R.D. N° 147 2022-INSN-DG

RESOLUCIÓN DIRECTORAL

Lima, 09 de Junio del 2022

VISTO:

El expediente con Registro N° 001125-2022, que contiene el Informe Nº 341-2022-UI-OEI-INSN, emitido por el Jefe de Unidad de Informática de la Oficina de Estadística e Informática, sobre la elaboración de la Resolución de aprobación del "Manual de Políticas de Seguridad de la Información".

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 004-2016- PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos- 2da Edición; en todas las entidades integrantes del Sistema Nacional de Informática;

Que, el proyecto de documento normativo propuesto tiene como objetivo crear un marco referencial para gestionar de manera apropiada la Seguridad de la Información del Instituto Nacional de Salud del Niño, establecer las disposiciones con respecto al uso de los activos de información de la Institución, así como de las medidas que se deben adoptar para la protección de estos activos, concientizar a todo el personal asistencial y administrativo del Instituto Nacional de Salud del Niño sobre la importancia y la comprensión de sus responsabilidades individuales sobre la Seguridad de la Información, proporcionar a todo el personal asistencial y administrativo del Instituto Nacional de Salud del Niño los lineamientos que faciliten una adecuada toma de decisiones en aspectos relacionados a la Seguridad de la Información;

Que, el literal k) del artículo 20º del Texto Único Ordenado del Reglamento de Organización y Funciones del Instituto aprobado con Resolución Directoral Nº 083-2010/MINSA, establece que la Oficina de Estadística e Informática tiene asignadas entre sus funciones, la de "Establecer y mantener la seguridad, integración y operatividad de las redes de información y base de datos institucionales necesarias;

Que, con Memorando Nº 559-OEI-INSN-2022, de fecha 11 de Abril del 2022, el Jefe de la Oficina de Estadística e Informática, remite la propuesta de Manual de Políticas de Seguridad de la Información en el Instituto Nacional de Salud del Niño", para la aprobación correspondiente;

Que, con Informe N° 396-OEPE-INSN-2022, de fecha 20 de mayo del 2022, el Director Ejecutivo de la Oficina Ejecutiva de Planeamiento Estratégico, emite opinión favorable del Manual de Políticas de Seguridad de la Información en el Instituto Nacional de Salud del Niño";

Que, con Memorando N° 449-2022-DG/INSN, de fecha 21 de mayo del 2022, el Director General, aprueba y solicita la elaboración de la Resolución Directoral del Manual de Políticas de Seguridad de la Información;

En uso de las facultades conferidas en el Manual de Organización y Funciones de la Dirección General, aprobado por Resolución Directoral Nº 275-DG-INSN-2014; y

Con las visaciones, del Director Ejecutivo de la Oficina Ejecutiva de Planeamiento Estratégico, el Jefe de la Oficina de Estadística e Informática, y el Jefe de la Oficina de Asesoría Jurídica;

SE RESUELVE:

Artículo 1º.- Aprobar el Documento Técnico: "Manual de Políticas de Seguridad de la Información", el mismo que consta de treinta y tres (33) páginas que forman parte de la presente Resolución.

Artículo 2º.- Encargar a la Oficina de Estadística e Informática la publicación de la presente Resolución Directoral, en el Portal de Transparencia del Instituto Nacional de Salud del Niño.

Regístrese y Comuníquese;

MINISTERIO DE SALUD
INSTITUTO NACIONAL DE SALUD DEL NIÑO

M.C. JAIME AMADEO TASAYCO MUÑOZ
DIRECTOR GENERAL (e)
C.M.P. 28872 - R.N.E. 034554

JTM/JLSE/NND

Distribución:
( ) Dirección General
( ) OEPE
( ) OEI
( ) Directores Ejecutivos
( ) Jefes de Oficina.
( ) Archivo

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Oficina de Estadística e Informática - Unidad de Informática

2022

MINISTERIO DE SALUD – UNIDAD DE INFORMÁTICA – INSTITUTO NACIONAL DE SALUD DEL NIÑO

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Índice

I. INTRODUCCION

Las Políticas de Seguridad de la Información del Instituto Nacional de Salud del Niño, han sido elaboradas tomando como marco de referencia la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos 2° Edición, cuya finalidad principal es asegurar la confidencialidad, integridad y disponibilidad de la información almacenada en los sistemas de información de la Institución.

II. FINALIDAD

Asegurar la confidencialidad, integridad y disponibilidad de la información almacenada en los sistemas de información del Instituto Nacional de Salud del Niño

III. OBJETIVOS

- Crear un marco referencial para gestionar de manera apropiada la Seguridad de la Información del Instituto Nacional de Salud del Niño.
- Establecer las disposiciones con respecto al uso de los activos de información de la Institución, así como de las medidas que se deben adoptar para la protección de estos activos.
- Concientizar a todo el personal del Instituto Nacional de Salud del Niño sobre la importancia y la comprensión de sus responsabilidades individuales sobre la Seguridad de la Información.
- Proporcionar a todo el personal del Instituto Nacional de Salud del Niño los lineamientos que faciliten una adecuada toma de decisiones en aspectos relacionados a la Seguridad de la Información.

IV. AMBITO DE APLICACIÓN

Las Políticas de Seguridad de la Información son de aplicación para todo el personal que tengan acceso a la información y sistemas de información del Instituto Nacional de Salud del Niño.

V. BASE LEGAL

- Ley N° 27444: Ley de Procedimiento Administrativo General.
- Ley N°30096 Ley de Delitos Informáticos
- Ley N°27269 Ley de firmas digitales
- Ley N°29733 Ley de protección de datos personales
- MS-SGSI-001 "Manual del Sistema de Gestión de Seguridad de la Información"
- P-GTI-02 "Respaldo de Información"
- Ley N" 27927 -Ley de Transparencia y Acceso a la Información Pública
- Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos 2° Edición.
- Resolución Ministerial N° 083-2010/MINSA, que aprueba el Texto Único Ordenado del Reglamento de Organización y Funciones del Instituto de Salud del Niño.
- Resolución Ministerial N° 826-2021/MINSA. Que aprueba las Normas para la Elaboración de Documentos Normativos del Ministerio de Salud.

VI. CONTENIDO

6.1 POLÍTICA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.1.1 Objetivos

- Gestionar la seguridad de la información dentro del Instituto Nacional de Salud del Niño.
- Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información del Instituto Nacional de Salud del Niño.
- Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas identificadas.

6.1.2 Política

El Instituto Nacional de Salud del Niño debe mantener una organización interna que le permita prevenir, detectar y responder apropiadamente a eventos de Seguridad de la Información. Para ello, es necesario que se definan en forma clara las responsabilidades de cada trabajador en el contexto de la Seguridad de la Información.

6.1.3 Institución de Seguridad

Se debe definir a los responsables para cada activo de información, las áreas deben mantener un inventario de sus activos de información, indicando para cada uno de ellos el responsable de su mantenimiento y protección. Esto implica la clasificación de la información y definir al personal autorizado para su acceso

6.1.4 Funciones sobre Seguridad de Información

Se han establecido los roles y funciones en el Instituto Nacional de Salud del Niño para el cumplimiento de la normativa vigente, las que se precisan en el 6.2 Comité de Gestión de Seguridad de la Información.

6.2 COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.2.1 Aspectos Generales

El Comité de Gestión de Seguridad de la Información estará integrado y representado por:

- Representante del Directorio Ejecutivo.
- Director General.
- Director Ejecutivo de la Oficina Ejecutiva de Administración.
- Jefe de la Oficina de Asesoría Jurídica.
- Jefe de la Oficina de Estadística e Informática.
- Jefe de la Oficina de Personal.
- Oficial de Seguridad de la Información.
- En calidad de "Asesores" se podrá requerir la asistencia del personal del Instituto Nacional de Salud del Niño o consultores externos, cuyo aporte se estime necesario para la correcta toma de decisiones técnicas específicas. Estos miembros Asesores sólo tendrán derecho a voz, más no a voto.

