Manual de Políticas y Lineamientos para la Gestión de Aplicaciones de la Subdirección de Tecnología de la Información

Superintendencia Nacional de Salud

Fecha del documento (23 – 09 – 2024)

Supersalud

Contenido

OBJETIVO

Establecer las políticas y lineamientos para el desarrollo de aplicaciones, durante su ciclo de vida, a partir la arquitectura de solución, diseño, construcción, soporte, operación, gestión y la calidad en el desarrollo de las aplicaciones, a través del uso de SCRUM[1] y *DevOps*[2], para la entrega productos y servicios de calidad de manera rápida, usando de forma óptimo los recursos con que cuenta la Entidad.

ALCANCE

El presente manual establece las políticas y lineamientos que se deben cumplir en el ciclo de vida de desarrollo de aplicaciones en la Superintendencia Nacional de Salud.

NORMATIVIDAD

Ley 1266 de 2008 “por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.” La entidad

[1] Metodología ágil de trabajo colaborativo para proyectos de desarrollo de software

[2] Metodología de trabajo, basada en el desarrollo colaborativo de código mediante el uso de nuevas herramientas y prácticas para reducir la distancia entre programadores y sistemas

cumplirá con los deberes y responsabilidades para garantizar la protección de los derechos del titular de los datos, en la información proveniente de terceros.

Decreto Ley 1151 de 2008 “Establecen los lineamientos generales de la estrategia de gobierno en línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.

Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones." entidad.

Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales.” La Superintendencia deberá aplicar los principios sobre protección de datos en todas y cada una de las bases de datos que gestione la entidad.

Decreto 2364 de 2012, “Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.”

Decreto 2462 de 2013 “Por medio del cual se modifica la estructura de la Superintendencia Nacional de Salud” En el artículo 11 se establecen las funciones que debe cumplir la Oficina de Tecnologías de la Información para el cumplimiento de los objetivos estratégicos de la entidad.

Decreto 2573 de 2014: “Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en Línea, se reglamenta parcialmente, la Ley 1341 de 2009 y se dictan otras disposiciones”

Decreto 1078 DE 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”

Decreto 415 DE 2016, “por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones”

Resolución Mintic 02893 de 2020: “Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano, y se dictan otras disposiciones”

Decreto 088 del 2021: “(…) digitalización y automatización de trámites y su realización en línea”

Directiva Presidencial 03 de 2021: Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión

Resolución Mintic 0500 del 2021: “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”

Resolución Mintic 460 de 2022: Se expide el Plan de Infraestructura de Datos y su hoja de ruta.

Directiva Presidencial 02 de 2022: Reiteración Política Pública en materia de Seguridad Digital

Decreto 767 del 2022: Mediante el cual se realiza la actualización Política Colombiana de Gobierno Digital

Decreto 338 del 2022: lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"

Resolución Mintic 0746 del 2022: Se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales.

GLOSARIO Y/O SIGLAS

Solución Nueva: Sistema de información o aplicación adquirida para resolver nuevos problemas o necesidades identificadas en los procesos de la entidad.

Solución a la medida: Sistema de información o aplicación que da respuesta a requerimientos específicos solicitados por los diferentes procesos de la entidad.

Actualización: Mejora a una solución requerida o solicitada por la entidad.

Guiones: Paso a paso para establecer las pruebas técnicas y funcionales de una solución tecnológica.

Bases de datos: Serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información.

Implementación: Conjunto de actividades necesarias para poner a disposición de los usuarios el sistema de información.

Diseño de Sistemas: se define el proceso de aplicar ciertas técnicas y principios con el propósito de definir un dispositivo, un proceso o un Sistema, con suficientes detalles como para permitir su interpretación y realización física.[3]

Ambiente de Desarrollo: proveer la infraestructura de hardware y software necesaria para realizar la implementación del sistema y la ejecución de pruebas unitarias por parte de cada desarrollador.

[3] Tomado de http://a1255681.sites.myregisteredsite.com/ciencias/tecnologia/computadoras/conceptosyprincipios.htm

Ciclo de Vida del Software (SDLC): El ciclo de vida del Software hace referencia al marco usado para estructurar, planear y controlar los procesos de desarrollar sistemas de información.

CMMI (Capability Maturity Model Integration): CMMI es un modelo de referencia que cubre las actividades esenciales para desarrollar productos y servicios, contiene las prácticas necesarias para la gestión de proyectos, administración de proyectos, ingeniería de sistemas, ingeniería de software, y soporte a los procesos usados en el desarrollo y mantenimiento.

Scrum: Marcos de desarrollo ágiles caracterizados por:

- Adoptar una estrategia de desarrollo incremental, en lugar de la planificación y ejecución completa del producto.
- Basar la calidad del resultado más en el conocimiento tácito de las personas en equipos auto organizados, que en la calidad de los procesos empleados.
- Solapamiento de las diferentes fases del desarrollo, en lugar de realizar una tras otra en un ciclo secuencial o en cascada.

