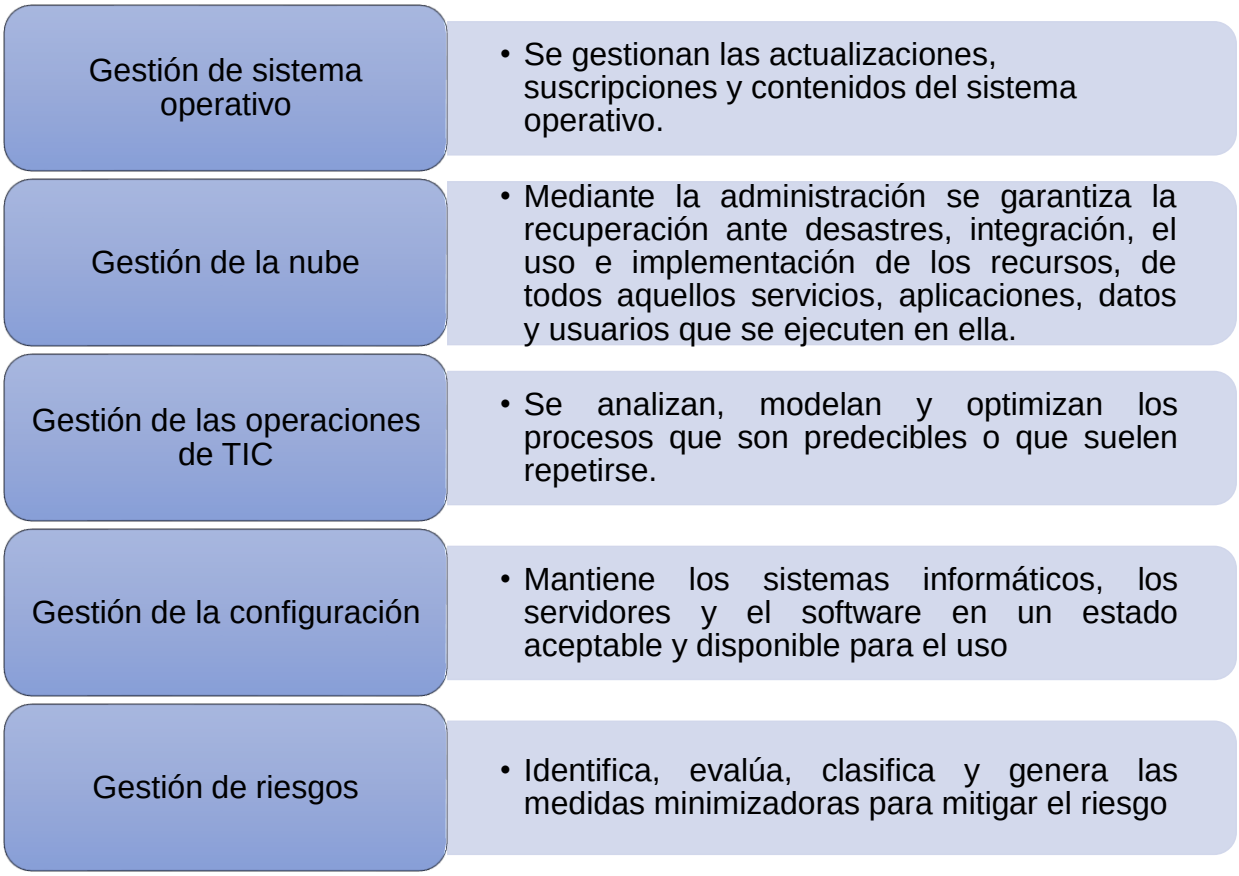

Ilustración 15. Aspectos de la gestión de infraestructura tecnológica

El DTIC debe elaborar los procedimientos y lineamientos que involucren los temas de gestión de la infraestructura tecnológica.

5.8 Gestión de redes de telecomunicación

La gestión de redes abarca muchos aspectos, como por ejemplo el despliegue, integración y coordinación del hardware, software y los usuarios para monitorizar, probar, investigar, configurar, analizar, evaluar y controlar los recursos de una red para conseguir niveles de trabajo y de servicio adecuados a los objetivos institucionales.

Es necesario establecer mecanismos adecuados para el uso de la red de datos institucional, con base en las telecomunicaciones, metodologías, procesos, técnicas y servicios, que puedan resultar útiles para la institución.

Adicional a esto, la red de datos debe proponer criterios de homologación de equipos y sistemas, que garanticen la compatibilidad con la infraestructura tecnológica y de comunicación de la institución, así como con los estándares y otras especificaciones

técnicas.

El DTIC debe ejecutar e implementar una serie de controles que garanticen el uso eficiente de las redes de comunicación, así como elaborar los procedimientos y lineamientos que involucren los temas de gestión de las redes de comunicación.

5.9 Gestión de activos

El DTIC asesora y brinda los estándares, especificaciones y lineamientos técnicos para la adquisición de bienes y servicios informáticos.

Toda adquisición de bienes y servicios de TIC debe ser canalizada a través del DTIC, quien brinda acompañamiento y asesoría como respuesta a las necesidades actuales basándose en los planes estratégicos institucionales, estandarización en la tecnología, factibilidad e integración con los equipos y software existentes, en apego a la normativa establecida y la implementación de acciones de control y seguimiento.

El DTIC colabora con las unidades organizativas en la realización de estudios de factibilidad, mercado y especificaciones técnicas, con base a factores críticos que puedan afectar tanto la compra de bienes y servicios como a nivel técnico.

El propósito de la práctica de gestión de activos de TI es planificar y gestionar el ciclo de vida completo de todos los activos de TI, para ayudar a la organización a:

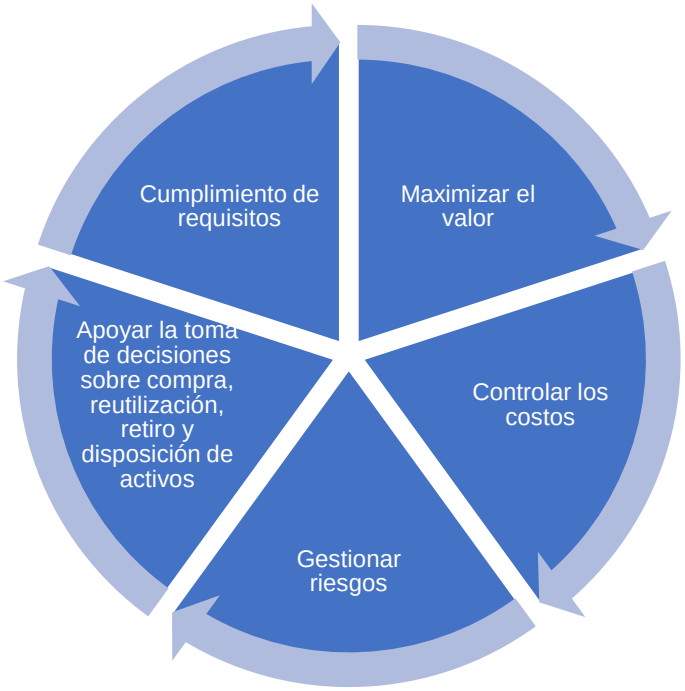

Ilustración 16. Ciclo de vida de los activos TI

5.9.1 Inventarios

El DTIC debe implementar una serie de buenas prácticas para administración de inventarios, se debe contar con un registro de los bienes de tecnologías de información y comunicación disponibles, controlar la obsolescencia, el ingreso y salida de equipos para donación o eventual retiro, así como el adecuado mantenimiento, instalación y configuración de estos. Asimismo, con lo referente a los activos de software se debe realizar un monitoreo y revisión constante, el cual tiene como objetivo principal rendir cuenta de todo el software utilizado en la institución, respecto a sus licencias de uso y software libre correspondiente.