6.2.2 Funciones y Responsabilidades del Comité de Gestión de Seguridad

Las obligaciones del Comité de Gestión de Seguridad de la Información serán:

- Asegurar que las metas de la Seguridad de la Información sean identificadas, relacionarlas con las exigencias institucionales y que sean integradas en procesos relevantes.
- Formular, revisar y enviar la propuesta de la política de seguridad de información al Directorio del Instituto Nacional de Salud del Niño para su aprobación.
- Revisión de la efectividad en la implementación de la política de seguridad de la información.
- Proveer lineamientos claros y un visible apoyo en la gestión para iniciativas de seguridad de la información.
- Apoyar planes y programas de capacitación para mantener la conciencia en seguridad de la información.

6.2.3 Funciones Específicas

Las funciones del presidente del Comité de Gestión de Seguridad son las siguientes:

- Mantener una agenda actualizada de los temas de seguridad que el Instituto Nacional de Salud del Niño debe abordar y que deben ser discutidos en el Comité de Seguridad de la Información.
- Coordinar y fijar la fecha de las sesiones.
- Revisar y aprobar las Actas, previa rúbrica de los miembros titulares.
- Moderar los debates a fin de que se cumpla el propósito de llevar el tema de la seguridad sin que se generen discusiones.

Las funciones del secretario del Comité de Seguridad de la información serán las siguientes:

- Elaboración de las citaciones a los miembros del Comité, de acuerdo a la calendarización que disponga el presidente, o cuando se convoque a sesión extraordinaria.
- Redacción de las Actas y lectura de las mismas.
- Conservar las Actas y documentación de todas las actuaciones del Comité.

6.2.4 Funcionamiento del Comité de Seguridad de la Información Sesiones

- Las sesiones o reuniones del Comité, serán coordinadas por el presidente del Comité, ya sean de carácter ordinario o extraordinario. Se aplicará la siguiente pauta de convocatoria:
  - **Sesiones Ordinarias:** A celebrarse en forma periódica, previa convocatoria del presidente con 7 días de anticipación. Esta reunión debe celebrarse en forma rutinaria, por lo que la convocatoria sólo constituye una confirmación de fecha, lugar y hora.
  - **Sesiones Extraordinarias**: A celebrarse por libre convocatoria del presidente, o a petición de uno o más de sus miembros titulares.

- Las convocatorias a reuniones extraordinarias, tendrán que realizarse con el tiempo de anticipación posible según la urgencia del asunto a tratar.
- Las convocatorias para sesiones ordinarias y extraordinarias deben ser realizadas por escrito (correo electrónico) indicando el lugar, día y hora fijados por el secretario del Comité.
- Por cada sesión se levantará un acta, la cual será confeccionada por el secretario del Comité.

6.2.5 Acuerdos del Comité de Seguridad de la Información

Los acuerdos tomados en cada sesión quedarán reflejados en las respectivas actas, pero para adoptar el carácter de acuerdos válidos, dichas actas serán leídas al final de la sesión y se considerarán como aprobadas de manera inmediata creándose el registro necesario. En el caso que un miembro titular haya sido reemplazado por inasistencia, la persona que lo representó deberá entregarle los antecedentes del caso que le permitan validar la decisión.

6.2.6 Funciones del Oficial de Seguridad de la Información

Las funciones del Oficial de Seguridad de la Información serán las siguientes:

- Coordinar y proponer la agenda del Comité de Seguridad de la Información.
- Liderar los grupos de respuesta ante la ocurrencia de incidentes, conforme a lo establecido en el procedimiento de gestión de incidentes.
- Gestionar las actividades que materializan las funciones de seguridad, en concordancia con lo establecido en las políticas de seguridad del Instituto Nacional de Salud del Niño.
- Liderar la realización de actividades orientadas al análisis de riesgos periódicos sobre los activos de información, a fin de mantener un conocimiento actualizado de las amenazas y vulnerabilidades sobre éstos.
- Supervisar las actividades de seguridad perimetral como de la red interna.
- Monitorear los permisos de acceso a los activos informativos.
- Establecer y mantener contactos con los recursos o fuentes externas de apoyo técnico y especializado en el tema de la Seguridad de la Información.

6.2.7 Seguridad en el Acceso de Terceros

- Identificación del riesgo de acceso por parte de terceros, cada responsable de área deberá evaluar, establecer y documentar los requerimientos de acceso, tanto físicos como lógicos. Para cada caso deberá indicarse las razones para tal acceso.
- Los contratos de servicios por terceros deben reflejar los requerimientos de seguridad para mantener el cumplimiento de la presente política, velándose por la correcta interpretación entre el Instituto Nacional de Salud del Niño y los terceros.

6.3 POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

6.3.1 Objetivos

- Identificar en forma clara los activos de información y mantener un inventario de todos los activos de información.
- Asegurar un nivel de protección adecuado a los activos de información.

6.3.2 Política de Inventario y Propiedad de los Activos de Información

- Se deben identificar los activos importantes asociados a cada sistema de información, sus propietarios y ubicación. El inventario será actualizado ante cualquier modificación de la información registrada y revisado periódicamente.
- La propiedad de los activos de información está referida al responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos.

6.3.3 Clasificación de Activos de Información

- Toda la información de la Institución debe ser clasificada de acuerdo al estándar que maneja el Instituto Nacional de Salud del Niño, el cual define 03 tipos:
  - **Confidencial:** Información cuyo contenido no debe ser divulgado ni distribuido a personas que no sean autorizadas y cuya difusión generaría un impacto importante en el Instituto Nacional de Salud del Niño.
  - **Uso Interno**: Información cuyo contenido sólo debe ser de uso y divulgación para el personal del Instituto Nacional de Salud del Niño.
  - **Pública:** Información no sensible, de acceso público y que su divulgación no genera impacto al Instituto Nacional de Salud del Niño.
- El "propietario de la información" es responsable de la clasificación de los activos de información que se encuentran a su cargo.
- Se debe realizar la actualización en forma anual y/o cuando se estime que un activo de información ha aumentado su nivel de sensibilidad, en este caso se deberá cambiar su nivel de clasificación en forma inmediata, sin esperar el próximo ciclo de actualización. Caso contrario, al considerarse que la información ha disminuido su sensibilidad, podrá opcionalmente esperarse el próximo ciclo de actualización o modificar su clasificación con efecto inmediato. La responsabilidad de la decisión corresponde al propietario de la información.
- Toda la información que no ha sido específicamente clasificada, es considerada como "Uso Interno", por lo que debe asumirse que no se permite su divulgación, salvo que el "propietario de la información" así lo autorice formalmente.

6.3.4 Etiquetado de Activos de Información

- El etiquetado de los activos de Información se debe realizar conforme a la clasificación de activos definida.
- Toda la información que es considerada Confidencial o de Uso Interno, debe ser etiquetada (marcada) según su categoría.

- Todos los envíos de información confidencial deben ser realizados por medios de transporte conocidos y seguros.
- Se debe realizar un seguimiento a los originales y copias de información sensible, indicando como mínimo, la clasificación de información, el número de copias, la ubicación de las copias y las personas responsables de las copias.
- Antes de enviar dispositivos de almacenamiento a algún tercero, la información sensible debe ser removida o manejada según criterios establecidos por el propietario de la información.
- Cada área es responsable de ejecutar los procedimientos para que se dé cumplimiento a lo que establece esta política.

6.3.5 Privacidad de la Información Personal

- La protección y privacidad de los datos de información del personal debe asegurarse de conformidad con los requerimientos legales.
- Se debe implementar medidas técnicas y organizacionales apropiadas para proteger la información personal.

6.4 POLÍTICA DE SEGURIDAD EN RECURSOS HUMANOS

6.4.1 Objetivos

- Asegurar que el personal del Instituto Nacional de Salud del Niño entienda sus responsabilidades, las cuales deben ser adecuados a los roles para los que han sido contratados, esto permite reducir el riesgo de robo, fraude o mal uso de las instalaciones.
- Asegurar que el personal del Instituto Nacional de Salud del Niño que cese sus labores o relaciones contractuales y cambien de empleo de forma ordenada.

