1. INTRODUCCIÓN

El presente manual de seguridad de la información establece los controles generales que el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - INVIMA debe implementar, con el fin de proteger la información generada, administrada, almacenada, procesada y publicada apoyándose en las políticas definidas en el presente documento, que pretende generar y socializar controles para la mitigación de futuros riesgos, la calidad de la información y la prestación continua de los servicios, supervisando la actividad diaria y reaccionando con certeza ante cualquier incidente.

2. OBJETIVO DEL MANUAL

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, para la implementación de controles que aporten a la protección de la información y que son complemento a lo definido en la “Política General de Seguridad de la Información de la Entidad” con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA.

3. ALCANCE DEL MANUAL

El presente manual de políticas aplica a funcionarios, contratistas, terceros, usuarios y visitantes del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA que por alguna razón tengan cualquier tipo de interacción con los activos de información.

4. 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: se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
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.
BYOD: El término BYOD, las siglas en inglés de «traiga su propio dispositivo», hace referencia a la política de seguridad de la información que determina cuándo y cómo pueden los servidores públicos utilizar sus propios ordenadores portátiles, smartphones y otros dispositivos personales en la red del INVIMA para acceder a los datos institucionales y realizar sus funciones laborales. Los equipos BYOD no son propiedad del INVIMA.
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: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
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: Propiedad de la información que busca preservar su exactitud y completitud.
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.
Sistema de Gestión de Seguridad de la Información: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas.

5. POLÍTICAS
El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

POLÍTICA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES
La gestión de riesgos se realiza para apoyar el logro de los objetivos estratégicos, misionales, de apoyo y, de evaluación y mejora del Instituto.

El control de riesgos se realiza de forma permanente al interior de los procesos estratégicos, misionales, de apoyo y de evaluación y mejora.
Los resultados de las actividades de gestión de riesgo son insumos para la toma de decisiones sobre seguridad de la información, ciberseguridad y protección de datos personales por parte de la dirección.
La gestión de los riesgos utiliza la mejor información disponible en los procesos estratégicos, misionales, de apoyo y, de evaluación y mejora para diseñar las estrategias que permitan reducir la probabilidad e impacto de eventos no deseados que afecten los objetivos estratégicos, misionales, de apoyo y, de evaluación y mejora.
Todas las acciones de gestión de riesgo toman en consideración las capacidades, conocimientos, herramientas y tecnología de información y comunicaciones que están disponibles en los procesos estratégicos, misionales, de apoyo y, de evaluación y de mejora para diseñar controles que sean reales y aplicables que permitan reducir la probabilidad e impacto de eventos no deseados.
La gestión de riesgo se adapta continuamente a los cambios en el entorno interno y externo que afectan a las capacidades del INVIMA para salvaguardar la seguridad
de la información, la ciberseguridad y la protección de los datos personales que

están bajo su responsabilidad.

POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.
Se debe identificar, definir y articular los mecanismos técnicos, tecnológicos y de personal que permitan proteger la privacidad de la información de los empleados, validando el cumplimiento de las normas y legislación vigente relacionada con la protección de datos personales.
Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.
Todo el personal que ingrese a la entidad ya sea de planta, contratista o personal contratado por un proveedor que requiera acceso a información física o digital, a un sistema de información, elemento técnico o tecnológico, custodia, almacenamiento o cualquier tipo de actividad relacionada con la información debe tener una socialización del Sistema de Gestión de Seguridad de la Información y sus políticas.

POLÍTICAS PARA EL TELETRABAJO Y ACCESO REMOTO A LA INFORMACIÓN

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 con el apoyo del Oficial de Seguridad 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, teniendo en cuenta las indicaciones del Oficial de Seguridad de la Información.
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.

POLÍTICAS PARA EL ALMACENAMIENTO DE LA INFORMACIÓN

Con el fin de mantener salvaguardad la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA esta debe ser almacenada en
los medios tecnológicos dispuesto para tal fin, y socializados por el proceso de
Gestión de Tecnologías de la Información.
La información almacenada en los repositorios dispuestos por el proceso de Gestión de Tecnologías de la Información será respaldada de acuerdo con lo definido en la política de copias de seguridad y de acuerdo con la o las herramientas tecnológicas disponibles para su ejecución.