Los funcionarios son responsables del buen uso del equipo, en el entendido que debe utilizarse para el cumplimiento de sus funciones y ajustarse a la normativa del DTIC para su buen funcionamiento.

Para garantizar el resguardo de los bienes patrimoniales, al realizarse movimientos de ingreso, salida, traslado de equipos o bien desecho, las unidades organizativas deben acatar los mecanismos de control de activos establecidos y actualizar el correspondiente inventario, según se establece en el procedimiento *Registro, Mantenimiento y Control de Bienes y Servicios MS.NI.SLA.05.04*

5.10 Gestión del software

Los sistemas de información gestionan la optimización y agilización de los procesos institucionales por medio de la automatización de estos, para ofrecer servicios basados en buenas prácticas de calidad y que la información institucional se mantenga en un ambiente de confiabilidad, integridad y seguridad, para atender los distintos planes, programas, proyectos y actividades en los tres niveles de gestión.

La gestión de software abarca actividades tales como:

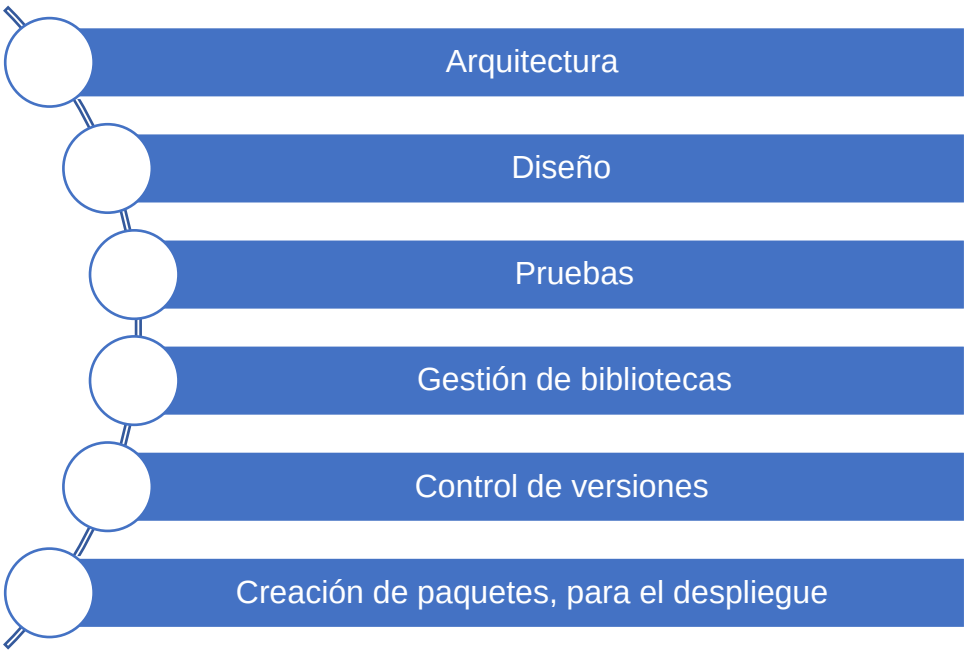

Ilustración 17. Actividades de la gestión del software

Las actividades de diseño, prueba, operación y mejora de aplicaciones se pueden evaluar continuamente mediante metodologías que rastrean el componente desde la detección de necesidades hasta la mejora continua y finalmente, su retiro. Se muestra gráficamente:

Ilustración 18. Ciclo de vida del desarrollo de software

Las bases de datos y sistemas de información que se desarrollen a lo interno o por terceros deben apegarse a la metodología y estándares definidos, que satisfagan las necesidades en términos de funcionalidad, confiabilidad, mantenibilidad, cumplimiento y auditabilidad. Además de la búsqueda de la integración con los sistemas ya desarrollados y la debida documentación de estos, ajustándolos a los planes estratégicos institucionales, en procura del uso racional y el mejor aprovechamiento de los recursos.

Para el desarrollo se deben realizar todos los estudios necesarios para conocer los requerimientos, la viabilidad del proyecto, donde se contemplen factores críticos como recursos técnicos, administrativos, financieros, recursos humanos, entre otros. Además de valorar la factibilidad técnica, operacional, económica y legal, riesgos asociados, entregables y documentación necesaria a lo largo del ciclo de desarrollo y el compromiso de la unidad organizativa interesada.

Si en el resultado del análisis realizado, se recomienda una contratación externa, se deben definir los términos de referencia, los cuales deben incluir las especificaciones, requisitos o condiciones requeridas o aplicables, según la ley de contratación administrativa y su reglamento vigente.

Le corresponde al DTIC elaborar los procedimientos, lineamientos y mecanismos de control para garantizar la disponibilidad, integridad y confidencialidad de la información capturada, procesada y desplegada en las bases de datos institucionales, así como de las actividades de priorización, análisis, desarrollo, mantenimiento y despliegue de aplicaciones, cumpliendo con los requisitos de usabilidad, apertura de datos y accesibilidad.

5.11 Gestión y continuidad de los servicios e incidentes

Los servicios TIC son el resultado de los planes estratégicos institucionales, la infraestructura tecnológica implementada, los sistemas de información disponibles, las necesidades institucionales y requerimientos de los usuarios, los cuales deben ser ofrecidos de forma efectiva, oportuna, segura, con calidad y en búsqueda del mejoramiento continuo, como se muestra en la siguiente ilustración:

