POLÍTICAS ESPECÍFICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Contenido

1. INTRODUCCIÓN

Las organizaciones o entidades sin importar su tamaño sean éstas del sector público, privado, comercial o sin ánimo de lucro, recolectan, procesan, administran, almacenan y transmiten información de muchas formas entre ellas formatos electrónicos, físicos y comunicaciones verbales por ejemplo Conversaciones presentaciones Charlas

El valor de la información va más allá de palabras escritas, números e imágenes, incluido el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas de información intangibles. En un mundo como el actual que se encuentra interconectado y donde la información, los sistemas, las redes y el personal involucrado se consideran como otro activo importante para cualquier organización, por lo que ameritan o requieren protección contra diversos peligros.

Estos activos pueden ser objetos de amenazas deliberadas o accidentales, ocasionadas por cambios en los procesos, nuevas leyes y reglamentaciones, da igual forma se pueden hablar de vulnerabilidades inherentes a procesos, sistemas, redes y personas. Por lo que dadas las diversas formas en las que las amenazas pueden aprovecharse de vulnerabilidades qué perjudiquen a una entidad, siempre debe existir la presencia de riesgos que afecten la información y su seguridad con el fin de reducir la materialización de estos riesgos y proteger así la organización.

Proteger la información se puede lograr mediante un conjunto adecuado de controles, incluidas lineamientos o políticas, procesos, procedimientos, estructuras organizacionales, aplicaciones y elementos físicos. Por lo que se hace necesario establecer, implementar, hacer seguimiento, revisar y mejorar estos controles, asegurando que se cumplan los objetivos de la organización y protegiendo su información.

Por todo lo anterior la implementación de un sistema de gestión de seguridad de la información SGSI cómo lo especifica la norma ISO 27001, asume una visión holística y coordinada de los riesgos que pueden afectar la información implementando un conjunto amplio de controles bajo el marco de referencia global de un sistema de gestión coherente.

El Sistema de gestión de seguridad de la información (SGSI) hace parte del cumplimiento del Invima, frente a los requerimientos del Modelo Integrado de Planeación y Gestión MIPG, a la protección de la información enfocada en la gestión de riesgos, y al Modelo de Privacidad y Seguridad de la Información MSPI.

Por lo que el Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, implementando el modelo de seguridad y privacidad de la información adopta controles para asegurar la información y define políticas específicas en el Sistema de Gestión de Seguridad de la información que toman como base la normatividad y las regulaciones aplicables.

2. DEFINICIONES

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Activo de información:** Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Entidad y, en consecuencia, debe ser protegido
- **Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
- **Anonimización:** Método por el cual se pretende mitigar los riesgos que se pueden presentar al momento de compartir un activo de información que contenga datos sensibles o confidenciales permitiendo la divulgación de la información pública contenida y la protección de la información sensible o confidencial.
- **Autenticidad**: Es la condición de poder identificar que el generador o receptor (interlocutor) de la información es realmente quien dice ser.
- **Autenticación:** provisión de una garantía de que una característica afirmada por una entidad es correcta.
- **Ciberseguridad**: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Ciberespacio**: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.
- **Confidencialidad:** Principio básico que impide la divulgación de información a personas o sistemas no autorizados.
- **Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- **Disponibilidad:** Principio básico que permite encontrar la información a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Dispositivo móvil:** Es un dispositivo electrónico pequeño con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para acceder a información, administrarla y almacenarla, por ejemplo, un computador portátil de mano, Tablet, celulares de última generación entre otros.
- **Evento de seguridad de la información**: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
- **Gestión de incidentes de seguridad de la información:** procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión de riesgos**: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- **Impacto**: el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- **Incidente de seguridad de la información**: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información**: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.
- **Integridad:** Principio básico que busca mantener los datos libres de modificaciones no autorizadas.
- **Inventario de activos**: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc. que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- **No repudio**: También conocido como “no negación”, es la condición que evita que se niegue la autoría o recepción de un mensaje o información.
- **Propietario de la información:** es la unidad organizacional o proceso donde se crean los activos de información.
- **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior del instituto.

- **Responsable por el activo de información:** es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **Riesgo**: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.
- **Seguridad de la Información**: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta.
- **Sistema de información:** es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el Invima o de origen externo ya sea adquirido por la Entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.
- **Vulnerabilidad**: debilidad de un activo o control que pueda ser explotado por una o más amenazas.

3. ALCANCE

Todos los lineamientos establecidos en el presente documento aplican para todos los procesos, servidores públicos, contratistas y terceros o grupos de interés que utilicen la información generada y/o custodiada por el Invima.

4. OBJETIVO

El objetivo de las políticas específicas del sistema de gestión de seguridad del Invima es generar lineamientos para la implementación de controles que aporten a la protección de la información, estos lineamientos se definen de acuerdo con los requerimientos del modelo de seguridad y privacidad de la información MSPI de MINTIC, alineado con la Política de Seguridad Digital.