Tester: El profesional **probador de software** (**tester**, por su denominación en inglés) planifica y realiza pruebas de software, con el propósito de comprobar su correcto funcionamiento. Identifican riesgos del software, descubren errores y los

transmiten a los encargados. Realizan la evaluación del funcionamiento en general del software y proponen alternativas de mejora.[4]

Pruebas. La ejecución de pruebas requiere de personal especializado para medir los procesos que intervienen de principio a fin. Un tester tiene además a cargo la función de analizar la información contenida en los requisitos, identificar riesgos y características de calidad a probar, debe también seleccionar la mejor estrategia para el proyecto, producto o sistema a probar, a fin de garantizar que las pruebas permitan obtener un producto que satisfaga las necesidades del usuario, de la entidad y que cumpla con los requisitos de seguridad establecidos para afrontar los retos del presente.

Pruebas unitarias: Las pruebas unitarias son definidas para comprobar el correcto funcionamiento de un módulo de código. Esto sirve para asegurar que cada uno de los módulos funcione correctamente por separado, en esta sección se definen los módulos o funcionalidades sobre los cuales se deben realizar pruebas unitarias, estos componentes o funcionalidades debe relacionarse en el formato de pruebas unitarias.

Pruebas de integración: Las pruebas de integración se definen como las pruebas para evaluar un proceso compuesto por varios componentes o funcionalidades y se deben relacionar con el formato de pruebas de integración.

[4] Tomado de: https://www.educaweb.com/profesion/probadores-software-testers-238/

Pruebas de aceptación: Los test de aceptación son aquellos destinados a determinar si los requisitos de cierta funcionalidad han sido cumplidos, como usuarios finales, no tienen por qué preocuparse por los detalles de la implementación, sino que deberían poder centrarse más en que la parte funcional cumple las expectativas creadas al inicio del Sprint.

Pruebas de regresión: Se definen el conjunto de pruebas necesarias para validar, que ante eventuales cambios en el software, como parches, ajuste en datos, cambios en la configuración, interfaces, orígenes de datos etc. Las características del software se comporten de manera correcta.

Pruebas de rendimiento: Se definen el conjunto de pruebas asociadas al rendimiento del software y los mecanismos por los cuales se realizarán estas pruebas.

Diseño de Sistemas: se define el proceso de aplicar ciertas técnicas y principios con el propósito de definir un dispositivo, un proceso o un Sistema, con suficientes detalles como para permitir su interpretación y realización física.[5]

Ambiente de Desarrollo: proveer la infraestructura de hardware y software necesaria para realizar la implementación del sistema y la ejecución de pruebas unitarias por parte de cada desarrollador.

[5] Tomado de: https://www.utp.edu.co/~wilopez/ExposicionesFII/Analisis%20y%20Diseno.ppt#:~:text=El%20dise%C3%B1o%20de%20sistemas%20se,su%20interpretaci%C3%B3n%20y%20realizaci%C3%B3n%20f%C3%ADsica.&text=El%20dise%C3%B1o%20de%20los%20datos,El%20dise%C3%B1o%20Arquitect%C3%B3nico

Ciclo de Vida del Software (SDLC): El ciclo de vida del Software hace referencia al marco usado para estructurar, planear y controlar los procesos de desarrollar sistemas de información.

CMMI (Capability Maturity Model Integration): CMMI es un modelo de referencia que cubre las actividades esenciales para desarrollar productos y servicios, contiene las prácticas necesarias para la gestión de proyectos, administración de proyectos, ingeniería de sistemas, ingeniería de software, y soporte a los procesos usados en el desarrollo y mantenimiento.

Scrum: Marcos de desarrollo ágiles caracterizados por:

- Adoptar una estrategia de desarrollo incremental, en lugar de la planificación y ejecución completa del producto.
- Basar la calidad del resultado más en el conocimiento tácito de las personas en equipos auto organizados, que en la calidad de los procesos empleados.
- Solapamiento de las diferentes fases del desarrollo, en lugar de realizar una tras otra en un ciclo secuencial o en cascada.

Pruebas unitarias: Las pruebas unitarias son definidas para comprobar el correcto funcionamiento de un módulo de código. Esto sirve para asegurar que cada uno de los módulos funcione correctamente por separado, en esta sección se definen los módulos o funcionalidades sobre los cuales se deben realizar pruebas unitarias, estos componentes o funcionalidades debe relacionarse en el formato de pruebas unitarias.

Pruebas de integración: Las pruebas de integración se definen como las pruebas para evaluar un proceso compuesto por varios componentes o funcionalidades y se deben relacionar con el formato de pruebas de integración.

Pruebas de aceptación: Los test de aceptación son aquellos destinados a determinar si los requisitos de cierta funcionalidad han sido cumplidos, como usuarios finales, no tienen por qué preocuparse por los detalles de la implementación, sino que deberían poder centrarse más en que la parte funcional cumple las expectativas creadas al inicio del Sprint.

Pruebas de regresión: Se definen el conjunto de pruebas necesarias para validar que ante eventuales cambios en el software, como parches, ajuste en datos, cambios en la configuración, interfaces, orígenes de datos etc. Las características del software se comporten de manera correcta.