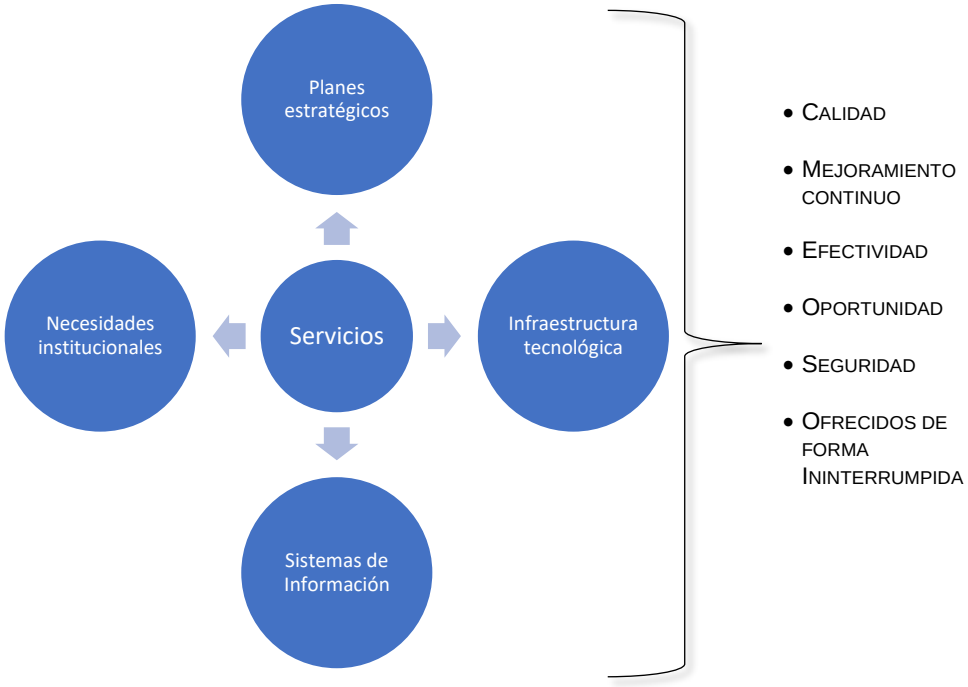

Ilustración 19. Aspectos de la gestión de servicios

Para lograr que los servicios funcionen de forma óptima es necesario disponer de una gestión de incidentes eficiente y capaz para solucionar cualquier problema en el menor tiempo posible, según los acuerdos de nivel de servicio basados en el Catálogo de Servicios.

5.11.1 Normativa TIC

La normativa técnica en la gestión TIC, es fundamental en la mejora continua y búsqueda de la calidad, la estandarización de los procesos, el desempeño de las actividades alineadas a las mejores prácticas en todas las funciones del DTIC.

La normativa técnica recopila leyes, reglamentos, directrices, decretos, estrategias y

resoluciones en materia de las TIC, que constituyen el marco regulatorio base para la elaboración de políticas, procedimientos, lineamientos y guías de operación.

Todas las actividades llevadas a cabo por el DTIC deben estar documentadas mediante la normativa técnica, procedimientos, lineamientos, guías de usuario, acuerdos de nivel de servicios (SLA, por sus siglas en inglés), entre otros documentos normativos.

Los procedimientos y guías de operación son elaborados y validados por el DTIC, revisados por la Dirección de Planificación y oficializados por la Dirección General de Salud.

Las políticas son elaboradas por el DTIC, formuladas y oficializadas por el CGTIC.

Los lineamientos, catálogo de servicios y SLA son elaborados y oficializados por el DTIC.

La actualización de los documentos normativos se programa cada año o al darse un cambio importante en la legislación nacional vigente.

Toda la documentación que se elabora, valida y oficializa es publicada en la Intranet institucional para estar disponible de consulta y acatamiento de todos los funcionarios del Ministerio de Salud.

5.11.2 Gestión de incidentes

La gestión de incidentes en DTIC pretende identificar y mitigar los riesgos, por medio de la recuperación y restauración del nivel habitual de funcionamiento de los servicios y minimizar en todo lo posible el impacto negativo para la institución, mediante la implementación de buenas prácticas, las cuales aseguren la calidad de los servicios, la disponibilidad de estos y la satisfacción de los usuarios.

La supervisión del funcionamiento continuo, seguro y eficiente de los recursos informáticos es necesario para garantizar el correcto desempeño de los equipos y los sistemas de información que estos soportan. Para esto, el personal del DTIC o un tercero a quien delegue vía contrato o convenio, son las únicas figuras autorizadas para instalar, configurar y dar mantenimiento a los bienes y servicios tecnológicos.

Las notificaciones de incidentes se canalizan por los medios de comunicación oficiales al Centro de Servicios, encargado de administrar la atención, basado en los Acuerdos de Nivel de Servicio (SLA) derivados del Catálogo de Servicios.

5.11.3 Catálogo de Servicios

El Catálogo de Servicios del DTIC describe los servicios que se ofrecen al ciudadano y a todos los funcionarios en sus tres niveles de gestión. Cada servicio se define de una forma sencilla y práctica a efectos de lograr una mayor comprensión de su disponibilidad, requisitos y la forma en que pueden ser solicitados al DTIC.

Respecto a los acuerdos de nivel de servicio, son un acuerdo escrito entre el proveedor del servicio, en este caso el DTIC y los usuarios, así mismo entre el DTIC y sus proveedores de servicios, con el objetivo de establecer el nivel de calidad del servicio brindado, tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio y otros.

También constituye un punto de referencia para el proceso de mejora continua, ya que el poder medir adecuadamente los niveles de servicio es el primer paso para mejorarlos y de esa forma aumentar los índices de calidad y satisfacción.

5.11.4 Centro de Servicios TIC

El DTIC debe contar con un sistema de administración que sea un punto de contacto o de atención primaria que centralice y canalice el registro de las incidencias de forma individual que contemple fecha y hora, los datos de la persona que realiza la notificación y la mayor cantidad de información posible para lograr su resolución.

Dicho sistema debe basarse en los acuerdos de nivel de servicio, definidos por el Catálogo de Servicio, que permita el registro, diagnóstico, categorización y priorización de las incidencias y asignar aquellas que requieran la atención presencial, así como el seguimiento del caso hasta su solución y cierre.

5.11.5 Plan de continuidad de los servicios

El DTIC es responsable de elaborar un plan de continuidad de los servicios, cuyo propósito es la gestión de la continuidad del servicio para asegurar que la disponibilidad y el rendimiento de un servicio se mantengan a niveles suficientes en caso de desastre, con el fin de producir una respuesta efectiva que salvaguarde los intereses institucionales.

Los planes de continuidad se activan al producirse una interrupción del servicio o un riesgo organizacional en una escala mayor que la capacidad normal de respuesta y recuperación en la gestión de incidentes. Un evento de esta magnitud generalmente se denomina desastre.

Se muestran ejemplos de incidentes y desastres:

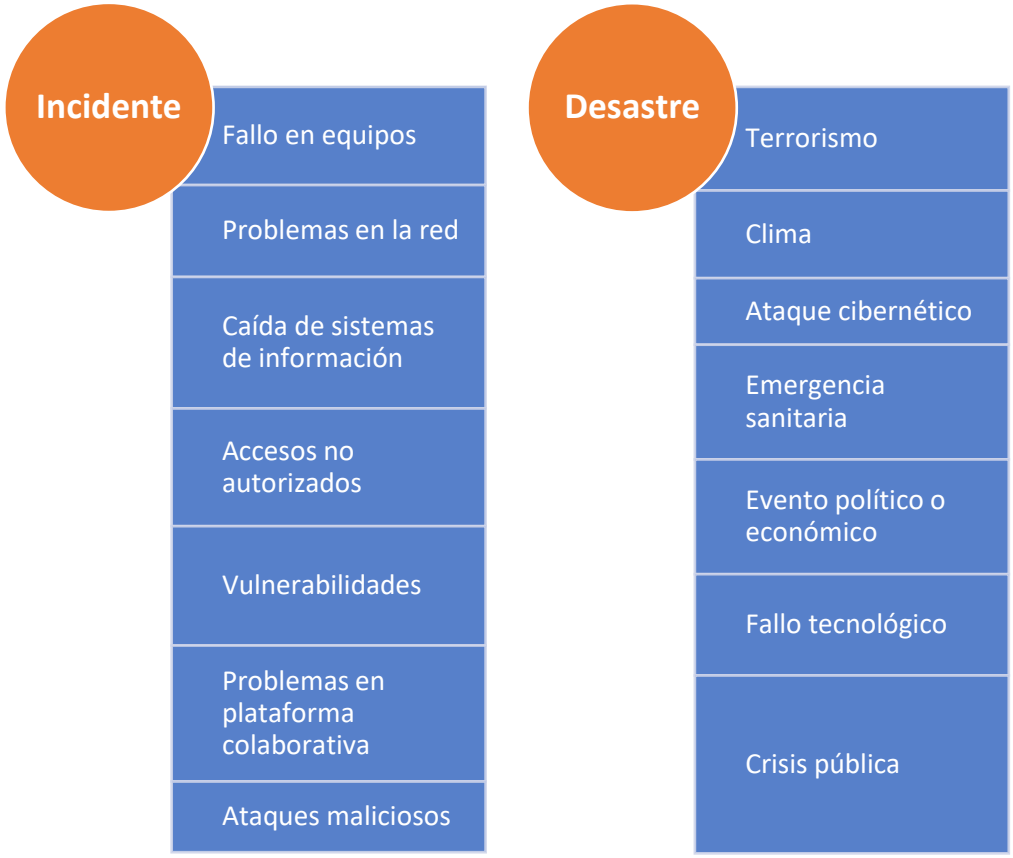

Ilustración 20. Ejemplos de incidentes y desastres

En la siguiente imagen se muestran elementos a considerar para la elaboración del plan de continuidad:

Tiempo de recuperación	• Tiempo máximo aceptable después de la interrupción del servicio
Punto de recuperación	• Punto al que debe restaurarse una actividad para reanudar su funcionamiento
Recuperación ante desastres	• Definir plan o planes que garanticen volver a la condición previa al desastre
Análisis de impacto	• Llevar a acabo estudios del impacto de los desastres en los servicios en la institución, para la mejora continua.

Ilustración 21. Aspectos del plan de continuidad de los servicios

Este plan de continuidad elaborado por el DTIC debe considerar todos los recursos críticos disponibles y establecer los puntos de control necesarios para garantizar la continuidad de todas las operaciones y servicios TIC, los roles y responsables para su ejecución en caso necesario.

5.12 Gestión de proveedores

La gestión de proveedores consiste en la relación con los suministradores de los servicios que gestiona el DTIC. Su principal objetivo es alcanzar la mayor calidad a un precio adecuado, sin embargo, pueden enumerarse otros objetivos:

1. Verificar que los contratos y acuerdos con proveedores permanezcan alineados con las necesidades actuales y futuras de la institución.
2. Gestionar la relación y el rendimiento de los proveedores, garantizando que queda constancia de los acuerdos financieros y de calidad alcanzados.
3. Negociar los contratos con los proveedores y gestionarlos a lo largo de su ciclo de vida, lo que incluye velar por el cumplimiento de los contratos o actualizarlos si éstos pierden vigencia.
4. Renovar y terminar contratos según las necesidades y servicios.
5. Evaluar el cumplimiento del proveedor del bien o servicio.

6. Mantener un registro de toda la información relacionada con los proveedores, contratos y los servicios que prestan, el registro debe contener:
    a. Número de contrato
    b. Descripción del servicio
    c. Partida presupuestaria
    d. Costo anual o mensual en dólares o colones
    e. Justificación del servicio
    f. Nombre del funcionario o funcionarios responsables de la ejecución del contrato
    g. Nombre de la empresa que brinda el servicio
    h. Fecha de inicio y fin del contrato
    i. Nombre completo del contacto directo o administrador del contrato por parte de la empresa que brinda el servicio
    j. Correo electrónico, página web, número telefónico del contacto con la empresa que brinda el servicio
    k. Cualquier otro dato o información de interés del funcionario o funcionarios responsables de la ejecución del contrato.

El DTIC debe mantener este registro disponible y permanentemente actualizado.

En relación con los proveedores deben definirse Acuerdos de Nivel de Servicio (SLA) y acuerdos de confidencialidad, en primera instancia entre el proveedor del servicio y el DTIC, donde se establezca las responsabilidades de ambas partes, la continuidad de los servicios y la recuperación de la información en caso de un incidente, la redundancia de la información, el mantenimiento, ubicación de los datos, la seguridad de la información, entre otros criterios que se puedan considerar. Además, deben existir Acuerdos de Nivel de Servicio (SLA) entre el DTIC y los usuarios internos que requieran hacer uso de las diferentes herramientas y definiendo claramente las responsabilidades.

5.13 Gestión del cumplimiento

La gestión del cumplimiento es el proceso permanente de supervisión y evaluación de los sistemas, la infraestructura tecnológica y los servicios, para asegurar que cumplen con las buenas prácticas de seguridad, de calidad y marco regulatorio interno, nacional e internacional.

El incumplimiento de este proceso incurriría en procesos legales, fallos de seguridad, pérdida de información, entre otros. Es importante mantener la actualización de los bienes de TIC, para evitar la interrupción de los servicios.

Para supervisar y gestionar con éxito el cumplimiento, debe incluir:

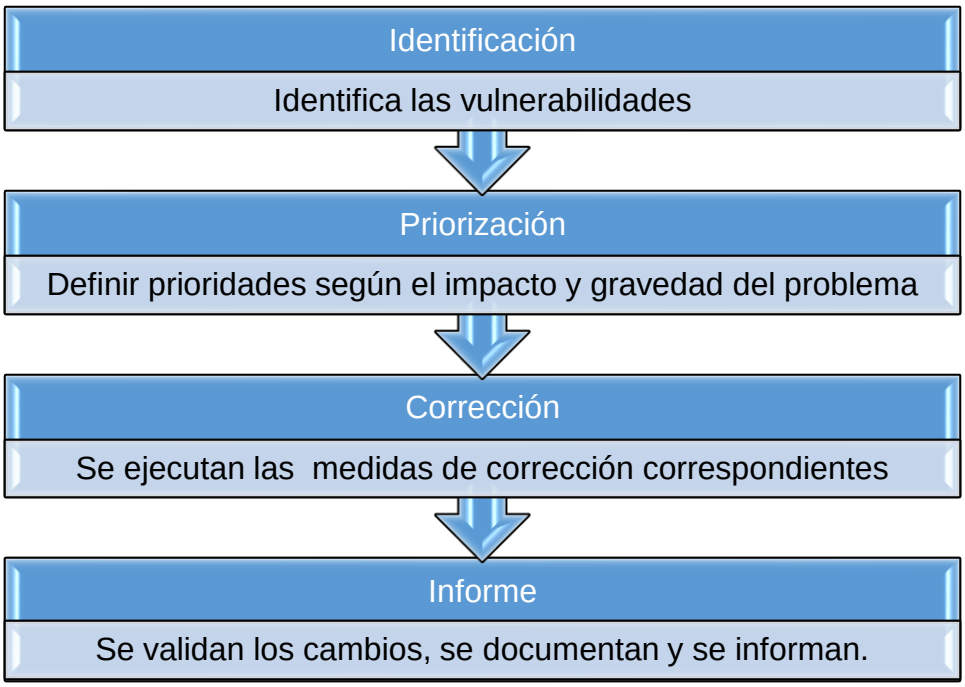

Ilustración 22. Aspectos de gestión de cumplimiento

El DTIC debe elaborar una revisión permanente de los servicios, los riesgos asociados, planes de mejora de calidad y de seguridad para garantizar el cumplimiento de las actividades técnicas y operativas de tecnologías de información y comunicación.