6.4.2 Política

- La seguridad de los recursos humanos, involucra a toda persona que utiliza la información del Instituto Nacional de Salud del Niño para el desempeño de sus actividades.

6.4.3 Selección de Personal

- Se deben realizar todas las comprobaciones necesarias sobre la veracidad de la información brindada por el personal a contratar en el Instituto Nacional de Salud del Niño.

6.4.4 Acuerdos de Confidencialidad

- El personal del Instituto Nacional de Salud del Niño debe firmar acuerdos de confidencialidad y no divulgación para proteger adecuadamente los activos de información.
- Estos acuerdos señalan las obligaciones del personal y las obligaciones de la Institución para la seguridad de la información.

- El acuerdo de confidencialidad debe ser parte del legajo personal y en el caso de proveedores establecerse en el contrato de servicios.

6.4.5 Durante el Empleo y/o Servicio

Las personas que ingresan a laborar en el Instituto Nacional de Salud del Niño bajo cualquier modalidad deben conocer la normatividad interna y el Manual de Políticas de Seguridad de la Información. Asimismo, deben de recibir el material inductivo, escrito o audio/visual, que permita dar a conocer sus roles y responsabilidades sobre la información, comprometiéndose a aplicarlas en el desempeño de sus funciones:

- Los activos y/o recursos necesarios serán asignados al inicio de las labores del personal que ingresa a la Institución. Igualmente, al momento del cese de sus funciones, deberá devolver los activos y/o recursos asignados.
- El personal del Instituto Nacional de Salud del Niño, externos o terceros deberán cumplir con las Políticas de Seguridad de la Información, establecidas y sólo tendrán acceso a la información que requieran para realizar los servicios establecidos en el contrato.
- El personal del Instituto Nacional de Salud del Niño es responsable del buen uso y cuidado de los activos de información asignados. Asimismo, son responsables del uso correcto y mesurado de cada servicio que brinda la Institución para el desarrollo de las funciones asignadas.

6.4.6 Responsabilidad de los Miembros del Comité de Gestión de Seguridad de la Información

- Los Miembros del Comité de Gestión de Seguridad de la Información del Instituto Nacional de Salud del Niño, deben asegurar que el personal a su cargo, bajo su responsabilidad estén capacitados en sus roles y responsabilidades sobre seguridad en el contexto de la labor que desempeñan.

6.4.7 Entrenamiento de la Seguridad de la Información

- El personal del Instituto Nacional de Salud del Niño, debe ser capacitado permanentemente con la finalidad de concientizarlos en la importancia de la Seguridad de la Información.
- El Jefe de la Oficina de Estadística e Informática en coordinación con el Jefe de la Oficina de Personal y el Oficial de Seguridad de la Información deben de planificar las actividades de capacitación.

6.4.8 Infracciones a las Políticas de Seguridad de la Información

- Las infracciones a las Políticas de Seguridad de la Información serán sancionadas conforme a las disposiciones señaladas en la normatividad vigente, sin perjuicio de las acciones civiles y/o penales que pudieran corresponder.

6.4.9 Finalización del Empleo

- Debe existir un proceso de finalización del empleo y las responsabilidades deben estar incluidas en los contratos del personal del INSN.

6.4.10 Devolución de Activos

- El personal del Instituto Nacional de Salud del Niño debe devolver la totalidad de los activos asignados para cumplimento de sus labores, cuando finalice el empleo o contrato mediante un acta de Entrega de Cargo.

6.4.11 Retiro de Derechos de Acceso a la Información

- Los derechos de acceso a la información y a las instalaciones de procesamiento; del personal del Instituto, deben ser removidos o modificados al producirse el término del empleo o contrato.
- Los Directores Ejecutivos, Jefes de Departamentos, Jefes de Servicios, Jefes de Oficinas y Jefes de Unidades deben solicitar por escrito (utilizando la ficha de creación de usuarios) al Jefe de la Oficina de Estadística e Informática la creación, actualización, habilitación, suspensión o eliminación de los usuarios y sus cuentas, a fin de mantener actualizado los accesos a los sistemas de información y servicios informáticos.

6.5 POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

6.5.1 Objetivos

- Evitar accesos no autorizados, daños e interferencias contra las instalaciones y la información del Instituto Nacional de Salud del Niño.
- Evitar pérdidas, daños a los activos de información, así como la interrupción de las actividades del Instituto Nacional de Salud del Niño.

6.5.2 Perímetro de Seguridad Física

- El perímetro de seguridad física debe estar claramente definido y demarcado. Las especificaciones técnicas dependerán del nivel de protección que se requiera lograr.
- Se debe proteger las áreas donde funcionan las instalaciones de procesamiento de información, suministro de energía eléctrica, aire acondicionado y cualquier otra que sea considerada como crítica y que pudiera afectar el funcionamiento de los sistemas de información.

6.5.3 Controles Físicos de Entradas

- El acceso a la Institución deberá contar con un control de acceso físico que aseguren que sólo el personal del Instituto Nacional de Salud del Niño debidamente autorizados pueda ingresar.
- El acceso y la permanencia de visitantes sólo serán permitidos para propósitos específicos y con autorización respectiva, quedando debidamente registrados.

6.5.4 Seguridad de Oficinas, Despachos y Recursos

- Se debe diseñar y aplicar seguridad física en las oficinas e instalaciones del Instituto Nacional de Salud del Niño dedicadas al procesamiento de la información.

- Las áreas seguras deben ser ubicadas en un lugar que no presente riesgos desde el punto de vista de acceso al público.
- No deben ponerse a libre disposición del público guías ni listados que brinden información de ubicaciones, números de teléfono y cualquier otro dato relacionado con las instalaciones críticas de procesamiento de la información.
- Se debe prohibir el ingreso de computadoras portátiles, equipos fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido autorizados por la Oficina de Estadística e Informática.

6.5.5 Trabajo en las Áreas Seguras

- Las áreas seguras deben estar cerradas y ser monitoreadas por el personal de vigilancia fuera del horario de trabajo.
- Se debe anotar en un registro la fecha y hora de entrada y salida.
- Se debe prohibir comer, beber y fumar dentro de las áreas de trabajo.

6.5.6 Acceso a Áreas de Carga y Descarga

- Los accesos al área de carga y descarga serán restringidos únicamente al personal del Instituto Nacional de Salud del Niño autorizados y que esté debidamente identificado.

6.5.7 Seguridad de Activos de Información

- El propósito de evitar daños o pérdidas que afecten la continuidad de los activos de información del Instituto Nacional de Salud del Niño, es necesario implementar controles para la debida protección de los recursos de tecnología de información.

6.5.8 Protección de Infraestructura Segura

- Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto y otras formas de desastre natural o creados por el hombre.
- Todo material inflamable debe de almacenarse en lugares que no puedan comprometer las áreas seguras.
- El Data Center del Instituto Nacional de Salud del Niño, debe contar con un sistema dedicado de protección y extinción contra incendios y un sistema de acondicionamiento de temperatura, humedad y filtrado de aire.
- Deben monitorearse las condiciones ambientales de temperatura y humedad para que no afecten el normal funcionamiento de los equipos de tratamiento de información.

6.5.9 Suministro de Energía Eléctrica

- Se debe proteger los equipos de tecnología de la información de fallas por suministro de energía y otras anomalías eléctricas. La provisión de energía debe ser conforme a las especificaciones del fabricante de equipos. Asimismo, se debe incluir equipos de energía ininterrumpida (UPS) para los equipos que soportan las

operaciones críticas del Instituto Nacional de Salud del Niño y contar con un generador de energía (grupo electrógeno) en casos de interrupciones prolongadas de suministro de energía eléctrica.