5. MARCO LEGAL Y/ O NORMATIVO

- Constitución Política de Colombia, art 15 y 20.
- LEY 23 DE 1982 sobre Derechos de Autor. Congreso de la República.
- Ley 87 de 1993, Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
- Ley 527 de 1999, Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
- Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
- Ley 599 DE 2000, Por la cual se expide el Código Penal.
- Ley 734 de 2002, Por la cual se expide el Código Disciplinario Único.
- La Ley 850 de 2003, por medio de la cual se reglamentan las veedurías ciudadanas.
- Ley 962 de 2005, Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- Ley 1150 de 2007, Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
- 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.
- Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo 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.
- Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 235 de 2010, por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas
- Decreto 884 de 2012, Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.

- Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014, por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
- Decreto Nacional 2573 de 2014, Estrategia de Gobierno en Línea de la República de Colombia
- Decreto 103 de 2015, títulos I, II, III, IV, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1081 de 2015, capitulo 4, por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.
- Decreto 1499 del 11 de septiembre de 2017, Integración del Sistema de Gestión de Calidad y lo Sistemas de desarrollo administrativo.
- Decreto 1413 del 25 de agosto de 2017, Los lineamientos que se deben cumplir para la prestación de servicios ciudadanos digitales, y para permitir a los usuarios el acceso a la administración pública a través de medios electrónicos
- Decreto 612 de 2018, Las entidades del estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión – MIPG, deberán integrar los planes institucionales y estratégicos al Plan de Acción de que trata el Artículo 74 de la Ley 1474 de 2011.
- Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Decreto 620 de 2020, Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- CONPES 3701, Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.
- CONPES 3854, Política Nacional de Seguridad Digital.
- CONPES 3995, Política Nacional de Confianza y Seguridad Digital
- Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009, Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones.
- NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC colombiana 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

6. CUMPLIMIENTO

Las políticas específicas de Seguridad de la información contenidas en este documento deben ser reconocidas aceptadas y cumplidas por todos los servidores públicos, contratistas, colaboradores y terceros del Invima. El incumplimiento de estas, se considerará un incidente de seguridad, que, de acuerdo con el caso, podrá dar lugar a un proceso disciplinario para los servidores públicos, y se podrá convertir en un incumplimiento del contrato respecto a los contratistas, que pueda dar lugar a la imposición de sanciones e incluso a la terminación del contrato, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

7.1. POLÍTICAS ESPECÍFICAS

7.1. Política para dispositivos móviles

- El uso de dispositivos móviles para la realización o ejecución de las actividades de un proceso en el Invima debe ser definido por el propietario de la información e identificando los riesgos que puedan afectar la información Ocasionados por este uso.
- El Proceso de Gestión de Tecnologías de la Información debe asegurarse del registro de los dispositivos móviles, las restricciones de instalación de software y su versionamiento, así como los requisitos de conexiones a servicios de información, controles de acceso, configuración de cifrado y protección contra software malicioso, todo esto antes de ser entregado al servidor público que los requiera para su trabajo.
- El proceso de Gestión de Tecnologías de la Información debe garantizar la configuración de borrado remoto, así como inhabilitarlo y cierre de todas las sesiones que el dispositivo móvil pueda tener configuradas.
- El uso de dispositivos móviles debe ser restringido y solamente usado para los casos específicos que se requieran por la labor que realiza un servidor público, teniendo en cuenta los requisitos legales, seguros y otros requisitos de seguridad para los casos de robo o pérdida de este.
- Todo servidor público que bajo su responsabilidad cuente con un dispositivo móvil o varios debe ser debidamente informado de las responsabilidades de seguridad de este o estos dispositivos, así como de los mecanismos diseñados para informar inmediatamente al responsable de informar a aseguradoras y al proceso de Gestión de Tecnologías de la Información en caso de pérdida del dispositivo.
- Para los casos de dispositivos móviles personales que se usan para realizar labores de la entidad, es importante considerar la separación entre el uso privado de la de uso para labores contractuales, esto incluye el uso de software y la protección de datos del Invima.
- El proceso de Gestión de Tecnologías de la Información debe garantizar conexiones seguras para accesos remotos donde se usen dispositivos móviles ya sean de propiedad de la entidad o dispositivos móviles personales usados para realizar labores contractuales en la entidad.
- Es necesario que el servidor público, contratista, pasante y tercero que use un dispositivo móvil, firme un acuerdo de confidencialidad y un acuerdo de usuario final en el que reconozca sus deberes así como el desistimiento de la propiedad de los datos almacenados en el

mismo, con el fin de permitir el borrado seguro y remoto de la información de la organización en el caso de robo pérdida, o cuando ya no se posee autorización para usar el servicio teniendo en cuenta la legislación sobre privacidad de la información.
- Junto con el proceso de Gestión de Tecnologías de la Información se debe pactar una periodicidad de copias de respaldo de la información que pueda estar almacenada en el dispositivo móvil, así como la definición de protocolos de almacenamiento seguro ya sea en unidades de almacenamiento compartidas en la red, en la nube, de forma remota o interna en las instalaciones del instituto.