POLÍTICAS DE GESTIÓN DE ACTIVOS

Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA.
Los activos dispuestos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA para el apoyo de las labores desempeñada por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral del Instituto Nacional de Vigilancia de Medicamentos y Alimentos

INVIMA.
El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA identificará, clasificará y gestionará su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados y aprobados.
Los terceros que tengan acceso a dispositivos técnicos, tecnológicos que almacenen, soporten o se encuentren destinado a la protección de la información deberán ser parametrizados y actualizados de acuerdo con las necesidades derivadas de las amenazas técnicas, tecnológicas y/o de ingeniería social que se presenten en un momento determinado
Toda información digital impresa y/o que se conozca de forma verbal por asistencia o participación en reuniones es de uso exclusivo del INVIMA para su operación y no se podrá difundir a menos que se cuente con la autorización respectiva.
Es responsabilidad del funcionario, contratista o tercero el cuidado, manejo y cumplimiento de los requisitos de seguridad de la información en los activos de información que le sean asignados, que estén a su cargo o administre.
La instalación de software en los equipos de computo suministrados por El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, se debe restringir, por lo tanto, toda solicitud de instalación de cualquier tipo de software debe tramitarse a través de un ticket a la mesa de servicio.
Los mecanismos tecnológicos de almacenamiento que ha dispuesto el Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA deben ser utilizados exclusivamente para almacenar información relacionada con las responsabilidades y obligaciones laborales o contractuales.

POLÍTICAS DE CONTROL DE ACCESO LÓGICO

Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.
Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.
Los accesos físicos o lógicos a instalaciones, aplicaciones, repositorios serán completamente restringidos durante los periodos de vacaciones, licencias o cualquier permiso o ausencia mayor a 15 días. Salvo excepciones específicas para personal de confianza y presidentes de sindicatos.
Los permisos de acceso a las áreas seguras o a información física o digital deberán ser otorgados por los lideres del área o propietarios de la información.
La validación de los usuarios activos y accesos a la información será realizada por el Oficial de Seguridad de la Información o quien designe la dirección general de la entidad en caso de ausencia de este.
Se podrá bloquear el acceso a la información o instalaciones a cualquier funcionario, contratista o tercero cuyo usuario se haya visto comprometido por cualquier motivo y se procederá de acuerdo con el control tecnológico activo en el momento

CRIPTOGRAFÍA

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA implementará herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información. Así mismo el proceso de Gestión de Tecnologías de la Información junto con el Oficial de Seguridad de la Información determinará los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera y de acuerdo con la valoración de confidencialidad de la información a cifrar.

POLÍTICAS PARA LA TRANSFERENCIA DE LA INFORMACIÓN

Se debe identificar y socializar los medios que se pueden utilizar 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 usuarios deben utilizar los medios de transferencia aceptados solo para temas relacionados con la misión del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, y con sus labores institucionales, cumpliendo con las políticas presentadas en el presente Manual.
Toda información que se transfiera debe ser evaluada en cumplimiento de la ley de transparencia 1712 de 2014 y la de protección de datos personales 1581 de 2012. Así como sus decretos reglamentarios vigentes.
Toda transferencia de información debe ser formalizada, se deben identificar los medios técnicos o tecnológicos de transferencia, duración del acuerdo de
transferencia, definir las responsabilidades de protección de la información de

acuerdo con la legislación vigente y que aplique, definir los responsables de cada actor (quien envía y quien recibe), el uso que se le dará a la información y los tiempos de conservación de esta.