6.5.10 Protección del Cableado

- El cableado de la red de comunicaciones y suministro de energía debe protegerse para evitar una intercepción o daño. El cableado de la red debe cumplir con los estándares internacionales de cableado estructurado; cada elemento debe estar identificado, etiquetado y debe mantenerse una memoria técnica descriptiva actualizada.
- El cableado de suministro de energía eléctrica y telecomunicaciones en las zonas de tratamiento de información, debe contar con un sistema de puesta a tierra, el que debe ser revisado periódicamente para garantizar su adecuado funcionamiento.

6.5.11 Mantenimiento de Equipos

- Se debe considerar un programa de mantenimiento preventivo y correctivo de los equipos de tecnología de información y de los sistemas de acondicionamiento de temperatura, humedad y filtrado de aire, sistemas de energía ininterrumpida (UPS) y sistemas de detección y extinción de fuego según las especificaciones del fabricante.

6.5.12 Seguridad de Equipos Fuera del Local

- El uso de equipos de la Institución fuera de local debe ser autorizado y el personal del Instituto serán responsables de su uso. La Oficina de Estadística e Informática autorizará el uso de cualquier equipo de tratamiento de información fuera del Instituto Nacional de Salud del Niño.

6.5.13 Eliminación Segura o Reutilización de Equipos

- El Personal de Soporte Técnico de la Oficina de Estadística e Informática debe asegurar que la información sensible contenida en los equipos antes de ser reutilizados haya sido eliminada o sobrescrita de manera segura de modo que su recuperación sea irreversible.

6.5.14 Retirada de Materiales de Propiedad del INSN

- Se debe contar con autorización formal para el retiro de materiales como equipos, información o software que son de propiedad del Instituto Nacional de Salud del Niño.

6.6 POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

6.6.1 Objetivos

- Asegurar la operación correcta y segura de los recursos de tecnología de información del Instituto Nacional de Salud del Niño.

- Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos con terceros.
- Minimizar el riesgo de fallos de los sistemas.
- Proteger la integridad del software y de la información.
- Proteger la información de las redes y la protección de la infraestructura que la soporta.
- Monitorear las actividades de procesamiento de información no autorizadas.

6.6.2 Política

- Las actividades de gestión sobre los recursos de tecnología de información del Instituto Nacional de Salud del Niño son esenciales para el buen funcionamiento de los servicios de esta Institución.

6.6.3 Responsabilidades de Operación

- La Oficina de Estadística e Informática, deberá asegurar la existencia de documentación formal de sus procedimientos operativos, estableciendo las responsabilidades y los recursos utilizados para su ejecución eficiente.

6.6.4 Gestión de Cambios

- La Oficina de Estadística e Informática, deberá mantener un registro de control de cambios de los sistemas de información, equipos de comunicación, bases de datos, equipos de cómputo y perfiles de acceso a través de la implementación de acciones y procedimientos necesarios para asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de comprobación y estrés, controles de seguridad, reversión en caso de fallas y análisis de impacto.
- Los cambios deben ser solicitados a la Oficina de Estadística e Informática por el propietario de la información, y se llevará un registro sobre cada solicitud de cambio. En caso existiera algún problema con el cambio realizado se revertirá al estado anterior al cambio.

6.6.5 Segregación de Tareas

- Se debe separar las funciones críticas y áreas de responsabilidad con la finalidad de reducir el riesgo de una modificación no autorizada o accidental o el mal uso de los activos del Instituto Nacional de Salud del Niño.

6.6.6 Separación de los Recursos para Desarrollo y Producción

- Se debe separar los recursos de prueba, desarrollo y producción implementando los controles necesarios, asimismo se debe definir y documentar el procedimiento para pases de desarrollo a producción.
- El entorno de pruebas debe ser en lo posible igual al ambiente de producción en lo referido a recursos de tecnología de información.

- No se debe utilizar datos que contengan información personal u otra información sensible en el ambiente de pruebas.

6.6.7 Gestión y Niveles de Servicios Externos

- Se debe asegurar que todos los controles de seguridad y los acuerdos de niveles de servicio (SLA) acordados con los terceros sean implementados y se cumplan.
- Todos los servicios provistos por terceros deben ser monitoreados, revisados y auditados regularmente.
- Los cambios en los servicios que proveen terceros deben ser planificados y autorizados considerando los riesgos que podrían generar.

6.6.8 Planificación y Aceptación del Sistema

- La Oficina de Estadística e Informática, debe supervisar la planificación de capacidades de los sistemas en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado.
- La Oficina de Estadística e Informática, debe establecer los criterios y las pruebas a realizar a los sistemas existentes o nuevos, que permitan al área usuaria su evaluación y aceptación formal previa a su puesta en ambiente de producción.

6.6.9 Protección Contra Software Malicioso

- La Oficina de Estadística e Informática, deberá de adoptar las medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de servidores de red, computadores portátiles, estaciones de trabajo y smartphones.
- La Oficina de Estadística e Informática, debe asegurar que todas las estaciones de trabajo están protegidas con el antivirus corporativo y que esté actualizado. Asimismo, que el sistema operativo y los aplicativos de oficina deben contar con las últimas actualizaciones de seguridad (parches).
- La Oficina de Estadística e Informática, es responsable de la renovación de licencias de software, y deberá de definir su cronograma de renovación, para evitar que se produzca incumplimiento de uso legal de software.
- El software utilizado por el Instituto Nacional de Salud del Niño debe ser autorizado en forma expresa por la Oficina de Estadística e Informática.
- El usuario final no debe tener el privilegio de deshabilitar los sistemas de control y prevención de malware.
- Los equipos portátiles (laptops) de terceros que por motivos laborales sean autorizados a ingresar en la red del Instituto Nacional de Salud del Niño, deben de ser revisados por el personal de Soporte de la Oficina de Estadística e Informática, verificando que tengan instalado software antivirus actualizado, sistema operativo actualizado y que no exista algún software instalado que implique un riesgo de seguridad.
- El personal de Soporte Técnico de la Oficina de Estadística e Informática, como medida de prevención si detecta que algún servidor de red, estación de trabajo o

computadora portátil está infectada con algún tipo de malware o virus deberá de aislarla inmediatamente desconectándola de la red del Instituto Nacional de Salud del Niño.

6.6.10 Gestión Interna de Respaldo y Recuperación

- La Oficina de Estadística e Informática deberá establecer procedimientos rutinarios para el respaldo de la información de acuerdo a la criticidad de la misma, realizando copias de seguridad y pruebas de recuperación conforme a un cronograma definido.
- Las copias se seguridad deben resguardarse en un lugar externo al de la institución que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad. Asimismo, los equipos y los medios de respaldo deben estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el Data Center.
- Los equipos y los medios de respaldo deben contar con un programa de mantenimiento preventivo y correctivo para asegurar su correcto funcionamiento.
- La Oficina de Estadística e Informática debe estimar anticipadamente la cantidad necesaria de medios magnéticos requeridos para realizar las copias de respaldo y en caso de no contar con ello solicitar su oportuna adquisición.
- El personal de la Unidad de Informática, deberá mantener el registro actualizado de las operaciones de gestión de respaldo y recuperación, así como de las fallas que pudieran presentarse y las soluciones realizadas.
- Se deben de programar y realizar pruebas de recuperación de las copias de respaldo.
- Se debe revisar periódicamente la vigencia tecnológica de los equipos y software utilizado para el respaldo y recuperación de la información.

6.6.11 Diseño de la Infraestructura de Seguridad

La Oficina de Estadística e Informática debe implantar los controles y medidas requeridas para proteger y conservar la seguridad de los datos en las redes y la protección de los servicios conectados contra accesos no autorizados. Estos controles deben de incluir:

- Implementar un esquema de segmentación de redes.
- El desarrollo de procedimientos para la gestión remota de los recursos de Tecnología de Información de manera segura.
- Registro y Monitoreo de las acciones de seguridad relevantes.
- Coordinación de las actividades de gestión para optimizar el servicio y para asegurar que los controles se apliquen adecuadamente a través de toda la infraestructura de procesamiento de la información.
- Se debe establecer controles y medidas especiales para salvaguardar la confidencialidad y la integridad de los datos que pasen a través de redes públicas, así como para proteger los sistemas conectados tales como Firewall, UTM, Filtro de Contenidos, Antispam, entre otros.