Pruebas de rendimiento: Se definen el conjunto de pruebas asociadas al rendimiento del software y los mecanismos por los cuales se realizarán estas pruebas.

Pruebas de seguridad: Se definen el conjunto de pruebas asociadas a la seguridad del software y los mecanismos por los cuales se realizarán estas pruebas.

POLITICAS DE OPERACIÓN

Generales

- La Superintendencia Nacional de Salud debe garantizar la disponibilidad de personal para liderar y supervisar los proyectos en ejecución tanto internos como contratados; así como el perfil para la definición de arquitectura de aplicaciones, la aplicación técnica de pruebas funcionales, no funcionales y la generación de la documentación que se requiera.

- La verificación de la aplicación de la política de desarrollo de software debe estar a cargo de un equipo de profesionales asignados por la Subdirección de Tecnologías de la Información.

- El subdirector de Tecnologías de la Información, o quién haga sus veces, debe seleccionar un grupo de profesionales de las diferentes disciplinas, grupos funcionales o equipos de trabajo, existentes en la subdirección para conformar el Equipo de Gestión de Cambios, que se encargará de analizar las solicitudes de cambio en las aplicaciones e infraestructura tecnológica, para los casos en los que se requiera.

- Todo cambio relacionado con TI, que pretenda efectuarse en la Superintendencia Nacional de Salud y que pueda afectar de manera directa o indirecta la infraestructura tecnológica de la entidad y la disponibilidad de las aplicaciones, deben surtir el respectivo estudio y aprobación por parte del Equipo de Gestión de Cambios de la Subdirección de Tecnologías de la Información (STI)

- Los cambios proyectados que puedan en un momento determinado comprometer la operación de la entidad, deberán ser llevados al Comité Directivo para su aprobación, previa revisión por parte del Equipo de Gestión de Cambios de la STI. En todo caso ningún cambio podrá ser llevado a cabo sin la aprobación correspondiente por parte del Equipo de Gestión de Cambios de la STI, o, en su defecto por el Comité Directivo en los casos que se requiera.

Aspectos generales de Arquitectura de referencia

- Los profesionales encargados del desarrollo de aplicaciones deben garantizar la trazabilidad y control de los proyectos de TI que se ejecuten en la entidad y proponer prácticas gobernables de desarrollo de soluciones de software orientadas a servicios.

- Toda aplicación o sitio web que sea desarrollada para la Superintendencia Nacional de Salud debe garantizar la aplicación del esquema para la arquitectura de referencia (dominio, aplicación e infraestructura) sobre el cual se implementen los requerimientos funcionales y no funcionales.

- Toda aplicación o sitio web realizada para la Superintendencia Nacional de Salud debe tener la capacidad de intercambiar de información, acatando los aspectos de seguridad establecidos en este documento.

- Toda aplicación o sitio web que sea desarrollada para la Superintendencia Nacional de Salud debe soportar la arquitectura y componentes de información establecidos por la Entidad.

Aspectos generales de los desarrollos.

- Todo desarrollo o sitio web que se deba implementar en la Superintendencia Nacional de Salud deberá garantizar el cumplimiento de lo establecido en la Ley 1581 de 2012, en lo pertinente a la protección de datos personales y el registro de las bases de datos en los casos que aplique.

- Toda aplicación o sitio web, que sea desarrollado para la Superintendencia Nacional de Salud debe garantizar el cumplimiento estricto de todas las actividades previstas en el ciclo de vida del Software (norma ISO 12207 / IEEE 1074) y los lineamientos previstos en la documentación interna de la Entidad, con el propósito de estructurar, planear y controlar los procesos de desarrollo de sistemas de información.

- Todos los requerimientos de negocio que surjan a partir de la necesidad de las diferentes dependencias de la entidad y que pueden ser cubiertos mediante la implementación de una solución tecnológica, bien sea una nueva capacidad o servicio o la realización de un cambio a una solución ya existente, deben ser radicadas en la Dirección de Innovación y Desarrollo a través del formato establecido para tal fin.

- Los requerimientos que se han identificado se deben trabajar en estrecha colaboración con los usuarios y las partes interesadas de manera que se puedan registrar sus necesidades y expectativas en el documento de análisis de requerimientos; de esta manera se deben definir los requerimientos funcionales (qué debe hacer el software) y los requerimientos no funcionales (características de calidad, rendimiento, escalabilidad, seguridad, etc.)

- La Superintendencia Nacional de Salud ha establecido el formato “Especificación de Caso de Uso”, código DIFT37, con el objeto de que todo desarrollo, cumpla con el diligenciamiento y firma a satisfacción del formato, por las partes interesadas (usuario funcional responsable y analista que construye el requerimiento), en el cual deberá registrar el objetivo de la solicitud, detallando el sistema de información y las funcionalidades que serán objeto de dicho desarrollo, conforme al requerimiento del usuario funcional.

- El subdirector de Tecnologías de la Información, o quién haga sus veces, debe informar mediante comunicación interna (Memorando) dirigido a los profesionales que integrarán el Equipo de Gestión de Cambios, su participación en el equipo, detallando en el mismo documento las tareas que deberán adelantar para la aprobación o no de los cambios solicitados.