POLÍTICAS DE 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 o 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 de forma segura y con las protecciones necesarias en lugares remotos, nube y/o a una distancia prudente que permitan mitigar los riesgos de pérdida de información en el caso de eventos que afecten las instalaciones del instituto.
Las copias de seguridad realizadas deben ser debidamente rotuladas, maquilladas o nombradas con el fin de ser fácilmente identificable su contenido y la fecha de realización

POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO
El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la integridad, confidencialidad y disponibilidad de la información. Su revisión y seguimiento se deberá realizar al menos una vez al año.
El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.
Todas las personas que ingresen a las instalaciones del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.
Se debe procurar la seguridad física, continuidad energética y debida protección ante posibles amenazas ambientales y naturales de todos los equipos de cómputo y elementos tecnológicos que soporten la operación misional de la entidad.
Todo el personal que labore o se encuentre de visita dentro de las instalaciones del Invima sebe portar su carnet o identificación como visitante de forma visible, en las situaciones donde no sea visible la identificación esta puede ser solicitada.
El ingreso de todo personal interno y externo a los centros de procesamiento de datos, debe quedar debidamente registrado en una bitácora o formato de ingreso y salida.
El personal de vigilancia debe registrar en una bitácora, formato o medio tecnológico el ingreso y retiro de todo dispositivo, equipo de cómputo, servidor, elementos de red de equipos propiedad del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA o de propiedad de terceros.
Deshabilitar de manera inmediata los privilegios de acceso físico a las instalaciones del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, en los eventos de desvinculación o ausencia transitoria, de acuerdo con los reportes enviados por la oficina de Talento Humano o la oficina de gestión contractual.

POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, la entidad planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en el SGSI.

POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

El Oficial de Seguridad de la Información junto con el proceso de Gestión de Tecnologías de la Información, establecerá los controles para acceso lógico y protección de las redes del El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la alta dirección.
El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

Se debe mantener información de las actividades realizadas por los usuarios con privilegios de red en el Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, manteniendo estos registros disponibles por un tiempo de al menos un año.
Cualquier cambio de configuración, alteración, adecuación o instalación de dispositivos electrónicos, tecnológicos o técnicos que permita compartir acceso a redes, servicios de red o información de propiedad de la institución se encuentra prohibida.
El proceso de Gestión de Tecnologías de la Información debe realizar un monitoreo continuo de la red generando alertas de consumo, intentos fallidos de acceso,
intentos de acceso restringido y cualquier anomalía que requiera el apoyo en
sensibilización, avaluación o escalamiento a investigación disciplinaria y/o judicial.

POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El proceso de Gestión de Tecnologías de la Información velará que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimientos y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.
Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesarios para su desarrollo e implementación.
En caso de contratar un desarrollo externo, 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.

POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesarios durante y después del contrato.
Se debe identificar los riesgos de seguridad originados por la gestión de transacciones, el uso de instalaciones de procesamiento de información y cualquier otro mecanismo de administración, acceso o almacenamiento de información por parte del proveedor.
Se debe socializar con el proveedor la política de seguridad de la información, la política de protección de datos personales, el presente manual de políticas, así como identificar las responsabilidades que el proveedor tiene con respecto a la protección de la información.
Es obligación de la empresa proveedora, el reporte de cualquier anomalía relacionada con la protección de la información con el objeto de ser tratada de manera oportuna y se prevengan incidentes de seguridad de la información.

SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.
El proceso de Gestión de Tecnologías de la Información generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

POLÍTICAS DE GESTIÓN DE INCIDENTES

Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar al Oficial de Seguridad de la Información por cualquiera de los medios dispuestos para tal fin por ejemplo la mesa de servicio.
Sera responsabilidad de todas las dependencias del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA

comunicar y seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.

POLÍTICAS DE CUMPLIMIENTO

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA velara por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

POLITICAS PARA EL ESCRITORIO Y PANTALLA LIMPIOS

No deberán dejarse documentos críticos en el “Escritorio” tanto físico como el Escritorio virtual (se denomina “Escritorio” al espacio digital en los equipos de cómputo).
Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
Emplear las cajoneras o archivadores bajo llave para el almacenamiento de la información sensible/crítica, token o mecanismos técnicos o tecnológicos que restrinjan acceso a aplicaciones y/o información.
Se debe proteger la información de daños ocasionados por cualquier tipo de comida y/o bebida de tal forma que se proteja la integridad o disponibilidad de la información.