6.6.12 Buen Uso de los Medios de Almacenamiento

- Con la finalidad de prevenir daños a los recursos e interrupciones a las actividades del Instituto Nacional de Salud del Niño, se deberá contar con mecanismos de seguridad que garanticen que los medios sean controlados y físicamente protegidos. Asimismo, el Instituto Nacional de Salud del Niño debe implementar los controles que aseguren que todos los medios de almacenamiento que contienen información sensible son: almacenados, protegidos contra el acceso no autorizado y eliminados de manera segura y efectiva.

6.6.13 Uso Adecuado de los Recursos y Servicios Informáticos

- Los recursos y servicios informáticos asignados al personal del Instituto Nacional de Salud del Niño, son de uso exclusivo para las funciones encomendadas a su cargo. Está prohibido utilizarlos para cualquier otra actividad que no forme parte de sus labores.
- El personal del Instituto Nacional de Salud del Niño que hacen uso de los servicios y recursos de tecnología de información, deben cumplir, según corresponda, con las normas establecidas en los reglamentos, directivas, procedimientos e instructivos aprobados.
- El personal del Instituto Nacional de Salud del Niño que incumplan con lo establecido en las normas quedará sujetos a las sanciones establecidas en el Reglamento Interno de Trabajo.

6.6.14 Seguridad del Correo Electrónico

- El Instituto Nacional de Salud del Niño se reserva el derecho de deshabilitar una cuenta de correo electrónico por algún uso indebido que atente contra lo establecido en el presente documento.
- El personal del Instituto Nacional de Salud del Niño es responsable de la información que se maneja desde su cuenta de correo electrónico. Cualquier opinión en los mensajes pertenece al autor remitente y no al Instituto Nacional de Salud del Niño.
- En caso de recibir mensajes con asuntos sospechosos y/o de origen desconocido, este debe ser eliminado sin abrir el contenido o comunicar a la Oficina de Estadística e Informática para el asesoramiento del caso.
- El personal del Instituto debe usar firmas estandarizadas las cuales serán establecidas por la Oficina de Estadística e Informática.
- El envío de mensajes masivos de correo electrónico solo está permitido al personal o dependencias del Instituto Nacional de Salud del Niño que lo requieran como parte de sus funciones laborales y será solicitado por su Jefe inmediato para la aprobación por parte de la Oficina de Estadística e Informática.
- Todos los mensajes que se envíen y/o reciban a través del correo electrónico son de propiedad del Instituto Nacional de Salud del Niño. El Instituto Nacional de Salud del Niño, se reserva el derecho de conservar y/o revelar el contenido de algún

correo electrónico en caso de ser necesario (cumplir con procesos legales, responder a quejas de terceras personas, seguridad e integridad del personal del Instituto Nacional de Salud del Niño que considere pertinente).

6.6.15 Registros de Auditoría y Monitoreo

- Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de la Oficina de Estadística e Informática y en caso de detectarse usos indebidos de parte del personal del Instituto serán sancionados según lo que corresponda.
- Deben generarse registros de auditoría sobre el uso de los recursos de Tecnología de Información.
- Las actividades de operadores y administradores de los sistemas deben ser monitoreadas, registradas y verificadas regularmente.
- Se debe contar con registro de fallas en los sistemas para asegurar que han sido corregidas oportunamente.
- Los registros de auditoría y monitoreo se deben de respaldar.
- El personal del Instituto Nacional de Salud del Niño es completamente responsable de todas las actividades realizadas con sus cuentas de acceso a red, correo electrónico y sistemas de información asociados al Instituto Nacional de Salud del Niño.

6.7 POLÍTICA DE CONTROL DE ACCESOS

6.7.1 Objetivos

- Controlar los accesos a la información.
- Mantener el acceso autorizado del personal del Instituto Nacional de Salud de Niño y prevenir accesos no autorizados a los sistemas de información y a los servicios de red.

6.7.2 Requerimientos del INSN para el Control de Accesos

Todos los accesos a los recursos de información del Instituto Nacional de Salud del Niño deben basarse en la necesidad y rol del usuario se deberá tomar en cuenta los siguientes aspectos:

- Los requerimientos de seguridad de cada una de las aplicaciones.
- Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.
- Coherencia entre las políticas de control de accesos y las políticas de clasificación de la información.
- Uso de perfiles de usuarios estandarizados definidos según roles.
- Revisión periódica de los controles de acceso.
- Revocación de los derechos de acceso.

6.7.3 Gestión de Acceso de los Personal asistencial y administrativo

- Con el propósito de impedir accesos no autorizados a los recursos de información, deben establecerse procedimientos formales para asignar los derechos de acceso a los sistemas.
- Los Directores Ejecutivos, Jefes de Departamentos, Jefes de Servicios, Jefes de Unidades u Oficinas, serán los encargados de autorizar y solicitar el acceso del personal a su cargo a los recursos de tecnología de información según los procedimientos establecidos. Asimismo, deben informar y solicitar a la Oficina de Estadística e Informática la eliminación de accesos en caso de que un trabajador deje de pertenecer al Instituto Nacional de Salud del Niño o cuando sus funciones ya no lo requieran.
- La Oficina de Estadística e Informática, debe asignar un identificador (cuenta) único y exclusivo a toda persona que haga uso de los recursos de información ya sea de forma temporal o permanente y que le permita contar solo con los accesos autorizados para el normal desarrollo de sus actividades.
- Se debe controlar que no se compartan identificadores entre diferentes usuarios, para ello deben definirse políticas de control a nivel sistema operativo de red, de manera que se pueda detectar duplicidad de sesiones de usuarios.
- La Oficina de Estadística e Informática debe establecer las políticas para permitir que el usuario pueda cambiar su contraseña en caso de que lo requiera (incluyendo el primer inicio de sesión), para ello se le informará que:
  - Deben seleccionar secuencias de caracteres o palabras claras y fáciles de recordar. Se deben considerar una longitud mínima de 6 caracteres.
  - No debe considerar información relacionada directamente con el usuario (nombre, fecha de nacimiento, teléfono, etc.) para elegir una contraseña.
  - Deben cambiar su contraseña si tiene alguna sospecha de su conocimiento por otro usuario.
  - No deben usar las contraseñas usadas en el Instituto Nacional de Salud del Niño para sistemas externos (por ejemplo, correo personal).

6.7.4 Responsabilidad del Personal

- El personal del Instituto Nacional de Salud del Niño es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que terceras personas puedan hacer con el uso de la misma.
- El personal del Instituto Nacional de Salud del Niño debe cambiar sus contraseñas regularmente o cada vez que el sistema se lo solicite. Está prohibido compartir las contraseñas asignadas.
- Para realizar la restauración de contraseñas se debe seguir un procedimiento formal de comunicación establecido por la Oficina de Estadística e Informática para la restauración de contraseñas por pérdida u olvido de la anterior.
- El personal del Instituto Nacional de Salud del Niño debe bloquear su estación de trabajo si por algún motivo se retiran de su ubicación.

- Las estaciones de trabajo deben tener un protector de pantalla con clave y activación automática de bloqueo de usuario cuando no se estén utilizando.
- El personal del Instituto Nacional de Salud del Niño debe mantener sus escritorios libres de documentos y/o medios de almacenamiento removibles cuando no los utilicen, procurando guardarlos en gabinetes con llaves y siempre fuera del horario de trabajo.

6.7.5 Control de Acceso a la Red

El acceso a los recursos de red, tanto internos como externos, debe ser controlado, de manera que el personal del Instituto Nacional de Salud del Niño no comprometa la seguridad de los activos de información. Se debe tener en cuenta los siguientes aspectos:

- Lineamientos de uso de la red.
- Segmentación de redes.
- Control de conexiones a redes en base a políticas.
- Controles de enrutamiento de redes.
- Seguridad en los servicios de red.