5.14 Gestión documental

La gestión documental es el conjunto de normas técnicas y prácticas usadas para administrar los documentos de todo tipo, recibidos y creados en la institución, facilitan la recuperación de información desde ellos, determinan la vigencia de los documentos y como deben guardarse, eliminarse y asegurar la conservación a largo plazo de los documentos declarados con valor científico y cultural, según se establece en la Ley 7202, su reglamento y leyes conexas del Archivo Nacional.

En el Ministerio de Salud se establecen los siguientes procedimientos para la gestión documental:

Ilustración 23. Procedimientos para la gestión documental

Para los documentos electrónicos y la correspondencia institucional debe disponerse de un sistema de información que permita el almacenamiento de los documentos digitales, que consideren los aspectos de archivo y formatos de conservación.

6. Glosario

Accesibilidad: El arte de garantizar que cualquier recurso, a través de cualquier medio, esté disponible para todas las personas, tengan o no algún tipo de discapacidad.

Acuerdo de nivel de servicio: (SLA por sus siglas en inglés) Compendio de los servicios ofrecidos a los usuarios donde se describe cada uno de ellos, describiendo cada uno de ellos de una forma sencilla y práctica a efectos de lograr una mayor comprensión de estos, así como su disponibilidad, requisitos y la forma en que pueden ser solicitados y soportados.

Archivística: Ciencia que trata de los archivos, de su conservación, administración, clasificación, ordenación, interpretación, entre otros; de las colecciones de documentos que en los archivos se conservan como fuente para su conocimiento ulterior y servicio público.

Auditabilidad: Los sistemas basados en servicios Web deben mantener una traza de todas las acciones que llevan a cabo de forma que sea posible realizar un análisis posterior que permita averiguar, por ejemplo, lo ocurrido en escenarios de desastre.

Autenticación: Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos. Normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una contraseña.

Big data: Conjuntos de datos o combinaciones de conjuntos de datos cuyo tamaño (volumen), complejidad (variabilidad) y velocidad de crecimiento (velocidad) dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales, tales como bases de datos relacionales y estadísticas convencionales o paquetes de visualización, dentro del tiempo necesario para que sean útiles.

Bit: Es la abreviación de Binary Digit (digito binario), la cual en términos técnicos es la menor unidad de información de una computadora. Un bit tiene solamente un valor (que puede ser 0 o 1). Varios bits combinados entre sí dan origen a otras unidades, como “byte”

Calidad: La totalidad de las características de un producto o servicio, que satisfacen necesidades explícitas o implícitas de un cliente.

Campus virtual: Se designa cualquier sitio web que tiene la finalidad de dirigirse a una comunidad de aprendizaje poniendo a su disposición los recursos pedagógicos y las funcionalidades de comunicación colaborativas correspondientes para el desarrollo de un entorno de capacitación.

Certificado digital: es un archivo informático generado por una Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física o jurídica, confirmando de esta manera su identidad digital en Internet. El certificado digital tiene como función principal autenticar al titular (propietario), pero puede servir también para firmar digitalmente.

Ciberseguridad: El conjunto de procesos utilizados para la gestión y protección de la transmisión, el procesamiento, el uso y el almacenamiento de datos e información, mediante tecnologías de información y comunicación (TIC).

Cifrado: Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos.

CIO (Chief Information Officer): es el responsable de los sistemas y de las tecnologías de la información de la empresa y, además, es el responsable de identificar y proveer las tecnologías necesarias para que los procesos de la empresa funcionen lo mejor posible.

Confidencialidad: Esto significa que la información solo está siendo vista o utilizada por personas que están autorizadas para acceder a ella, por tanto, se debe de suscribir el respectivo acuerdo de servicio donde se establezcan claramente las condiciones de las partes, que garanticen la confidencialidad de cualquier tipo de información que se gestione

Control de versiones: Se llama control de versiones a la gestión de los diversos cambios que se realizan sobre los elementos de algún producto o una configuración de este. Una versión, revisión o edición de un producto, es el estado en el que se encuentra el mismo en un momento dado de su desarrollo o modificación.

Criptografía: El arte y la técnica de crear mensajes codificados con procedimientos o claves secretas con el objeto de que no pueda ser descifrado salvo por la persona a quien está dirigido o que detenta la clave.

Datos abiertos: El concepto datos abiertos es una filosofía y práctica que persigue que determinados tipos de datos estén disponibles de forma libre para todo el mundo, sin restricciones de derechos de autor, de patentes o de otros mecanismos de control.

Disponibilidad: Esto significa que la información es accesible cuando los usuarios autorizados la necesitan.

DNS: El DNS (Domain Name System, Sistema de Nombres de Dominio) es un conjunto de protocolos y servicios que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

Especificaciones técnicas: Documento que define una serie de requisitos que un producto o servicio deben cumplir o satisfacer.

Firma digital: Quienes frecuentemente utilizan una computadora y trabajan con programas informáticos de oficina tipo Microsoft Office o similares, posiblemente hayan escuchado hablar del término “Firma Digital”. Sin embargo, muchas personas utilizan el término de forma incorrecta, ya que desconocen su verdadero significado.
En términos generales, podemos decir que la Firma Digital es una solución tecnológica que permite identificar al autor de un documento electrónico (autoría) y verificar que el mismo no ha sido modificado desde su creación (integridad).

Firmware: También conocido como soporte lógico inalterable, es el programa básico que controla los circuitos electrónicos de cualquier dispositivo. El firmware puede ser calificado tanto como parte del hardware como del software de un dispositivo.

Gestión de bibliotecas: Es el lugar en el que se almacena y se puede realizar la distribución del código de una aplicación o un programa. ... Debe contener las diferentes versiones de la aplicación o programa, disponiendo de un historial con los cambios realizados sobre el original y sobre cada nueva versión.

Innovación: Es un proceso que introduce mejoras, modifica y mejora elementos ya existentes, aunque también es posible en la implementación de elementos totalmente nuevos.

Integridad: Esto significa que cualquier cambio en la información por parte de un usuario no autorizado es imposible (o al menos detectado), y se realiza un seguimiento de los cambios realizados por usuarios autorizados; garantizando la exactitud, completitud de la información y los métodos de procesamiento.

Inteligencia de negocios: Conjunto de productos y servicios que permiten a los usuarios finales accesar y analizar de manera rápida y sencilla, la información para la toma de decisiones de negocio a nivel operativo, táctico y estratégico.

Interoperable: Capacidad de compartir datos informáticos en diferentes máquinas.

IP: La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.

Licencias de software: es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribución) y el licenciatario (usuario consumidor, profesional o empresa) del programa informático, para utilizarlo cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar o modificar el producto bajo una licencia determinada. Además, se suelen definir los plazos de duración, el territorio donde se aplica la licencia (ya que la licencia se soporta en las leyes particulares de cada país o región), entre otros.

Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones, incluyendo cualesquiera redes de comunicación abiertas o restringidas como internet, telefonía fija y móvil u otras.

Mejora continua: Revisión sistemática y continua de los procesos y sistemas implantados, mediante la cual se analizan y eliminan las fuentes de improductividad, y se simplifican los procedimientos de trabajo, con el fin de obtener mejores resultados.