7.2. Teletrabajo

- Teniendo en cuenta las directrices y lineamientos definidos en el Invima para realizar teletrabajo, trabajo en casa, a distancia o remoto se definen y determinan Algunos lineamientos sobre el acceso proceso y almacenamiento en modalidad de teletrabajo o trabajo en casa.
- Se debe identificar la seguridad física existente en el lugar donde se realizará teletrabajo y su entorno físico, los requisitos de seguridad en las comunicaciones teniendo en cuenta las necesidades de acceso remoto a los sistemas de información de la entidad y a la sensibilidad de la información a la que se tendrá acceso.
- El proceso de Gestión de Tecnologías de la Información es el encargado de definir los canales de comunicación y mecanismos de acceso a la información que el teletrabajador utilizará, teniendo en cuenta los requisitos de seguridad y protección de la información que viaja a través de estos medios.
- Es necesario identificar las amenazas que corresponden al acceso no autorizado a información o recursos del instituto por parte de otras personas que usan el mismo equipo de cómputo del teletrabajador ejemplo familias o amigos.
- Es indispensable la definición de requisitos de protección contra software malicioso en el equipo de cómputo ya sea móvil o de escritorio con el cual se realizará las labores de teletrabajo, así como la responsabilidad del proceso de Gestión de Tecnologías de la Información definir la protección o el acceso seguro a la información de forma remota.
- Se debe tener clara la clasificación de la información y mantener la protección de esta, a través de la definición de permisos de control de acceso remoto y horarios permitidos para este acceso.
- Se debe informar al teletrabajador sobre las reglas de acceso a la información evitando el uso del dispositivo, por parte de personas ajenas al Invima, con el fin de proteger la información que pueda llegar a ser almacenada en el equipo de teletrabajo o los mecanismos de acceso configurados en el mismo.

7.3. Uso Aceptable de Activos

- Teniendo en cuenta la importancia de los activos de información o que administren información Se presentan algunas reglas para su uso aceptable, Es importante aclarar que se consideran activos de información Todos aquellos activos asociados con la información, sus medios de almacenamiento y las instalaciones de procesamiento.
- Se deben identificar los activos de información, así como valorarlos en cuanto a su integridad, confidencialidad y disponibilidad según sea el caso con el fin de generar conciencia sobre los requisitos de seguridad que estos deben tener de acuerdo con la criticidad de la información que contengan.
- El acceso a las instalaciones de procesamiento de información debe ser definido por los responsables de estas, así como mantener una bitácora de las acciones realizadas en las mencionadas instalaciones de procesamiento.
- Los servidores públicos y/o contratistas que tengan acceso a las instalaciones de procesamiento deberán contar un acuerdo de confidencialidad debidamente estipulado de acuerdo con los requisitos de seguridad y protección de la información.
- Se debe definir un responsable de los activos de información identificados, en la eventualidad que éste se retire o termine su vinculación laboral con el Invima, deberá entregar los activos físicos y electrónicos o digitales que tenga a su cargo, para que sea el Invima el que determine qué se hará con esta información y a quién definirá como su nuevo propietario o responsable.
- Se debe formalizar y socializar el proceso de devolución de activos físicos y electrónicos, de tal forma que se tenga en cuenta en el momento de entregar paz y salvo a un servidor público o contratista que termine su vinculación laboral con el Invima.
- Para los contratistas, pasantes o terceros que tengan acceso a información ya sea esta privilegiada o no del instituto esta información Deberá ser salvaguardada y permanecer bajo la custodia del Invima, no se debe permitir qué información de la entidad esté por fuera de la custodia y protección que el Invima a determinado o definido para esta.
- Se debe controlar el copiado no autorizado de la información pertinente por parte de empleados o contratistas que finalicen su vínculo laboral por ejemplo temas de propiedad intelectual.
- Se debe valorar la información Frente a los pilares de seguridad de la información Que son la confidencialidad o permisos de acceso, integridad o veracidad de la información, Y disponibilidad o facilidades de acceso.
- Se debe evitar la divulgación, modificación, Retiro destrucción No autorizada de la información que se encuentra almacenada en los diferentes medios tecnológicos o físicos.
- Se debe establecer lineamientos o protocolos debidamente formalizados para la disposición segura de medios con el fin de minimizar los riesgos de fuga de información confidencial a personas no autorizadas.
- Se debe identificar los medios que se utilizan Para la transferencia de información Ya sean estos medios físicos o digitales, para los medios físicos se deben determinar lineamientos de protección Y acuerdos de confidencialidad con los servicios de mensajería o transporte de documentos, para los medios digitales es necesario determinar y configurar medios de transferencia de información Que garanticen la protección y seguridad de esta.
- Los activos de información del Invima deben ser usados para fines estrictamente laborales y orientados a garantizar la prestación de los servicios necesarios y el cumplimiento de la misión del instituto el uso diferente no debe ser autorizado.