6.7.6 Control de Acceso al Sistema Operativo

El acceso al sistema operativo de las estaciones de trabajo del Instituto Nacional de Salud del Niño debe ser debidamente controlado, a fin de evitar accesos no autorizados a recursos o información. Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen:

- Identificación automática de estación de trabajo.
- Procedimientos de inicio de sesión seguros.
- Identificación y autenticación de usuarios.
- Sistema de gestión de contraseñas.
- Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad.
- Desconexión automática de computadoras por tiempo de inactividad.
- Limitación de horarios y tiempo de conexión.

6.7.7 Control de Acceso a las Aplicaciones

- Se debe de establecer los lineamientos de control de accesos a la información y a las aplicaciones restringiéndolas solo para el personal del Instituto Nacional de Salud del Niño debidamente autorizados.
- Los accesos concedidos deben revisarse periódicamente, revocando los derechos del personal del Instituto Nacional de Salud del Niño cuya vigencia de autorización haya caducado.
- Se deben aislar los sistemas identificados con información sensible asignándoles un entorno de procesamiento dedicado, creado a partir de métodos físicos o lógicos.

6.7.8 Conexiones Externas

- Se deben establecer e implementar normas y procedimientos relativos a las actividades de teletrabajo o trabajo remoto.

- Las actividades de teletrabajo deben ser autorizadas por la Dirección General y Jefe de la Oficina de Estadística e Informática y obedecer a necesidades justificadas.
- Se debe definir el tipo de trabajo permitido, las horas de trabajo, la información que puede utilizar y los sistemas y servicios internos a los que está autorizado acceder y el periodo de autorización de acceso.
- En cualquier caso, para el acceso remoto se debe utilizar la tecnología de acceso seguro (SSL-VPN) y su uso debe ser autorizado por el Comité de Seguridad de la Información.

6.8 POLÍTICA DE AQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

6.8.1 Objetivos

- Asegurar que los sistemas de información cumplan con los requisitos de seguridad del Instituto Nacional de Salud del Niño.
- Evitar pérdidas, modificaciones o mal uso de la información que se encuentra dentro de las aplicaciones.
- Proteger la confidencialidad, autenticidad o integridad de la información de los sistemas del Instituto Nacional de Salud del Niño.

6.8.2 Metodología Para la Adquisición, Desarrollo y Mantenimiento de Sistemas

- El Instituto Nacional de Salud del Niño, debe tener una metodología estandarizada para la adquisición, desarrollo y mantenimiento de los sistemas de información.
- Todo desarrollo y/o mantenimiento de sistemas será documentado, con la finalidad de que personas no familiarizadas con los sistemas implementados en el Instituto Nacional de Salud del Niño, ejecuten las actividades con facilidad.

6.8.3 Requisitos de Seguridad

- Se debe definir un procedimiento que incluya controles de seguridad durante las etapas de análisis y diseño del sistema.
- Todo software desarrollado por el personal de la Oficina de Estadística e Informática del Instituto Nacional de Salud del Niño, debe satisfacer los requisitos de seguridad definidos para el desarrollo y mantenimiento de los sistemas, los cuales deben ser referenciados en el caso de un proveedor externo en el contrato suscrito.
- El personal del Instituto Nacional de Salud del Niño debe cumplir con los controles y metodologías establecidas por las cuales podrán ser auditadas.
- La Oficina de Estadística e Informática, debe verificar que los acuerdos suscritos con terceros, incluyan sesión de derechos y cláusulas de confidencialidad con el personal del Instituto involucrados para el resguardo de la propiedad intelectual y de la confidencialidad de la información.
- Todo software desarrollado por el personal de la Oficina de Estadística e Informática son de propiedad del Instituto Nacional de Salud del Niño.

6.8.4 Procesamiento Correcto de las Aplicaciones

- Se deben implementar controles de seguridad apropiados en las aplicaciones utilizadas por el Instituto Nacional de Salud del Niño para validar los datos de entrada, el procesamiento interno y los datos de salida.
- La validación de los datos de entrada debe tener un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.
- Para el control del proceso interno, se deben realizar comprobaciones del correcto funcionamiento del proceso (validación de los datos generados por el sistema, tiempos de respuesta, funciones para cambio de datos, alertas para el procesamiento).
- Deben identificarse los requerimientos para asegurar la autenticidad y la integridad de los mensajes en las aplicaciones, debiendo definirse e implementarse los controles apropiados.
- La validación de datos de salida debe realizarse a fin de asegurar que el procesamiento de la información es correcto. Asimismo, definirse las responsabilidades de todos los implicados en el proceso de salida de datos.

6.8.5 Seguridad de los Archivos del Sistema

Se debe de implementar controles sobre lo siguiente:

- Control del Software en Producción: Se deben formular y poner en práctica procedimientos para controlar la instalación de software en los sistemas en producción.
- Protección de Datos de Prueba del Sistema: Los datos de prueba de los sistemas deben ser cuidadosamente seleccionados, protegidos y controlados.

6.8.6 Control de Acceso al Código Fuente del Programa

- Se debe restringir y controlar el acceso al código fuente de los programas.
- Se debe contar con un responsable del acceso al código fuente de los programas, quien deberá de implementar un registro de uso si es que el código es requerido.

6.8.7 Uso de Controles Criptográficos

Se deben implementar el uso de controles para cifrar la información y proteger la confidencialidad, autenticidad e integridad de la información.

6.8.8 Seguridad en los Procesos de Desarrollo y Pase a Producción

- Se deben definir los requerimientos referidos a arquitectura, tecnología necesaria, seguridad y otros requerimientos especiales.

6.8.9 Procedimiento Para Desarrollo

Todo desarrollo y mantenimiento de sistemas en el Instituto Nacional de Salud del Niño debe ser realizado según los procedimientos y estándares establecidos. Para todo desarrollo de sistemas deben considerarse las siguientes etapas:

- Especificación de Requerimientos (de seguridad, de hardware y software).
- Análisis y Diseño de Sistemas (especificación detallada del sistema de información y definición de la arquitectura del sistema).
- Desarrollo del Sistema (Construcción del sistema).
- Pruebas (funcionales, estrés y de vulnerabilidades técnicas).
- Implementación y Entrenamiento (entrega del sistema, aprobación del sistema y entrenamiento).
- Pase a Producción (puesta en marcha del sistema).
- Manuales de Usuario y de Sistemas (manual de uso y manual técnico).

6.8.10 Pase a Producción

- El personal del Instituto Nacional de Salud del Niño encargados del desarrollo y mantenimiento de los sistemas, no tendrán acceso a los datos de producción. Los datos sensibles con los que trabajen deben ser diferentes a los datos del ambiente de producción.
- Los ambientes de desarrollo y producción deben ser configurados en servidores diferentes, limitando el acceso solo a personal del Instituto Nacional de Salud del Niño autorizados.
- El pase a producción debe ser realizado exclusivamente por el responsable autorizado por la Oficina de Estadística e Informática, quien llevará un control de los pases efectuados y/o actualizaciones de los sistemas en un registro o bitácora.
- Todo desarrollo antes de su pase a producción debe ser revisado, para asegurar que se cumpla con los estándares establecidos por la Unidad de Informática de la Oficina de Estadística e Informática.

6.8.11 Control de Cambios de las Aplicaciones

- El control, registro y monitoreo de los cambios de los sistemas del Instituto Nacional de Salud del Niño debe ser supervisado por el responsable de la Unidad de Informática de la Oficina de Estadística e Informática. El proceso de control de cambios debe considerar:
  - Planificación del cambio.
  - Responsabilidades y canales de comunicación.
  - Identificación de los recursos comprometidos.
  - Análisis de impacto.
  - Pruebas de comprobación y estrés, controles de seguridad y reversión en ambiente de desarrollo.
  - Registro documentado de los cambios.
  - Acta de conformidad de puesta en producción.
- Todo acceso a la librería o repositorio de los programas fuente será controlado por un responsable designado de la Unidad de Informática de la Oficina de Estadística e Informática para evitar accesos y/o cambios no autorizados.
- Todo cambio efectuado en los sistemas del Instituto Nacional de Salud del Niño deberá ser documentado, contar con un registro de los cambios efectuados y archivado por el responsable designado de la Unidad de Informática.