- Para todos los casos, una vez se han recolectado los requerimientos para desarrollo y se han registrado en lista de SharePoint “Requerimientos DID-STI”, se deben evaluar y clasificar en función de su importancia, alcance y factibilidad.

- Todo cambio debe surtir el protocolo formal establecido para la gestión de cambios, mantener actualizada la lista de SharePoint "Registro de Gestión de Cambios” e informar a todos los involucrados respecto de los cambios realizados.

- Para todos los casos, los funcionarios, contratistas o terceros encargados de realizar desarrollo de aplicaciones o sitios web para la Superintendencia Nacional de Salud deben conocer y acatar las políticas aquí establecidas, incluyendo temas arquitectura y seguridad.

- Toda aplicación o sitio web, que sea desarrollada para la Superintendencia Nacional de Salud, debe garantizar el estricto cumplimiento en la adopción de los lineamientos y buenas prácticas sugeridas para el desarrollo seguro.[6]

- El personal de Seguridad de la Información de la Subdirección de Tecnologías de la Información (STI), asignado por la Subdirección, debe ser el responsable de impulsar la ejecución y cumplimiento del atributo de

[6] https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/assets/docs/OWASP_SCP_Quick_Reference_Guide_v21.pdf - OWASP Secure Coding Practices Quick Reference Guide

calidad: Seguridad de los sistemas de información, incluidos en el presente documento.

- Los funcionarios responsables del desarrollo, adquisición y mantenimiento de los sistemas de información deben velar porque estos activos de información se mantengan disponibles, íntegros y confidenciales, mientras se encuentren en proceso de desarrollo, mantenimiento y puesta en marcha.

- Todos los componentes desarrollados para la Superintendencia Nacional de Salud deben incluir documentación como: manuales, tutoriales y diagramas de proceso, entre otros.

- En el diseño de un sistema de información se deben definir los componentes del sistema, las interacciones y diagramas de diseño especificando la arquitectura y el plan detallado para su posterior implementación. Adicionalmente, se deben considerar aspectos como la interfaz de usuario, la seguridad y el rendimiento.

- Se debe definir e identificar la arquitectura adecuada para el sistema de información, definiendo los componentes, las interacciones y las dependencias. Se deben elaborar los diseños detallados de cada componente y módulo del sistema, definiendo interfaces, estructuras de datos, algoritmos y reglas de negocio.

- De forma periódica, el Arquitecto de Aplicaciones asignado debe realizar revisiones del diseño para asegurar su calidad, identificar posibles mejoras y garantizar la alineación con los requerimientos del sistema.

- Para el desarrollo de software y las aplicaciones en la Superintendencia Nacional de Salud se debe adoptar el uso de metodologías que cubran las diferentes fases del desarrollo de software, incluyendo la fase de definición y planeación, así como instrumentos o herramientas para la gestión de seguimiento de las implementaciones tecnológicas.

- Para el desarrollo de software y las aplicaciones en la Superintendencia Nacional de Salud se debe adoptar la metodología formal establecida para el desarrollo y mantenimiento de software, que oriente los proyectos de construcción o evolución de los sistemas de información desarrollados a la medida, tanto internamente o a través de terceros.

- Los productos de software o sitio web desarrollados para la Superintendencia Nacional de Salud deben seguir parámetros de usabilidad como simplicidad, organización de los elementos y adaptación a diversos dispositivos, navegación intuitiva y accesibilidad sin perjuicio del su sistema operativo y/o navegador utilizado. La validación la se realizará en su momento por parte del funcionario o contratista encargado de efectuar las pruebas correspondientes.

- Todas las aplicaciones de software o sitio web desarrollados para la Superintendencia Nacional de Salud deben garantizar el manejo de una

carga constante y creciente de datos y trabajo, en simultáneo con el crecimiento y la demanda de información por parte de la Superintendencia Nacional de Salud.

- Las aplicaciones deben permitir escalamiento tanto horizontal como vertical, bajo demanda o automatizado.

- Las aplicaciones críticas deben estar configuradas en alta disponibilidad, preferiblemente con un sistema de balanceo de carga con el fin de mantener la disponibilidad de los sistemas de información en caso de fallo o mantenimiento de la infraestructura que la soporta.

- Todas las aplicaciones o sitio web desarrolladas por y para la Superintendencia Nacional de Salud, debe permitir la realización de pruebas (unitarias de código, integración, funcionales y de regresión) a los componentes desarrollados o modificados con el fin de identificar posibles efectos secundarios o adversos durante su ejecución.

- Para todos los casos, la realización de pruebas previas a la liberación de cualquier desarrollo es indispensable para asegurar que el software cumpla con los requisitos establecidos y que funciona correctamente.

- Para todos los casos, antes de llevar a producción las aplicaciones se deben realizar pruebas unitarias, para verificar el funcionamiento de cada componente individual; pruebas de integración, para probar la interacción

entre los componentes; pruebas de sistema, para verificar el funcionamiento del software como un todo.

- Para todos los casos, cada aplicación debe permitirse instalar y configurar en el entorno de producción sin afectar su integridad ni su total funcionalidad.