7.4. Usos medio tecnológicos de comunicación y acceso a Internet

- El servicio de acceso a internet es de uso exclusivo para las tareas o actividades propias de la misión del instituto, los usos diferentes al cumplimiento de las funciones asignadas son de entera responsabilidad del usuario a quién se le ha configurado el acceso.

- El acceso a internet por parte de personal externó que se encuentre dentro de las instalaciones del Invima debe ser configurado y segmentado de forma independiente a los segmentos de red definidos para el acceso a la información por parte del personal que cuenta con una vinculación laboral con el Invima.
- El Proceso de Gestión de Tecnologías de la Información es responsable por la configuración y la restricción de acceso a sitios qué pueden estar comprometidos o de dudosa reputación en la red, el abuso de estos privilegios o la manipulación de estas configuraciones acarreará investigaciones disciplinarias.
- Los servicios a los que cada usuario pueda acceder desde internet dependerán del rol definido para él mismo, rol que se debe encontrar debidamente autorizado y documentada.
- El Invima puede supervisar el acceso del servicio a internet con el fin de certificar que se está usando en el cumplimiento de las funciones institucionales, respetando el derecho a la intimidad y privacidad del titular de la cuenta de acceso a internet.
- Los accesos a sitios web por parte del usuario que son considerados ilegales por normatividad colombiana, la ley de delitos informáticos y aquellos prohibidos por ley de infancia y adolescencia serán informados a las autoridades competentes para su debida investigación y actuación.
- Todo usuario es responsable del contenido de las comunicaciones cómo de cualquier información que envíe desde la red del instituto o descargue desde el internet empleando cuentas de acceso suministradas por el Proceso de Gestión de Tecnologías de la Información del Invima.
- Todos los usuarios se deben abstener del envío o descarga de información Sometida a derechos de autor por ejemplo música, vídeos, obras literarias, imágenes entre otros.
- El correo electrónico debe ser usado para comunicaciones oficiales internas o externas en el cumplimiento de las funciones asignadas en el Invima.
- El uso del correo electrónico para Compartir información Confidencial o reservada sin la debida autorización acarrea investigaciones disciplinarias.
- Se debe definir una firma para los correos electrónicos donde se garantice la perfecta identificación del servidor público, contratista o persona con la que se tenga un vínculo laboral, qué, por sus funciones requiera una cuenta de correo electrónico.

7.5. Política de Control de Acceso

- Proceso de Gestión de Tecnologías de la Información, es quien gestiona el control de acceso a través de usuario y contraseña, acceso a nivel de red, sistema operativo, sistemas de información y servicios tecnológicos, con la finalidad de mitigar riesgos asociados al acceso a la información, salvaguardando la integridad, disponibilidad y confidencialidad de esta en el Invima.
- La creación, reactivación o desactivación de usuarios de la red o sistemas de información, al igual que los roles y permisos otorgados, los realizará el Proceso de Gestión de Tecnologías de la Información a solicitud del Coordinador del proceso de Gestión de Talento Humano o su delegado, el Coordinador del proceso Contractual o su delegado, de acuerdo con lo establecido por los propietarios de la información a la que tendrá acceso el usuario.
- Las contraseñas serán de uso personal e intransferible, se considera un activo de información de carácter reservado por lo que no debe ser divulgada a ningún otro usuario, incluidas los jefes inmediatos o alguna autoridad dentro de la entidad.
- Se debe acceder a los sistemas de información o dispositivos de red a través de la cuenta de usuario asignada, la cual debe cumplir con los controles y estándares de seguridad definidos.
- Se debe socializar con los servidores públicos, contratistas y terceros las reglas de control de acceso definidas por el Invima y las políticas de control de acceso, así como las responsabilidades que se tienen frente a los medios físicos y lógicos que permitan el acceso a la información Y las consecuencias de no aplicar estos requisitos de seguridad.
- La definición de los roles para el control del acceso a la información debe ser acordé a la identificación y clasificación de la información tanto en los sistemas de información, redes, unidades de almacenamiento compartidas, como en el acceso físico a áreas restringidas o donde se encuentra información confidencial o reservada.
- Se debe mantener un registro de todos los eventos significativos concernientes al uso y gestión de autenticación e identificación de usuarios y sus acciones dentro de la red.
- Se debe estipular la periodicidad con la que los usuarios deben cambiar su contraseña, así cómo definir los parámetros de seguridad en la creación de la contraseña.
- Se debe estipular e implementar un proceso formal para el registro y cancelación total o temporal de usuarios y sus permisos de acceso.
- El acceso a los códigos fuente de los aplicativos o sistemas de información debe ser controlado con el fin de reducir potenciales riesgos de corrupción en los mismos y en la manipulación de la información, así como definir un registro de auditoría de todos los accesos y generar copias de respaldo sujetas a cambios realizados.