- La Oficina de Estadística e Informática, debe efectuar revisiones periódicas de los sistemas en el ambiente de producción a fin de asegurar que sólo se hayan efectuado los cambios autorizados.

6.8.12 Gestión de Vulnerabilidades Técnicas

- La Oficina de Estadística e Informática, debe programar la realización de pruebas de comprobación técnica a cargo de especialistas internos o externos según sea el caso para verificar que se han implementado correctamente los controles de seguridad definidos para el hardware y software.
- Identificadas las vulnerabilidades técnicas, se deben determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Los sistemas críticos y en alto riesgo deben ser tratados primero.
- Para la aplicación de una actualización de seguridad (parches) se debe probar y evaluar su efectividad en un ambiente de pruebas, asimismo considerar los riesgos asociados a su aplicación y en todos los casos se debe cumplir con los controles establecidos para la gestión de cambios.

6.9 POLÍTICA DE GESTIÓN DE INCIDENTES

6.9.1 Objetivos

- Asegurar que los eventos y debilidades en la Seguridad de la Información asociados con los Sistemas de Información sean comunicados de una manera que permita que se realice una acción correctiva a tiempo.

6.9.2 Reportando Eventos y Debilidades de la Seguridad de Información

- Los incidentes relativos a la seguridad deben comunicarse a la Oficina de Estadística e Informática y establecerse un procedimiento formal sobre los mismos.
- El personal del Instituto Nacional de Salud del Niño debe conocer el procedimiento de comunicación de incidentes de seguridad y deben informar de los mismos tan pronto como sea posible a la Oficina de Estadística e Informática.
- Son considerados Incidentes de Seguridad para el Instituto Nacional de Salud del Niño:
    a) Pérdida de servicio, equipos o instalaciones (disponibilidad del servicio de TI).
    b) Sobrecargas en los sistemas (software y hardware). Errores Humanos en uso de los sistemas. Incumplimientos de políticas, normas y/o procedimientos sobre seguridad de la Información. Cambios no controlados en los sistemas (software y hardware) y servicios.
    c) Fallas en software y/o hardware.
    d) Violaciones de acceso a los sistemas.
    e) Ataques por software de tipo malicioso (malware).
    f) Correos fraudulentos (phishing) solicitando información del usuario.
    g) Pérdida o Fuga de Información.
    h) Mal Uso y Abuso del Correo electrónico.
    i) Detección de vulnerabilidades de la seguridad.

6.9.3 Gestión de las Mejoras e Incidentes en la Seguridad de Información

- El personal del Instituto Nacional de Salud del Niño debe conocer su responsabilidad respecto a la comunicación de eventos de seguridad y el procedimiento para informar de los mismos tan pronto como sea posible a través de un flujo adecuado para garantizar que el personal del Instituto que comunican los incidentes sean notificados de los resultados una vez que el tema haya sido resuelto.
- Reportados los incidentes de seguridad a las partes correspondientes, se debe proceder al seguimiento detallado de dichos incidentes, los cuales serán investigados por el personal designado por la Oficina de Estadística e Informática para determinar la severidad de los mismos.
- Las infracciones o faltas de seguridad serán corregidas mediante acciones específicas del Comité de Seguridad de la Información.
- Para el del Instituto Nacional de Salud del Niño, la acción disciplinaria a la que serán sometidos será acorde con la severidad del incidente, con base en las conclusiones determinadas por la investigación.
- Periódicamente la Oficina de Estadística e Informática deberá analizar las actividades realizadas y estudiar posibles mejoras o cambios que puedan efectuarse ante futuros incidentes, previniendo la recurrencia de los mismos y evitando que estos se transformen en problemas. Para esto se deberá de realizar un análisis exhaustivo a fin de corregir la situación.
- Este análisis deberá aportar información para poder actuar con medidas:
  - Correctivas; para apoyar a la solución del incidente.
  - Preventivas; para evitar la ocurrencia del mismo o emprender oportunidades de mejora que puedan disminuir la situación de riesgos actual.

6.10 POLÍTICA DE CONTINUIDAD DE NEGOCIO

6.10.1 Objetivos

- Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres.
- Documentar las actividades de recuperación de la operatividad y el servicio ante un incidente o evento severo.
- Documentar los planes y procedimientos de recuperación necesaria e indispensable para recuperar las operaciones y el servicio en el tiempo definido.

6.10.2 Incluyendo la Seguridad de Información en el Proceso de Gestión de la Continuidad del Negocio

- El Instituto Nacional de Salud del Niño, debe elaborar el Plan de Contingencia y Recuperación ante Desastres, el cual se desarrolla a raíz de la necesidad de mantener la disponibilidad ante una situación de contingencia severa que amenace paralizar totalmente los servicios informáticos de la Institución.

- El Plan de Recuperación, el Plan de Contingencia y Recuperación ante Desastres se activará en escenarios de desastres catastróficos y que imposibilite la operación normal de entrega de servicios de TI desde la Oficina de Estadística e Informática.

6.10.3 Continuidad del Negocio y Evaluación de Riesgos

- Los eventos que pueden causar interrupciones a los procesos de negocio deben ser identificados, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.
- En el análisis de impacto se deben de identifican los activos de TI y valorar el impacto en función a la criticidad de estos sobre los procesos de atención del Instituto Nacional de Salud del Niño, así mismo identificar el tiempo objetivo de recuperación y el punto objetivo de recuperación para lo cual el Instituto Nacional de Salud del Niño responde ante una contingencia de desastre.

6.10.4 Redacción e Implantación de Planes de Continuidad que Incluyen la Seguridad de Información

- Plan de Contingencia debe asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas, tras la interrupción o la falla de sus procesos críticos. Así mismo dentro del Plan de Contingencia se debe considerar los tiempos de recuperación y de la estrategia de recuperación por cada sistema de información (aplicaciones y plataformas críticas) que pueden afectar directamente al Instituto Nacional de Salud del Niño, en base a los resultados podemos determinar no sólo la criticidad sino también la priorización y los esfuerzos de recuperación ante una situación de desastre.
  - El Tiempo Objetivo de Recuperación (RTO), refiere al tiempo disponible para recuperar los servicios de TI.
  - El Punto objetivo de Recuperación (RPO) refiere a la magnitud de pérdida de datos medida en términos de un período de tiempo que puede ser tolerado.

6.10.5 Marco de Planificación para la Continuidad del Negocio

Es necesario establecer el marco bajo el cual se desarrollará y ejecutará el Plan de Contingencia y Recuperación ante Desastres, para ello se han definido las siguientes Políticas de este Plan:

- El Plan de Contingencia y Recuperación ante Desastres se ejecutará únicamente cuando ocurra una indisponibilidad severa y por tiempo prolongado que afecte negativamente el servicio en el centro de información principal del Instituto Nacional de Salud del Niño.
- La ejecución del Plan de Recuperación de Desastres no contempla contingencias parciales, es decir sólo se ejecuta ante una situación total de desastre.
- La ejecución del Plan es realizada íntegramente por los especialistas de cada plataforma, junto con proveedores previamente identificados para soporte.

- El Plan de Contingencia debe contar con un sólido procedimiento de respaldo y recuperación de información que se ejecute y permita asegurar la recuperación de toda la información.
- La estrategia de recuperación del Instituto Nacional de Salud del Niño permitirá recuperar dentro de la ventana de tiempo de recuperación definida, tiempo que permitirá recuperar las operaciones de la Institución, minimizando el impacto del evento.

6.10.6 Prueba, Mantenimiento y Reevaluación de los Planes de Continuidad

- El Plan de Contingencia y Recuperación ante Desastres del Instituto Nacional de Salud del Niño debe ser probado regularmente para asegurarse de su actualización y eficacia.
- Las pruebas de los planes deben asegurar que todos los miembros del de recuperación y otro personal relevante están prevenidos de los planes y de sus responsabilidades para la continuidad del negocio y la seguridad de la información. Todos deben saber su rol cuando el plan sea invocado.
- El calendario de pruebas del plan de Contingencia y Recuperación ante Desastres debe indicar cómo y cuándo probar cada elemento del plan.