- Las Subdirecciones de Tecnologías de Información, Metodologías y Analítica deben efectuar conjuntamente en los casos que se requiera el análisis de impacto ante cualquier solicitud de cambio, con el propósito de establecer la viabilidad del cambio y las acciones a seguir.

- Los sistemas de información de la Superintendencia Nacional de Salud, disponibles para el acceso a la ciudadanía o que por la caracterización de los usuarios lo requieran, deben cumplir con las funcionalidades de accesibilidad que indica la *Política de Gobierno Digital***.**

- Toda aplicación o sitio web que sea desarrollada para la Superintendencia Nacional de Salud debe ser realizado por un equipo interno de profesionales, al cual se le deben proveer de los recursos necesarios, salvo en casos particulares en que se amerite contratación externa.

- Toda aplicación o sitio web, que sea desarrollada para la Superintendencia Nacional de Salud, en los casos que se requiera, debe contar con el concepto técnico emitido por las subdirecciones de la Dirección de

Innovación y Desarrollo (DID) que sean necesarias, o quien haga sus veces, y la posterior aprobación y priorización por el Comité Directivo.

- La entrega de las aplicaciones o sitios web que se desarrollen para la Superintendencia Nacional de Salud debe cumplir durante su desarrollo con entregas progresivas, estableciendo entregables que permitan medir el avance y la aprobación por parte de la dependencia funcional y la STI.

- Todas las aplicaciones desarrolladas por y para la Superintendencia Nacional de Salud deben garantizar los atributos de calidad de software como modificabilidad, escalabilidad, usabilidad, accesibilidad, integración y seguridad de la información entre otros.

- En el desarrollo de aplicaciones o sitios web en la Superintendencia Nacional de Salud se debe adoptar el uso de metodologías que cubra las diferentes fases del desarrollo de software, incluyendo la fase de definición y planeación, así como instrumentos o herramientas para la gestión de seguimiento de las implementaciones tecnológicas.

- Para todos los casos, se debe garantizar la actualización de la documentación y arquitectura de solución de los sistemas de información de la Entidad, bajo los parámetros de las arquitecturas de referencia establecidas.

- Toda aplicación o sitio web, que sea desarrollado para la Superintendencia Nacional de Salud, debe establecer o adoptar los lineamientos establecidos

en el MANUAL DE IMAGEN INSTITUCIONAL – DIMN02 y debe aplicarse de conformidad con la caracterización de usuarios y de acuerdo con el canal utilizado por los sistemas de información, siempre alineados con los principios de usabilidad definidos por el gobierno nacional.

- Toda aplicación o sitio web, que sea desarrollado por y para la Superintendencia Nacional de Salud, debe identificar y mantener la independencia de los ambientes (desarrollo, pruebas, capacitación, producción) requeridos durante el ciclo de vida de los sistemas de información, ya sea de manera directamente o mediante terceros.

- Para el desarrollo de toda aplicación o sitio web que se pretenda implementar para la Superintendencia Nacional de Salud, se debe surtir un proceso formal de análisis y gestión de requerimientos de software durante el ciclo de vida de los sistemas de información de tal manera que se avale su trazabilidad y cumplimiento.

- Para todos los casos, dentro del proceso de desarrollo de sistemas de información se deben establecer estrategias de integración continua sobre los nuevos desarrollos de sistemas de información.

- En todos los proyectos de desarrollo de aplicaciones o sitios web para la Superintendencia Nacional de Salud, se debe alojar en DevOps el código fuente generado por cada desarrollador de manera obligatoria.

- El Plan de Pruebas debe formar parte del ciclo de vida del Desarrollo de Software.

- Toda aplicación o sitio web, que sea desarrollado por y para la Superintendencia Nacional de Salud, debe establecer un plan de pruebas que permita cubrir lo funcional y lo no funcional.

- Para todos los casos la aprobación de cada una de las etapas del Plan de Pruebas debe estar vinculada a la transición del Sistema de Información a través de los diferentes ambientes.

- Todos los proyectos de desarrollo de software que se adelantan en la entidad para la implementación de los sistemas de información deben garantizar una ejecución exitosa y eficiente de los componentes del sistema.

- Para todos los casos de implementación de los sistemas de información en la SNS en el entorno de producción, se debe requerir previa configuración de los recursos de hardware y software, la migración de datos si es necesario y la preparación para su uso por parte de los usuarios finales.

- Para los sistemas de información que se desplieguen en la Superintendencia Nacional de Salud, se deben establecer entornos de implementación de forma adecuada, incluyendo la infraestructura de servidores, red, así como el software necesario para la correcta ejecución del sistema.

- Para los sistemas de información que se desplieguen en la Superintendencia Nacional de Salud, se debe realizar la configuración adecuada de los componentes, incluyendo la conexión a la base de datos, la configuración de los parámetros y la instalación de los paquetes de implementación en el entorno de producción acorde con los criterios establecidos.