7.6. Uso de controles criptográficos - gestión de llaves

- Se debe definir por parte de la dirección el enfoque y uso de los controles de cifrado de información para el Invima, incluyendo los principios bajo los cuales se debe proteger la información de la entidad.
- De acuerdo con la valoración de riesgos, la identificación y valoración de los activos de información sea esta confidencial o reservada o contenga datos sensibles, se debe establecer los mecanismos de cifrado necesarios para garantizar su protección en el acceso, almacenamiento y transferencia de la información.
- Se debe establecer un responsable de la implementación de la presente política para la gestión de las llaves, incluida su generación y teniendo en cuenta las normas o lineamientos a adoptar de forma efectiva en toda la entidad mediante soluciones adecuadas a las necesidades del instituto.
- La implementación de los controles de cifrado puede ser usada para proteger la confidencialidad, la integridad, el no repudio y la autenticidad de la información.

- Las llaves de cifrado deben ser definidas con un ciclo de vida que incluya la generación de la clave, su almacenamiento, archivo, recuperación, distribución, retiro y destrucción.
- Todas las llaves o claves de cifrado deben ser protegidas contra la modificación no autorizada, perdida uso y divulgación no autorizadas, además los equipos usados para generar estas llaves deben estar protegidos físicamente siendo ubicados en áreas de acceso restringido.
- Es necesario realizar copias periódicas del respaldo de las llaves y archivarlas, así como registros de auditorías de las actividades relacionadas con la gestión de las llaves con el fin de reducir la posibilidad de uso inapropiado.

7.7. Escritorio y pantalla limpios

- Se debe tener en cuenta la clasificación de la información, Los requisitos legales y contractuales y los riesgos identificados en el Invima para determinar la información sensible o crítica que se puede encontrar en papel o en medio de almacenamiento digital y que debería ser guardada y protegida cuando no sea requiera, especialmente cuando el puesto de trabajo se encuentre desatendido (libre o desocupado).
- Todo el personal que cuente con acceso a la red al ausentarse del puesto de trabajo debe asegurarse de bloquear su equipo de cómputo y evitar así el acceso a la información Y el uso de los recursos o sistemas de información Por personal no autorizado.
- Se deben conservar sobre el escritorio únicamente los documentos necesarios para realizar sus actividades, si el responsable de esta documentación debe ausentarse de su puesto de trabajo, toda información identificada como pública reservada o pública Clasificada, así como los documentos que contengan información sensible deben ser guardados de forma segura, de igual forma se debe realizar esta actividad al terminar la jornada laboral.
- se debe evitar el uso no autorizado de fotocopiadoras o cualquier tipo de tecnología que permita reproducir información Por ejemplo escáner cámaras digitales para reproducir información catalogada como pública reservada o pública clasificada.
- Si se debe imprimir información en impresoras conectadas a la red debe garantizarse qué esta información será impresa bajo la vigilancia de la persona autorizada y llevar un control de esta.

7.8. Copias de respaldo

- Se deben realizar copias de respaldo a los sistemas de información, a la información, las aplicaciones y las configuraciones de servidores ya sean éstos virtuales físicos y poner a prueba regularmente las copias realizadas.
- De acuerdo con las necesidades de las áreas o procesos se deben definir los intervalos de tiempo en los que se realizarán las copias de respaldo de información, así como la verificación de estas en compañía del propietario o responsable de la información a la que se le realizó la copia de respaldo.
- Teniendo en cuenta los tiempos estipulados en las tablas de retención documental, las definiciones de conservación de la información y los requisitos legales se deben retener y proteger las copias de respaldo.
- Las copias de respaldo y sus pruebas de restauración deben ser documentadas con el fin de garantizar las pruebas de ejecución.
- Las copias de respaldo deben ser almacenadas en lugares remotos y a una distancia prudente que permitan mitigar los riesgos de pérdida de información en el caso de eventos que afecten las instalaciones del instituto.
- Se debe garantizar la protección física de las copias de respaldo, así como de los medios en los que se realizan estas copias.
- Las copias de respaldo que contengan información de carácter pública reservada o pública clasificada deberán ser protegidas por medio de cifrado.
- Las copias de respaldo de sistemas y servicios deberán ser probadas con mayor regularidad con el fin de asegurarse que cumplen con los requisitos de los planes de contingencia y continuidad de la operación, para los casos de sistemas y servicios críticos del Invima lo dispuesto para las copias de respaldo debe abarcar toda la información de sus sistemas, aplicaciones y datos necesarios para recuperar la operación de forma completa en caso de desastre.