No repudio: Prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibe (no repudio en destino). El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje, para entender mejor corresponde a la irrenunciabilidad, es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación.

Obsolescencia: Es la caída en desuso de máquinas, equipos y tecnologías motivada no por un mal funcionamiento de este, sino por un insuficiente desempeño de sus funciones en comparación con las nuevas máquinas, equipos y tecnologías introducidos en el mercado

Planes estratégicos: Es la determinación de los objetivos específicos y metas de largo plazo en una organización, junto con la adopción de cursos de acción y distribución de los recursos necesarios para lograr estos propósitos. Son estructurados, generalmente, a partir de una visión, misión, objetivos, metas e indicadores de gestión.

Portal web: Es aquel espacio en línea que presenta contenidos, servicios y herramientas para el usuario. Es mucho más robusto que un sitio, pues supone integrar más elementos interactivos.

Requerimiento: Es una necesidad para ser automatizada o que deben cumplir un sistema o

software a desarrollar para poder funcionar de manera correcta.

Riesgo: La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole perdidas o daños

Seguridad: La seguridad TIC es la responsable de implantar las medidas de seguridad necesarias para procurar la protección de la información a través de diferentes tipos de tecnología. Así, es capaz de proteger los datos de las empresas, tanto de formatos electrónicos o digitales, como en papel.

Servicios en la Nube: Lo que nos permite el servicio en la nube es la separación entre los programas que antes era obligatorio instalar en los equipos y con esto conseguimos utilizar aplicaciones o sistemas de gestión de manera remota gracias a Internet, sin necesidad de tenerlos instalados. Antes del concepto en la nube, todo lo referente al procesamiento y almacenamiento de datos se hacía desde el propio ordenador.

Software malicioso: Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

Software: Es un programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático. Software es: freeware (cuyas licencias son gratuitas); shareware (son gratuitas, pero con funcionamiento limitado); libre (puede ser cambiado, usado y redistribuido con las modificaciones); propietario (tanto de código abierto como cerrado).

Términos de referencia: Documento que define en forma ordenada y sistemática los objetivos y propósitos de un bien o servicio a contratar, los elementos que se requieren conocer para su evaluación, ejecución, administración y, el procedimiento mediante el cual se obtienen dichos elementos.

Transparencia: La rendición de cuentas obliga a que el ejercicio del poder y el cumplimiento de las funciones públicas asignadas se hagan de cara a los administrados.

Transversalidad: Colaboración de la tecnología con las diversas ramas del conocimiento, de forma tal que sea posible aportar soluciones y propuestas de valor a través de esta cooperación cruzada

Usabilidad: Cualidad de la página web o del programa informático que son sencillos de usar porque facilitan la lectura de los textos, descargan rápidamente la información y presentan funciones y menús sencillos, por lo que el usuario encuentra satisfechas sus consultas y cómodo su uso.

7. Referencias

7.1 Estándares

Este documento está orientado y considera aspectos de los estándares y mejores prácticas internacionales aplicables a la realidad institucional, con el objetivo de asegurar los mecanismos acordes a la actualidad tecnológica que fortalecen la gestión de las TIC. Algunas de ellas se definen seguidamente:

● ITIL

Acrónimo de Information Technology Infrastructure Library, es un conjunto de prácticas detalladas para la gestión de servicios de TI (ITSM) que se centra en alinear los servicios de TI con las necesidades de las empresas.

● COBIT

COBIT. Desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) y el Instituto de Gobernanza de TI (ITGI), consta de varios componentes, incluidos: 1. Marco de referencia: Organiza los objetivos de gobierno de TI y las mejores prácticas. 2. Descripciones de procesos: Proporciona un modelo de referencia y un lenguaje común. 3. Objetivos de control: Documenta los requisitos de gestión de alto nivel para el control de los procesos de TI individuales. 4. Directrices de gestión: Herramientas para asignar responsabilidades, medir el rendimiento e ilustrar relaciones entre procesos. 5. Modelos de madurez: Evaluar la madurez / capacidad organizacional y abordar las brechas.

• ISO 9001

La norma Internacional ISO 9001 está enfocada a la consecución de la calidad en una organización mediante la implementación de un método o Sistema de Gestión de la calidad (SGC).

Los requisitos especificados en las Normas de la serie ISO 9000 son genéricos y aplicables a todas las organizaciones sin tener en cuenta el tipo y el tamaño.

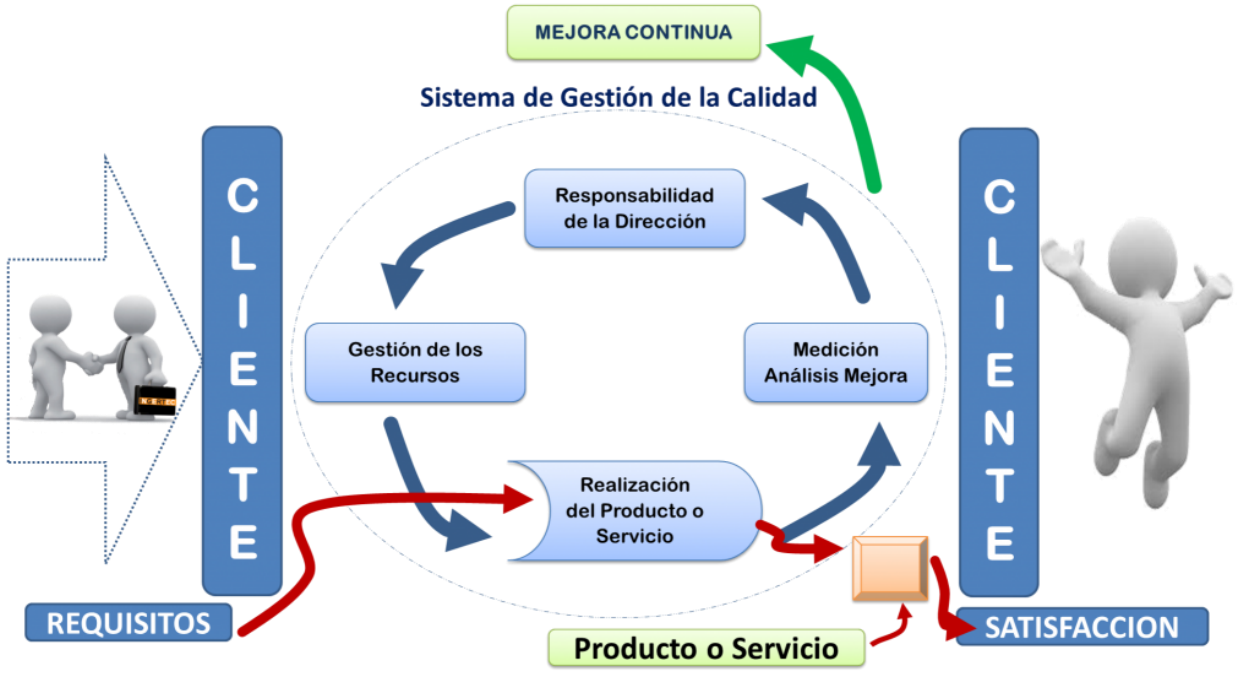

Ilustración 24. Aspectos de ISO 9001

La organización deberá definir y gestionar los procesos necesarios para asegurar que sus productos y servicios son conformes con los requisitos del cliente.