POLÍTICAS PARA EL USO ADECUADO DE INTERNET
El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.
Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes y/o represente un riesgo para la integridad, confidencialidad y disponibilidad de la información.
Estará limitado el acceso a redes sociales en general salvo aquellas que se requieren para el cumplimiento de las funciones de cada área, grupo de trabajo o proceso.
Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
El grupo de soporte tecnológico y/o la oficina de Tecnologías de la Información y de las Comunicaciones, podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.
El acceso a internet por parte de personal externo 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 documentado.
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.
Está prohibido el uso de cualquier pagina o herramienta de chat, o mensajería instantánea, diferente a la previamente autorizada por el instituto y esta deberá ser utilizada para fines laborales y que vayan en pro del desarrollo institucional de la entidad.

POLÍTICAS PARA EL USO ADECUADO DE CORREO ELECTRÓNICO

Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen al INSTITUTO NACIONAL DE

VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS INVIMA, por lo tanto, su contenido también es propiedad de la Entidad.
El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
La oficina de tecnología de la información previa autorización del responsable o propietario de la información podrá activar el uso y acceso al contenido de los buzones de los correos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.
El INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS INVIMA se reserva el derecho de deshabilitar, modificar o eliminar las cuentas del correo institucional en las cuales se evidencie un uso inadecuado o que incurran en el incumplimiento de las políticas plasmadas en el presente manual.
La oficina de tecnología de la información debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso, correos masivos y cualquier otra amenaza que pudiera ser trasmitido a través de los mensajes.
Se prohíbe el envió de correos masivos y la cuenta de correo electrónico puede ser bloqueada si se evidencia este comportamiento por sospecha de spam.
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.

POLÍTICA PARA EL USO DE USUARIOS Y CONTRASEÑAS:
Cada funcionario, contratista o tercera parte cuyas obligaciones o funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.
Las credenciales son personales e intransferibles.
Deben utilizarse esquemas de seguridad para la creación de contraseñas con un mínimo de características como se definen a continuación:
Uso de mayúsculas, minúsculas, caracteres especiales y números
Definir intervalos no mayores a 60 días para el cambio de contraseñas.
Se debe definir los mecanismos necesarios para identificar contraseñas similares o iguales (ej: n0$h@(k3@r0n1 - n0$h@(k3@r0n2).
Se debe implementar mecanismos para evitar duplicidad de letras en el uso de las contraseñas (ej: Qq22qq@@).
Se debe procurar que no se repitan al menos las últimas 5 contraseñas utilizadas.
Cada funcionario, contratista o tercero debe garantizar que las contraseñas no se almacenan en dispositivos propios o del Instituto.
Cada funcionario, contratista o tercero debe acatar las medidas de seguridad que se implementen en el INVIMA, de acuerdo con los cambios tecnológicos o riesgos identificados relacionados con la protección del usuario y contraseña, así como con el fin de mitigar el riesgo de suplantación.

POLÍTICA PARA EL USO DE DISPOSITIVOS DE PROPIEDAD PRIVADA (BYOD)

El personal de planta, los contratista y terceros responsables de la presentación de servicios para el INVIMA a los que se autorice el uso de equipos de su propiedad privada (BYOD1) para gestionar información del Instituto deben firmar un compromiso de confidencialidad y no divulgación de la información del INVIMA que almacenaran en sus equipos personales y la obligación de cumplir las políticas de seguridad de la información, ciberseguridad y de protección de datos personales
Todo dispositivo personal privado autorizado para gestionar información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA debe
1 BYOD (traiga su propio dispositivo) sigla con la que se identifica a los equipos que no son propiedad del Invima, siendo propiedad de los servidores públicos y que son usados para cumplir las funciones propias del cargo designado al servidor público.
Cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.
Todo dispositivo personal privado autorizado para conectarse a las redes de datos del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA debe ser gestionado a través del controlador de dominio del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA.
El personal de planta, contratista y/o proveedor responsable de la prestación de servicios para el INVIMA al que se le autorice el uso de su dispositivo de su propiedad personal debe garantizar bajo acuerdo de confidencialidad que la