7.9. Transferencia de información

- Se debe definir con cada proceso y área la información que requieren transferir como parte del ejercicio y ejecución de sus responsabilidades dentro del instituto y determinar los mecanismos de actualización de esta información En caso de eliminar privilegios de transferencia, crear nuevos privilegios para la transferencia y determinar los requisitos legales o de temporalidad en la transferencia de la información.
- Se debe contar con mecanismos tecnológicos que permitan proteger la información que se transfiere contra cualquier tipo de interceptación, copiado, modificación, en ruta do y destrucción.
- Por medio del uso de aplicaciones o de arquitectura segura que permita detectar el intento de instrucción o ejecución de software malicioso se debe proteger la información que se transfiere o comparte con terceros.
- Los usuarios deben evitar dejar mensajes o información confidencial en mensajes de voz Configurados en buzones empresariales, máquinas contestadoras o teléfonos celulares, esto con el fin de evitar que personas no autorizadas puedan tener acceso a esta información Ya sea por escuchas mal intencionadas o errores en la marcación.
- Se debe sensibilizar a los servidores públicos, contratistas o terceros que presten servicios a la entidad sobre conversaciones confidenciales en lugares públicos o mediante canales de comunicación no seguros.
- Se debe contar con acuerdos de transferencia de la información ya sea con empresas prestadoras de servicio de mensajería electrónica o física, donde se especifiquen las responsabilidades del acceso a la información no autorizado o divulgación de esta, así como la reserva de la información a la que pueden tener acceso por la prestación de sus servicios.
- La información que viaja a través de la mensajería electrónica debe ser protegida contra el acceso no autorizado, modificación o posible denegación del servicio de forma proporcional al esquema de clasificación de la información adoptado por el Invima.
- Se debe garantizar la anonimización de la información de carácter reservado o confidencial al momento de compartir el contenido de un activo de información Con cualquier entidad o persona.

- Se deben definir los requisitos de uso de firmas electrónicas para garantizar el no repudio de la información transmitida o recibida a través de medios de mensajería electrónica.
- Se deben establecer acuerdos de confidencialidad y no divulgación con los terceros ya sean estos públicos, privados de naturaleza jurídica o personal que puedan acceder a la información del instituto y puedan de forma directa o indirecta transferir o compartir esta información.

7.10. Desarrollo seguro

- Se deben establecer reglas para el desarrollo seguro en los sistemas de información y/o aplicaciones que sean implementadas en su ciclo de vida.
- En el ambiente de desarrollo de software se debe definir una metodología que garantice directrices de codificación seguras para los lenguajes de programación usados.
- En la fase del diseño se deben definir los requisitos de seguridad los chequeos o puntos de control para la verificación De la seguridad en el desarrollo y sus futuros versión amientos
- Se deben realizar pruebas durante el desarrollo que permitan evitar encontrar y resolver vulnerabilidades
- Se debe contar con técnicas de programación segura tanto para los nuevos desarrollos, como para escenarios de reúso de código y considerar estándares de codificación para los casos donde esto sea pertinente, además los desarrolladores deben recibir formación sobre el uso y prueba de verificación en la revisión de estos códigos.
- En caso de contratar un desarrollo externó, el Invima debe asegurarse de que este externo contemple reglas de desarrollo seguro y pruebas técnicas propias que puedan garantizar la seguridad de la aplicación o sistema de información contratado.
- Se debe contar con un procedimiento formal para el control de los cambios en el desarrollo de sistemas de información o aplicaciones y desde las primeras etapas de su diseño se deben aunar esfuerzos para el mantenimiento de la seguridad y confidencialidad de la información.
- Los cambios que se lleguen a efectuar en sistemas de información o aplicaciones deben ser debidamente documentados y justificados se deben especificar pruebas control de calidad y gestión en la implementación.
- Se deben realizar pruebas técnicas frente a la seguridad de las aplicaciones nuevas y a las que se les realizaron cambios, Asegurándose de la revisión De los procedimientos de integridad y control de las aplicaciones con el fin de determinar que no se encuentran comprometidas en su operación.
- Se debe garantizar que los cambios a ser implementados o puestos en producción cuenten con las pruebas necesarias antes de ser implementadas dadas con el fin de mitigar riesgos de continuidad en la operación.
- Para el desarrollo interno se deben garantizar datos de prueba seleccionados y controlados cuidadosamente, Si se usa información Operacional esta debe ser borrada inmediatamente después de finalizar las pruebas y su copiado y uso debe ser registrado en los de auditoría.
- La aplicación de parches o puesta en producción se debe realizar de forma metódica con pruebas de puesta en producción previas y copias de respaldo del ambiente de producción actual.