- Para todas las aplicaciones que se desplieguen en la Superintendencia Nacional de Salud, se deben establecer mecanismos de monitoreo para supervisar el rendimiento y el funcionamiento del sistema implementado, así como realizar los ajustes y optimizaciones en los casos que sea necesario para garantizar el rendimiento óptimo del sistema de información.

- En todos los casos de desarrollo de aplicaciones o sitios web para la Superintendencia Nacional de Salud, se debe documentar lo concerniente a la implementación, incluyendo los pasos, configuraciones realizadas y problemas detectados.

- Para todos los desarrollos de software que se tengan que implementar para la Superintendencia Nacional de Salud, la documentación y manuales relevantes deben ser entregados a los usuarios finales para facilitar el la adopción y uso efectivo del sistema implementado.

- Para todas las aplicaciones que se implementen en la Superintendencia Nacional de Salud, el responsable del proyecto de TI debe gestionar la

realización de las actividades para la apropiada transferencia del conocimiento.

- En todos los casos, posterior al despliegue de las aplicaciones, en un tiempo no superior a tres meses, se debe llevar a cabo el mantenimiento del software para corregir errores, realizar actualizaciones y mejorar su funcionalidad en los casos que se requiera.

- A todas las aplicaciones implementadas en la Superintendencia Nacional de Salud se les debe realizar mantenimiento con propósito de corregir posibles errores, la implementación de mejoras, realizar la optimización del rendimiento y/o la adición de nuevas características según las necesidades cambiantes de los usuarios.

- Toda solicitud (requerimiento) nuevo o que afecte la estructura de los datos es considerada como un cambio y debe ser discutido por el Equipo de Gestión de Cambios.

- Todos los cambios propuestos en el desarrollo de software, incluyendo nuevos requisitos, correcciones de errores y mejoras deben ser identificados y registrados en la lista de SharePoint “Requerimientos DID-STI”.

- Para todos los casos, se debe evaluar el impacto de los cambios propuestos en términos de tiempo, recursos, riesgos y afectación a otros componentes o funcionalidades del sistema.

- La STI mediante el Equipo de Gestión de Cambios debe realizar la aprobación de los cambios, con la participación de las partes interesadas relevantes garantizando y la toma de decisiones informadas basadas en la evaluación de impacto.

- El profesional asignado una vez que el cambio es aprobado debe realizar la implementación siguiendo los procedimientos y estándares establecidos en “Gestionar problemas y cambios” que hace parte de la actividad clave de éxito "Gestionar TI" del proceso de Gobierno y Gestión de Datos e Información.

- Todo requerimiento debe estar redactado y estructurado de manera lógica y modular (funcionalidades específicas, claras y realizables).

- Todos los cambios que se implementen deben surtir las pruebas previas a su liberación y contar con la aprobación del usuario funcional.

- Todo cambio que deba ser implementado debe surtir el paso por los tres ambientes: desarrollo, pruebas y producción.

- El Equipo de Gestión de Cambios debe ser responsable de revisar y aprobar los cambios propuestos, compuesto por representantes de los diferentes grupos de la STI, como Sistemas de Información, Seguridad, Infraestructura, Mesa de ayuda.

- Se debe asignar a un responsable del cambio, quien se encargará de gestionar y coordinar las actividades de cambio, incluyendo el registro en el instrumento definido para llevar el control, la documentación, seguimiento y comunicación.

- Para todos los casos relacionados con gestión de cambios, se debe evaluar los **criterios**, que permitan establecer si los cambios propuestos están alineados con los requisitos del sistema y si cumplen con los objetivos y metas del proyecto; además determinar el grado de impacto en términos de tiempo, recursos, riesgos y afectación a otras partes del sistema y evaluar si los cambios propuestos mantendrán o mejorarán la calidad, estabilidad y rendimiento del sistema.

- Todos los casos relacionados con gestión de cambios deben registrarse en la lista de SharePoint “Registro de Gestión de Cambios” de la STI. Debe registrarse además de los cambios propuestos, la descripción clara, la respectiva justificación, la evaluación de impacto y la decisión tomada (aprobado, rechazado o pendiente de revisión). De igual modo se debe mantener un registro actualizado de los cambios realizados, incluyendo la documentación relacionada y las acciones tomadas.

- Todo cambio que sea aprobado por el Equipo de Gestión de Cambios debe ser registrado en el instrumento definido y elaborado para tal fin, con el propósito de llevar un control de todos los cambios realizados y el responsable de cada uno.

- El profesional asignado debe comunicar de manera oportuna y efectiva a todas las partes interesadas relevantes sobre los cambios propuestos, las decisiones tomadas y los plazos asociados. Notificar a los equipos involucrados sobre los cambios aprobados y las acciones requeridas, asegurando una adecuada coordinación y seguimiento.

- La STI debe realizar el seguimiento periódico para verificar el cumplimiento de la política de control de cambios y evaluar la efectividad del proceso y realizar revisiones posteriores a la implementación para evaluar el impacto de los cambios realizados y tener en cuenta lecciones aprendidas para futuros cambios.

- En todos los casos, la liberación de los cambios debe realizarse de manera ordenada en la fechas y horas definidas para evitar generar traumatismo.