información reservada, pública clasificada o datos personales que gestione en el dispositivo será almacenada de forma aislada a la información personal que guarde en su dispositivo.
El propietario del dispositivo privado es responsable de mantener actualizado el sistema operacional y software de su equipo y de aplicar las actualizaciones de seguridad recomendadas por el fabricante del sistema operativo y las aplicaciones instaladas en el mismo.
Las conexiones remotas a las redes del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA desde dispositivos de propiedad personal privada se realizan utilizando las conexiones de VPN autorizadas por el Proceso de Gestión de Seguridad de la Información con el apoyo del Proceso de Gestión de Tecnologías.
El uso de software de análisis de tráfico, análisis de vulnerabilidades, análisis de seguridad de aplicaciones en equipos de propiedad personal privada solo se autoriza al personal con funciones asignadas o contratos suscritos para esos fines, la utilización de ese tipo de software sin autorización es considerado evento de seguridad de la información2.
2 Ley de delitos Informáticos. Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena
En los dispositivos personales privados, se debe configurar un perfil de usuario específico para el almacenamiento de la información correspondiente al INVIMA el cual debe ser diferente al usuario configurado para uso personal del propietario del dispositivo.
Todo dispositivo personal privado autorizado para gestionar información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA debe contar con un software de protección contra código malicioso.
Sin excepción todo dispositivo de propiedad particular debe tener activo el acceso mediante nombre de usuario y contraseña, bloqueo de sesión por inactividad y protección contra código malicioso.
El propietario del dispositivo personal privado debe informar sin demoras injustificadas al INVIMA y a la autoridad competente el robo o pérdida de su dispositivo. La pérdida o divulgación de información almacenada en los dispositivos BYOD se gestiona como un incidente de seguridad de la Información, ciberseguridad y protección de datos personales.
Al finalizar la vinculación laboral o relación contractual con el INVIMA, el propietario del dispositivo personal privado debe realizar la entrega de la información que se almacenó en el dispositivo y realizar el borrado de cualquier copia de dicha información que aún esté bajo su control.

6. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

SENSIBILIZACIÓN Y COMUNICACIÓN

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, definirá un “Plan de Comunicación en Seguridad de la Información” a través de su oficina de comunicación interna y externa y el Oficial de Seguridad de la Información, donde se planificará ANUALMENTE la manera en que se comunicarán nuevos lineamientos, recomendaciones o tips de seguridad de la información por diferentes medios a todos sus
de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
funcionarios, contratistas y terceros, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos del instituto. La creación de los contenidos se hará con apoyo del Oficial de Seguridad de la Información y/o el proceso de Gestión de Tecnologías de la Información.

CAPACITACIONES EN SEGURIDAD

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, a través de sus áreas/procesos de Talento Humano y Contractual, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario, contratista y/o tercero (proveedor) que se vincule a la entidad tenga pleno conocimiento del Sistema de Gestión de Seguridad de la Información incluidas las políticas de seguridad de la información, el Oficial de Seguridad de la Información apoyará en dichas inducciones.

7. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA.

8. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos que soportan y protegen la información o por el incumplimiento de los lineamientos aquí descritos.

a.Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.
b.Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.
c.El Oficial de Seguridad de la Información será el encargado de recopilar y entregar a la Oficina de Control Disciplinario las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, proceso de Gestión de Tecnologías de la Información será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

ELABORÓ	REVISÓ	APROBÓ
Nidia Nayibe Gonzalez Pinzon **Coordinador Grupo Soporte Tecnológico** **Fecha de elaboración:** 01/06/2026	Jina Marcela Lozano Bedoya **Jefe Oficina Asesora de Planeación** **Fecha de revisión:** 01/06/2026	Francisco Augusto Giuseppe Rossi Buenaventura **Director General** **Fecha de aprobación:** 01/06/2026