7.11. Relación con proveedores

- Se deben identificar y documentar los diferentes tipos de proveedores con los que la entidad cuenta actualmente por ejemplo proveedores en servicios de tecnología, almacenamiento, mensajería, servicios de aseo y vigilancia, entre otros a quienes el Invima les permitirá acceso a sus instalaciones y/o a su información.
- Se deben identificar y definir los requisitos mínimos de seguridad de la información para cada uno de los tipos de acceso que puedan tener los proveedores con base en las necesidades y requisitos de la entidad y su perfil de riesgo frente al acceso a la información de la entidad.
- De acuerdo con los servicios y obligaciones que el proveedor contraiga con el Invima se deberán firmar acuerdos de confidencialidad que incluyan al personal contratado por el proveedor. Donde se incluya el manejo de incidentes y contingencias asociadas al acceso que el proveedor pueda tener incluidas las responsabilidades de la entidad.
- Se debe identificar los riesgos de seguridad por la gestión De transacciones el uso de instalaciones de procesamiento de información Y cualquier otro mecanismo de administración, acceso o almacenamiento Por parte del proveedor.
- Se deben definir los acuerdos de nivel en la prestación del servicio Y la prioridad que estos deben tener de acuerdo con los riesgos de disponibilidad identificados por el Invima, con el fin de mantener la continuidad de la operación.
- Para los servicios esenciales contratados con proveedores se debe contar con una planeación de adquisición de servicios que mantenga la continuidad de este, sin que se presenten espacios de tiempo en los que estos servicios no se presten a la entidad.

8. PREMISAS DE OPERACIÓN

8.1. No repudio

El Invima a través del proceso de Gestión de Tecnologías de la Información se reserva el derecho de auditar las redes y sistemas periódicamente para asegurar el cumplimiento de la Política de Seguridad y Privacidad de la Información.

El uso de los sistemas de información del Invima debe ser monitoreado con el objetivo de identificar algún intento de intrusión. El monitoreo debe contemplar como mínimo los siguientes puntos:

- Intentos fallidos recurrentes para tener accesos a los sistemas.

- Intentos deliberados para evadir los controles de seguridad establecidos.
- Altas y bajas de usuarios en sistemas sin una solicitud aprobada correctamente.
- Modificaciones en los privilegios de usuarios sin una solicitud aprobada correctamente

Para tener control, los registros de auditoría deben ser respaldados de forma periódica y se debe proporcionar un reporte periódico mensual de los incidentes de seguridad identificados

8.2. Privacidad y Confidencialidad

El Invima, aplicara la política de Tratamiento y Protección de Datos Personales para toda la información que contenga datos personales los cuales deben ser identificados a través del inventario de Bases de datos personales.

Todo funcionario, contratista, colaborador, pasante y/o tercero que ingrese a la Entidad, debe leer y firmar el compromiso de Acuerdo de Confidencialidad, en el caso que maneje o tenga acceso a la información pública clasificada y/o reservada y tratamiento de datos personales.

8.3. Integridad

Todos los sistemas de información del Invima deben:

- Identificar e informar las fallas para que el encargado de la administración del sistema de información pueda corregir las fallas y evitar afectación en la información.
- Si el sistema operativo donde se aloja el aplicativo requiere actualizaciones, se deben realizar pruebas antes de proceder a la actualización, para evitar fallas en la ejecución de los sistemas de información o aplicativos de la entidad.
- En el proceso de gestión de cambios es necesario incluir las correcciones que se requieran.

Frente a la protección contra código malicioso, todos los sistemas del Invima deben:

- Emplear mecanismos de protección de código malicioso en las estaciones de trabajo, servidores o dispositivos de computación móvil para detectar y erradicar el código malicioso.
- Actualizar los mecanismos de protección de códigos maliciosos (incluidas las definiciones de firmas)
- Configurar mecanismos de protección de código malicioso (por ejemplo, análisis en tiempo real, análisis periódicos, detección de códigos maliciosos) para proteger los sistemas y activos de información de la empresa.

Respecto al monitoreo del Sistema de Información: Todos los sistemas del Invima deben:

- Identificar el uso no autorizado de los activos de información.
- Aumentar el nivel de actividad de monitoreo de activos de información siempre que exista una indicación de un mayor riesgo para los activos de la Entidad, basados en información del CSIRT, u otras fuentes creíbles de información.