● ISO 27001

Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

● ISO 27002

ISO / IEC 27002 (Organización Internacional de Normalización / Comisión Electrotécnica Internacional). Formalmente titulado "Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de la seguridad de la información" documenta las mejores prácticas de seguridad en 14 dominios, de la siguiente manera:

Ilustración 25. Dominios de la ISO / IEC 27002

- ISO 27032

Más específicamente el ISO / IEC 27032: 2017 titulado “Tecnología de la información - Técnicas de seguridad - Guías para ciberseguridad” proporciona una guía para mejorar el estado de la seguridad cibernética, explicando los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad, en particular:

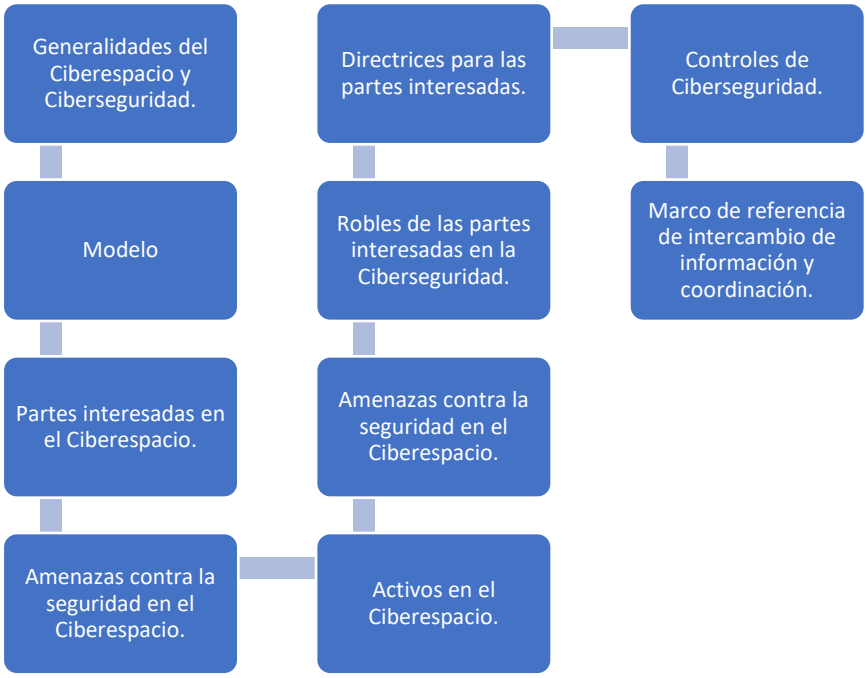

Ilustración 26. Dominios de la ISO 27032

● ISO 22301

La norma ISO 22301 establece todos los requisitos de planificar, establecer, implantar, operar, monitorear, revisar, mantener y realizar la mejora continua del sistema en cuanto a la respuesta y recuperación de los incidentes, cuando suceden.

Algunos beneficios de la gestión de continuidad del negocio son:

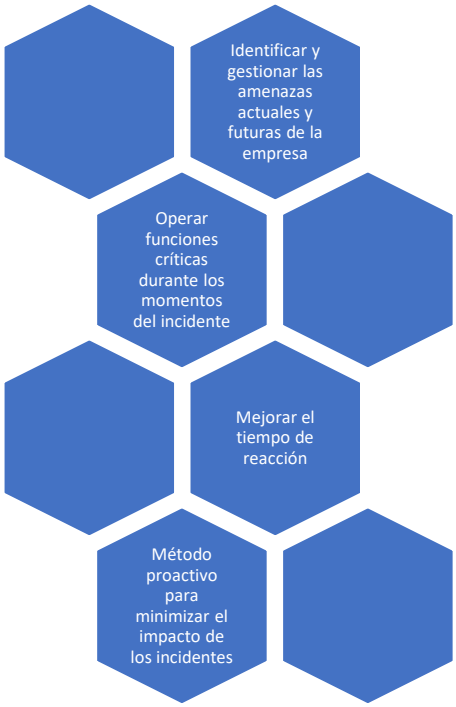

Ilustración 27. Beneficios de la gestión de continuidad del negocio de la ISO 22301

La norma ISO 22301 establece la metodología general para la continuidad de negocio. Dentro de la información documentada que se debe desarrollar:

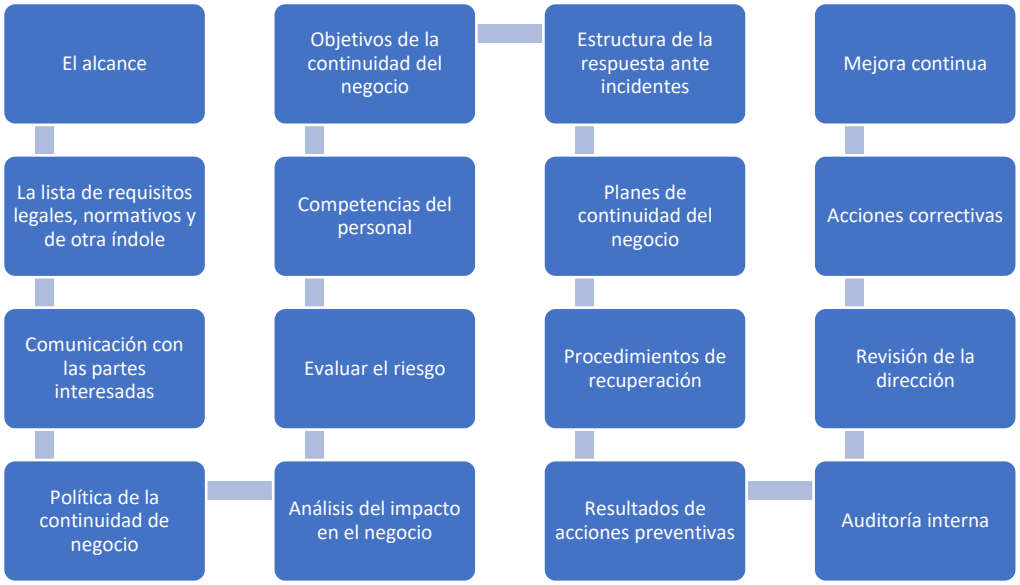

Ilustración 28. Documentación de ISO 22301

● ISO 31000

Tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos en la empresa de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Como complemento a esta norma se ha desarrollado otro estándar: la ISO 31010 "Gestión del riesgo. Técnicas de evaluación de riesgos". Esta norma provee de una serie de técnicas para la identificación y evaluación de riesgos, tanto positivos como negativos.

• SCRUM

Scrum es un proceso en el que se aplican de manera regular un conjunto de buenas prácticas para trabajar colaborativamente, en equipo**,** y obtener el mejor resultado posible de un proyecto.

En Scrum se realizan entregas parciales y regulares del producto final, priorizadas por el beneficio que aportan al receptor del proyecto. Por ello, Scrum está especialmente indicado para proyectos en entornos complejos, donde se necesita obtener resultados pronto, donde los requisitos son cambiantes o poco definidos, donde la innovación, la competitividad, la flexibilidad y la productividad son fundamentales.

● OWASP

OWASP es una organización sin fines de lucro líder en materia de desarrollo seguro de software, sus diversos proyectos han sido adoptados como estándares de la industria y se han convertido en lineamientos base para garantizar la seguridad del software.