Políticas de Seguridad

- La Dirección de Talento Humano y el supervisor del contrato debe reportar las novedades de personal y contratistas (ingreso, traslado, retiro, vacaciones, licencias no remuneradas o licencias de maternidad y reactivación) mediante la Mesa de Servicios a través del correo: soporte.oti@supersalud.gov.co. Lo anterior con el objeto de actualizar accesos, crear y eliminar usuarios de los sistemas de información de la SNS.

- El uso de la cuenta de usuario en los sistemas de información de la SNS debe ser responsabilidad de la persona a la que está asignada es para uso personal e intransferible y se protegerá mediante contraseña segura.

- Toda aplicación o sitio web que sean desarrollados para la Superintendencia Nacional de Salud deben acatar los “REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN” establecidos en el anexo “REQUERIMIENTOS DE SEGURIDAD PARA APLICACIONES – DIFT25”. El cumplimiento de estos requerimientos deberá ser revisados por el Grupo de Seguridad Digital de la STI

- Los roles y permisos asignados a los usuarios finales deben ser definidos por el jefe del área funcional, quién debe solicitar la asignación de permisos para los usuarios mediante comunicación a la STI (*a través del correo soporte.oti@supersalud.gov.co*), dando cumplimiento a lo definido en el presente documento.

- En ninguna circunstancia, se deben asignar roles y permisos de administrador a los usuarios de las áreas funcionales.

- Todas las aplicaciones de la Superintendencia Nacional de Salud deben tener la capacidad de proteger la información y los datos del acceso no autorizado tanto de usuarios, como por parte de sistemas de información.

- Todo proyecto de software debe contar con el visto bueno del oficial de seguridad de la entidad o quien sus veces.

- Todo desarrollo debe contar con un documento detallado de análisis de riesgos para lo cual puede apoyarse en la Estándar de Verificación de Seguridad en Aplicaciones de Owasp V3.0, o una versión liberada posteriormente y que se tenga disponible.

- Para todos los casos el oficial de seguridad o quien haga sus veces debe gestionar las vulnerabilidades detectadas en los desarrollos del software que entren en producción, realizando revisiones periódicas mensuales a los logs generados por las aplicaciones y por el servidor de aplicaciones.

- La Subdirección de Tecnologías de la Información mediante el uso de herramientas y técnicas criptográficas debe garantizar la protección, integridad y confidencialidad de la información sensible en todos sus estados (tránsito, en reposo y en uso).

- Todas las aplicaciones de software, desarrolladas para la Superintendencia Nacional de Salud, dispondrán de un módulo de administración para la asignación de usuarios, roles, perfiles y privilegios definidos en los diferentes sistemas de información para los usuarios, con log de auditoría para establecer traza de modificaciones.

- Para todos los casos, las aplicaciones implementadas en la Superintendencia Nacional de Salud solo podrán tener un único rol de administrador que se encarará de la configuración del Sistema de

Información, definir roles, perfiles y permisos para los usuarios del sistema. No podrán existir roles semejantes al de administrador.

- Las credenciales del usuario administrador son de uso exclusivo del funcionario que ostente dicho rol.

- Como mínimo una vez por trimestre o cuando se reporte una novedad, la STI debe revisar los usuarios asignados a cada Sistema de Información, con el fin de retirar los privilegios de acceso a quienes hayan cambiado de área funcional o ya no pertenezcan a la Entidad y por tanto ya no deban interactuar con el sistema.

- Cuando las actividades realizadas desde una cuenta de usuario comprometan la integridad y seguridad de la información, el administrador debe suspender la cuenta de manera temporal hasta tanto se hayan tomado las medidas necesarias que considere el Administrador del Sistema.

- El acceso a los archivos fuente de las aplicaciones, desarrolladas para la Superintendencia Nacional de Salud, se debe restringir al personal autorizado por el jefe de la Subdirección de Tecnologías de la Información.

- La Subdirección de Tecnologías de la Información debe proteger los archivos fuentes y las bases de datos de las aplicaciones propiedad de la Superintendencia Nacional de Salud.

- Todo contrato relacionado con el ciclo de vida de desarrollo de software o con la adquisición de software debe ser supervisado y monitoreado por la Subdirección de Tecnologías de la Información de la Superintendencia Nacional de Salud, con el fin que se cumplan con los requerimientos propios de la entidad y de la política de desarrollo de software.

- Todo contrato suscrito entre la Superintendencia Nacional de Salud y una persona natural o jurídica, cuyo objeto implique el desarrollo de un producto de software a la medida, debe garantizar la inclusión de la obligación que determine ceder los acuerdos de licenciamiento, propiedad de los códigos fuente y derechos de propiedad intelectual relacionados con el contenido de los aplicativos entregados a la Superintendencia Nacional de Salud, registrando los cambios en el código fuente en los repositorios oficiales de la entidad, conforme sea definido por la Superintendencia Nacional de Salud.

- La Subdirección de Tecnologías de la Información, como encargada de la administración y gestión de los usuarios en todos los sistemas de información y/o aplicaciones de la Superintendencia Nacional de Salud, debe asignar los privilegios teniendo en cuenta las funciones y el rol de cada usuario en el sistema, así como la verificación de identidad para ingreso al mismo.