Asegurarse que los usuarios de terceros, que requieren información del Invima que contengan información clasificada o reservada, hayan firmado un acuerdo de confidencialidad de la información o en el caso de contratistas, que el acuerdo este incluido como parte del contrato firmado con el Invima. El acuerdo de confidencialidad debe firmarse antes de intercambiar cualquier tipo de información clasificada o reservada y se determinará su vigencia, acorde con el tipo de información que se maneje (incluso después de terminado el vínculo contractual o laboral con la Entidad).
Para los casos en que el Invima, lleve a cabo intercambio de información con otras entidades deben existir procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información a intercambiar a través de cualquier tipo o infraestructura de comunicaciones, con base en la clasificación de la información, las políticas de seguridad y procedimientos del Invima.

8.4. Disponibilidad del Servicio e Información

Se debe crear y mantener un seguimiento al entorno de disponibilidad de los servicios y los componentes de la infraestructura para garantizar que los requerimientos de disponibilidad futuros puedan ser cubiertos.

El Comité Institucional de Gestión y Desempeño debe definir una estrategia para la continuidad del negocio, así como desarrollar, documentar, probar y mantener el Plan de Continuidad, que conduzca a la restauración de los procesos críticos del negocio y así dar continuidad en el servicio a las partes interesadas.

Dentro del proceso de desarrollo del plan de continuidad se debe hacer énfasis en mantener niveles de seguridad de información acordes con el resultado del análisis de riesgo y su clasificación, dentro de los procesos alternos utilizados antes, durante y después de la contingencia. Los documentos e información necesaria para llevar a cabo el proceso de continuidad del negocio deben ser clasificados como información “confidencial”.

La información debe ser copiada y resguardada en un lugar fuera de las instalaciones del Invima.

8.5. Registro y Auditoria

Todos los sistemas y/o aplicativos deben generar logs o trazas de auditoría, para los desarrollos de los Sistemas de Información que se generen a partir de la divulgación de esta política, se debe establecer este punto como obligación contractual.

Todos los logs del sistema y de las aplicaciones deben mantenerse en forma segura, de tal forma que evite el acceso no autorizado a esta información y deberán analizarse para determinar si existen intentos de vulneración del sistema.

Las siguientes actividades deberán ser registradas en el momento que sean desarrolladas por un sistema:

- Crear, leer, actualizar o eliminar información.
- Iniciar una conexión de red
- Aceptar una conexión de red
- Autenticación y autorización de los usuarios y desconexión de estos
- Conceder, modificar o revocar derechos de acceso, incluyendo la adición de un nuevo usuario o grupo, cambio en los niveles de privilegios de usuario, cambio de permisos de archivos, cambio de permisos de objetos de base de datos, cambio de reglas en el Firewall y cambios de contraseñas de usuario.

Cambios en la configuración de sistemas, redes o servicios, incluida la instalación de software, parches y actualizaciones, u otros cambios de software instalados. Todos los registros deberán contener los siguientes elementos de forma directa o indirecta:

- Tipo de acción: autorizar, crear, leer, actualizar, eliminar y aceptar.
- Subsistema que realiza la acción.
- Identificadores para el sujeto que solicita la acción.
- Identificadores para el objeto sobre el que se realizó la acción.
- Fecha y hora en que se realizó la acción, incluida la información pertinente sobre la zona horaria.
- Si la acción fue permitida o denegada por mecanismos de control de acceso: Descripción y/o razón de los códigos que indican que la acción fue denegada por el control de acceso, si aplica.

8.6. Gestión de Incidentes de Seguridad de la Información

El Invima cuenta con un procedimiento de Atención y Gestión de Incidentes en el que se puede reportar, registrar y dar tratamiento de los incidentes de seguridad de la información.

- Los usuarios deben asegurar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al proceso de Proceso de Gestión de Tecnologías de la Información para que se tomen las medidas correspondientes.
- Proceso de Gestión de Tecnologías de la Información, a través de su equipo de trabajo, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades detectadas en la plataforma tecnológica de la entidad.

8.7. Capacitación y Sensibilización en Seguridad de la Información

Todos los servidores públicos, contratistas, colaboradores y terceros deben recibir la inducción para tomar conciencia de la Seguridad de la Información y sus responsabilidades. Así como también debe participar en todas las actividades establecidas en el plan de capacitación, sensibilización y comunicación teniendo en cuenta que esto permite fortalecer la cultura de seguridad de la información y disminuir los posibles incidentes de seguridad de la información.

ELABORÓ	REVISÓ	APROBÓ
Nidia Nayibe Gonzalez Pinzon **Contratista**	Daladier Medina Niño **Jefe Oficina Asesora de Planeación**	Francisco Augusto Giuseppe Rossi Buenaventura

Fecha de elaboración: 01/11/2022	**Fecha de revisión:** 01/11/2022	**Director General** **Fecha de aprobación:** 01/11/2022