Específicamente para el desarrollo de software se debe garantizar que los procesos de desarrollo de software implementado deben incluir prácticas de seguridad utilizando como línea base el OWASP ASVS (Application Security Verification Standard) y que garantizan que los productos entregados son libres de los diez riesgos identificados por el proyecto OWASP Top 10 que sea vigente para el momento dado. El top 10 actual es el siguiente:

A1 - Inyección

A2 - Pérdida de Autenticación

A3 - Exposición de datos sensibles

A4 - Entidades Externas XML (XXE)

A5 - Pérdida de Control de Acceso

A6 - Configuración de Seguridad Incorrecta

A7 - Secuencia de Comandos en Sitios Cruzados (XSS)

A8 - Deserialización Insegura

A9 - Componentes con vulnerabilidades conocidas

A10 - Registro y Monitoreo Insuficientes

● NIST

NIST (Instituto Nacional de Estándares y Tecnología) Publicación especial 800-53: Controles de seguridad y privacidad para sistemas y organizaciones de información federales. Conocido como NIST SP800-53, este es un marco de controles muy popular e integral requerido por todas las agencias gubernamentales de los EE. UU. También es ampliamente utilizado en la industria privada.

7.2 Documentos consultados

Se anotan los documentos que han sido consultados para la elaboración del presente documento:

- Administración Profesional de Proyectos, La Guía, Yamal Chamoun, 2002
- Catálogo de Servicios, 2020
- Código Nacional de Tecnologías Digitales, MICITT 2020
- Directriz 29-2007 Junta Administrativa del Archivo Nacional, 2007
- Estrategia de Transformación Digital hacía la Costa Rica del Bicentenario 4.0, MICITT 2018-2022
- Guía Nacional para la Publicación de Datos Abiertos, 2020

- Guía para el desarrollo de sitios web 2.0, Secretaría Técnica de Gobierno Digital, febrero 2009.
- Lineamiento Gestión de Documentos con Firma Digital y Firma Autógrafa, 2020
- Lineamientos Administración y Uso de Impresoras Multifuncionales, 2020
- Lineamientos de Uso de Internet y Plataforma Colaborativa del Ministerio de Salud, 2021
- Lineamientos para el Uso del Campus Virtual del Ministerio de Salud, 2020
- Lineamientos para la Identificación y Entrega de Datos de Interés Público Almacenados en Soporte Digital en el Ministerio de Salud, 2018
- Lineamientos para Publicar Contenidos en el Portal Web Institucional, 2020
- Llineamientos para el Registro, Administración y Hospedaje de Dominios a Título del Ministerio de Salud, 2020
- Manual de Identidad Gráfica del Ministerio de Salud, 2010
- Manual de Organización y Funciones, enero 2020
- Marcos de Gestión revisados
- Modelo Conceptual y Estratégico de la Rectoría de la Producción Social de la Salud, Julio 2011.
- Norma técnica para la gestión de documentos electrónicos en el Sistema Nacional de Archivos, 2008
- Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) 2019-2022
- Plan Estratégico Institucional 2016-2020
- Políticas de Tecnologías de Información y Comunicación, 2019
- Procedimiento MS.NC.SLA.06.01, Gestión de Sistemas de Información, 2017
- Procedimiento MS.NC.SLA.06.01.01. Intercambio o Transferencia de Información Institucional
- Procedimiento MS.NC.SLA.06.02, Gestión de Infraestructura Tecnológica, 2017
- Procedimiento MS.NC.SLA.06.03, Gestión de Servicios de Tecnologías de Información y Comunicación, 2017
- Procedimiento MS.NC.SLA.06.03.02 Administración y Mantenimiento del Portal Web Institucional, 2020

- Procedimiento MS.NI.LI.07 Gestión de Recursos Financieros, setiembre 2007
- Procedimiento MS.NI.LI.07.05 Registro, Ejecución y Control de la Gestión Financiera, setiembre 2007
- Procedimiento MS.NI.SLA.05 Gestión de Bienes y Servicios, setiembre 2007
- Procedimiento MS.NI.SLA.05.04 Registro, Mantenimiento y Control de Bienes y Servicios, 2007
- Procedimiento MS.NI.SLA.09.01 Solicitud y Préstamo documental, 2017
- Procedimiento MS.NI.SLA.09.02 Valoración Documental, 2017
- Procedimiento MS.NI.SLA.09.03 Clasificación y Ordenación Documental, 2017
- Procedimiento MS.NI.SLA.09.03.P.01 Protocolo Apertura, Foliado y Préstamo de Expedientes Administrativos, 2020
- Procedimiento MS.UO.LI.06.04 Administración de Riesgos, 2013
- Protocolo de Actuaciones Datos Covid-19 del Ministerio de Salud, 2021
- Reglamento Autónomo de Servicio del Ministerio de Salud, febrero 2005
- Reglamento Orgánico del Ministerio de Salud, 2019

7.3 Marco Legal

- Decreto 067-MICITT-H-MEIC Masificación de la implementación y el uso de la firma digital en el sector público costarricense, 2014
- Decreto 39652-S-MICIT Reglamento sobre el Uso de Estándares para Datos de la Salud en Pacientes y creación de la Comisión Nacional de Estandarización de Datos de Salud, 2016
- Decreto 40200-MP-MEIC-MC, Transparencia y Acceso a la Información, 2017
- Decreto Ejecutivo 37695-MP-MTSS, Promociona el Teletrabajo en las Instituciones Públicas, mayo del 2013.
- Decreto Ejecutivo 37549-JP sobre Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central, noviembre del 2012
- Decreto Ejecutivo 41999-S sobre reforma al Reglamento Orgánico del Ministerio de Salud, de la Gaceta N°209 del 4 noviembre 2019
- Directriz 019-MP-MICITT Desarrollo del Gobierno Digital del Bicentenario, 2018.
- Directriz 073-MP-MEIC-MC Transparencia y Acceso a la Información Pública, 2017

- Directriz 074-MP Apertura de Datos Abiertos, 2017
- Directriz 46-H-MICITT, Computación en la Nube, mayo de 2013
- Directriz 53-H-MICIT, Regulación y normalización de adquisiciones de tecnología y/o desarrollo de sistemas informáticos de apoyo a la gestión, julio de 2019
- Ley 6227, Ley General de la Administración Pública, reglamento y reformas
- Ley 6683, Ley Sobre Derechos de Autor y Derechos Conexos, su reglamento y reformas
- Ley 7202, Ley del Sistema Nacional de Archivos, reglamento y reformas
- Ley 7494, Ley Contratación Administrativa, reglamento y reformas
- Ley 8039, Ley de Procedimientos de Observancia de Derechos de Propiedad Intelectual y reformas
- Ley 8131, Ley de Administración Financiera de la República y Presupuestos Públicos y reformas.
- Ley 8220, Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites, reglamento y reformas.
- Ley 8292, Ley General de Control Interno, reglamento y reformas
- Ley 8422, Ley contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública, reglamento y reformas
- Ley 8554, Ley de Certificados, firmas digitales y documentos electrónicos y reformas.
- Ley 8968, Ley de Protección de la Persona frente al tratamiento de sus datos personales, reglamento y reformas
- Ley 9738, Ley para regular el teletrabajo, reglamento y reformas