- El uso y creación de contraseñas para usuarios de correos, bases de datos, sistemas de información y redes deben estar alineados al buen uso y creación de contraseñas seguras.

- La Subdirección de Tecnologías de la Información, de manera periódica y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo debe revisar los derechos de acceso de los usuarios a la Infraestructura Tecnológica y sistemas de información de la Superintendencia Nacional de Salud.

- Con el fin de garantizar la integridad, confidencialidad, disponibilidad de la información, la Subdirección de Tecnologías de la Información debe propender porque que las contraseñas de acceso a las aplicaciones se almacenen de forma cifrada utilizando un algoritmo de cifrado unidireccional.

- Toda aplicación desarrollada para la Superintendencia Nacional de Salud debe mantener un registro de las tres (3) últimas contraseñas utilizadas por el usuario, y evitar la reutilización de estas.

- Toda aplicación desarrollada para la Superintendencia Nacional de Salud debe cumplir con los lineamientos de política componente de seguridad de la información y seguridad digital en el apartado de suministro de control de acceso y gestión de contraseñas.

- Toda aplicación desarrollada para la Superintendencia Nacional de Salud debe establecer el uso de contraseñas individuales para determinar las responsabilidades de su uso.

- Toda aplicación desarrollada para la Superintendencia Nacional de Salud debe establecer los procedimientos para cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial hasta su baja del sistema de información.

- En todos los casos, los sistemas de información de la Superintendencia Nacional de Salud deben bloquear de manera automática las cuentas de los usuarios que no hayan ingresado durante los últimos sesenta (60) días.

- Toda aplicación desarrollada para la Superintendencia Nacional de Salud debe establecer que, luego de cinco (5) intentos fallidos de ingreso de contraseña, se bloquee la cuenta de usuario.

- Los usuarios de los sistemas de información de la Superintendencia Nacional de Salud deben evitar acceder a las aplicaciones de la entidad desde sitios públicos (salas de internet, bibliotecas, etc.) de los cuales se desconozca su nivel de seguridad.
- Los usuarios de los sistemas de información de la Superintendencia Nacional de Salud deben cambiar la contraseña si evidencia que su equipo ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.

- Los usuarios de los sistemas de información de la Superintendencia Nacional de Salud deben acceder a los servidores únicamente en las instalaciones de la entidad. Las actividades de tipo remoto deben contar con la debida autorización.

- Los usuarios de los sistemas de información de la Superintendencia Nacional de Salud deben responder por el uso de las credenciales de acceso asignadas.

- La Subdirección de Tecnologías de Información, debe efectuar el seguimiento a los accesos realizados por los usuarios, mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

- La Subdirección de Tecnologías de Información, debe autorizar previo estudio, la conexión a nivel remoto de los colaboradores o terceros que por su labor lo requieran.

- La conexión remota a la red de área local de la Superintendencia Nacional de Salud debe ser establecida a través de una conexión VPN segura, suministrada por la entidad y garantizar el registro y monitoreo de las actividades realizadas por el usuario.

- La Subdirección de Tecnologías de la Información debe garantizar el acceso a la red y aplicaciones de la Entidad solo a usuarios autorizados, previa definición, verificación y control de los perfiles y roles para el acceso a los diferentes sistemas de información, en coordinación con Dirección de Talento Humano y las áreas funcionales.

- La Subdirección de Tecnologías de la Información debe diseñar, documentar e implementar los controles necesarios para el acceso la infraestructura tecnológica, a fin de preservar la confidencialidad, integridad y disponibilidad de la información.

- Para todos los casos los privilegios sobre la información deben ser otorgados y mantenidos de acuerdo con las necesidades de la operación, limitando el acceso sólo a lo que sea requerido.

- Todo desarrollo que se realice para la Superintendencia Nacional de Salud debe garantizar la separación de ambientes (Desarrollo, Pruebas y Producción), con el objetivo de controlar de manera más eficiente los cambios al sistema de información y la seguridad de la información.

- Todos los desarrollos que se realicen para la Superintendencia Nacional de Salud se deben implementar y realizar las pruebas de integración necesarias, con el propósito de asegurar que, en las aplicaciones desarrolladas se hayan implementado los requisitos de seguridad requeridos antes de comenzar el desarrollo, documentando las pruebas realizadas y aprobando los pasos a producción.

- La Subdirección de Tecnologías de la Información, debe definir los roles y perfiles de los usuarios con acceso a los activos de información de cada proceso, teniendo en cuenta los riesgos de seguridad de la información asociados a cada uno de ellos.

- En los casos que aplique, todo desarrollo para la Superintendencia Nacional de Salud deberá tener en cuenta lo definido por Mintic, en las guías publicadas en el apartado “Controles de seguridad y privacidad de la información”.[7]

ANEXOS

- Requerimientos de Seguridad para Aplicaciones – Formato DIFT25

- Especificación de Caso de Uso - Formato DIFT37

[7] https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150511:Controles-de-seguridad-y-privacidad-de-la-informacion