6.11 POLÍTICA DE CUMPLIMIENTO

6.11.1 Objetivos

- Evitar los incumplimientos de cualquier requisito reglamentario, regulación u obligación contractual, y de todos los requisitos de seguridad de la información implementados por el Instituto Nacional de Salud del Niño.
- Mantener la conformidad de los sistemas de información de acuerdo con las políticas y normas de seguridad de la información del Instituto Nacional de Salud del Niño.
- Mantener un efectivo proceso de auditoría a los sistemas de información.

6.11.2 Cumplimiento con los Requisitos Legales

- Las legislaciones, regulaciones y requerimientos contractuales deben ser identificadas y documentadas en todos los sistemas de información del Instituto Nacional de Salud del Niño.
- La información financiera, de impuestos y registros legales debe ser retenida por un período de al menos 10 años, mientras que el resto de información debe ser retenida por un período de al menos 5 años.
- El personal del Instituto Nacional de Salud del Niño no debe destruir o eliminar registros o información importante, sin la aprobación respectiva de los propietarios de información.

6.11.3 Uso de Software Licenciado

- La Oficina de Estadística e Informática debe velar porque todo el software del Instituto Nacional de Salud del Niño cuente con la respectiva licencia de uso. Cada

vez que se formule un requerimiento de compra de un equipo de cómputo este debe considerar el costo de licencia del sistema operativo y software de ofimática.

- La Oficina de Estadística e Informática debe de evaluar y aprobar cualquier solicitud de software. Las solicitudes de software deben de contar con la justificación necesaria indicando su frecuencia de uso y ser autorizadas por los Directores Ejecutivos, Jefes de Departamentos, Jefes de Servicios, Jefes de Oficinas y Jefes de Unidad donde labora el trabajador.

6.11.4 Protección de Datos y Privacidad de la Información Personal

Se debe asegurar la protección y privacidad tal como lo requiere la legislación aplicable.

6.11.5 Prevención de mal Uso de los Recursos de Procesamiento de Información

Se debe cumplir con las disposiciones establecidas en el Reglamento Interno de Trabajo sobre el buen uso de los bienes.

6.11.6 Revisiones de la Política de Seguridad y de la Conformidad Técnica

- Los Directores Ejecutivos, Jefes de Oficina, Jefes de Departamentos, Jefes de Servicios, Jefes de Oficinas y Jefes de Unidades del Instituto Nacional de Salud del Niño dentro de su área de responsabilidad deben asegurar que se cumplen todas las políticas y procedimientos de seguridad establecidos en la Institución.
- El personal del Instituto Nacional de Salud del Niño que hagan mal uso de los recursos de tecnologías de información serán sancionados según la gravedad de la falta cometida y de conformidad con la normatividad aplicable.
- El Oficial de Seguridad de la Información deberá evaluar el cumplimiento de las Políticas de Seguridad de la Información implantadas en el Instituto Nacional de Salud del Niño, una vez al año o cuando sea solicitado por el Comité de Seguridad de la Información.
- La Oficina de Estadística e Informática, debe programar la realización de pruebas de comprobación técnica (pruebas de intrusión y análisis de vulnerabilidades) a cargo de especialistas internos o externos según sea el caso para verificar que se han implementado.
- Correctamente los controles de seguridad definidos para el hardware y software.

6.11.7 Consideraciones para el Plan de Auditoría de Sistemas

- La Oficina de Estadística e Informática, debe establecer controles de auditoría que permitan contar con registro y supervisión sobre los accesos a los sistemas. La revisión de estos registros debe ser realizada por personal independiente a la actividad auditada.
- La Oficina de Estadística e Informática, debe planificar revisiones a las estaciones de trabajo del Instituto Nacional de Salud del Niño para evitar el mal uso de software no licenciado.

- La Oficina de Estadística e Informática, debe proteger el acceso a las herramientas utilizadas para la auditoría de los sistemas.
- Se debe establecer un Plan de Auditorías con la finalidad de verificar en forma objetiva el cumplimiento y efectividad de las actividades que conforman el Sistema de Gestión de Seguridad de la Información.
- El Plan de Auditorías incluirá 03 etapas: Planificación, Preparación y Ejecución.
- El Oficial de Seguridad de la Información elabora el Plan de Auditorías y lo presentará al Comité de Seguridad de la Información el mismo que contiene los objetivos, fecha a realizarse, duración, áreas o procesos involucrados.

VII RESPONSABILIDADES

- **Comité de Seguridad de la Información**: Es el responsable final de la existencia y cumplimiento de las medidas para mantener un nivel de Seguridad de la Información acorde con el rol de la Institución y los recursos disponibles.
- **Oficial de Seguridad de la Información**: Es el representante de la definición y aplicación de los criterios de Seguridad de la Información en el Instituto Nacional de Salud del Niño.
- **Personal del Instituto Nacional de Salud del Niño**: Tienen la responsabilidad de cumplir con lo establecido en este documento y aplicarlo en su entorno laboral. Además, tienen la obligación de alertar de manera oportuna y adecuada a su jefe inmediato, cualquier situación que atente contra lo establecido en esta política o pueda poner en riesgo la Seguridad de la Información.
- **Propietario de la Información**: Es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. Debe participar activamente en la definición del valor de la información para el Instituto Nacional de Salud del Niño, de manera que se puedan definir los controles apropiados para protegerla.

VIII ANEXOS:

- Anexo 1. Compromiso de Compromiso de sujeción a las Normas para el Uso de las Computadoras, Internet y Correo Electrónico en el Instituto Nacional de Salud del Niño.
- Formulario Nº 001-2021-INSN, Solicitud de Servicio de la Oficina de Estadística e Informativa.

Anexo N°1

Compromiso de sujeción a las Normas para el Uso de las Computadoras, Internet y Correo Electrónico en el Instituto Nacional de Salud del Niño

Por el presente, yo .....identificado con DNI N°....., con el cargo de..... en el Instituto Nacional de Salud del Niño, declaro bajo juramento que tengo pleno conocimiento de las disposiciones establecidas en la Directiva sobre Manual de Políticas de Seguridad del INSN, asumiendo el compromiso de sujetarme a la citada norma, bajo responsabilidad.

Asimismo, declaro tener conocimiento que este documento, debidamente firmado, formará parte de mi información personal.

Breña, ... de 2022

(Firma)

Huella Digital

MINISTERIO DE SALUD – INSTITUTO NACIONAL DE SALUD DEL NIÑO – UNIDAD DE INFORMÁTICA

Anexo N°2

FORMULARIO N° 001-2022- INSN

SOLICITUD DE SERVICIO DE LA OEI

FECHA: _ _/___/_____

DATOS DEL USUARIO

NOMBRE DEL SOLICITANTE: .....

CARGO DEL SOLICITANTE: .....

TIPO DE CONTRATO: .....

ÁREA O UNIDAD: .....

SERVICIOS SOLICITADOS

USUARIO DERED	☐	Creación de cuenta de usuario para hacer uso de una computadora, scanner / impresora de red.
CORREO INSTITUCIONAL	☐	El Correo Institucional es para uso institucional y no personal.
BASE DE DATOS	☐	Indicar el nombre de la DB, Tabla o Script: .....
INTERNET	☐	OTROS ☐ .....

ACCESO A LOS APLICATIVOS

SIAF	☐	SIGA	☐	TRAMITE DOC.	☐ *(1)
RENIEC	☐	LABORATORIO	☐	INTRANET	☐ *(2)
OTRO	☐	.....			

*(1) Para acceder al SISTEMA DE TRAMITE DOCUMENTARIO, se requiere llenar la hoja de acceso suministrado por la OEI.

*(2) Para acceder a la INTRANET, es necesario indicar el número del Documento Nacional de Identidad (DNI).

*(3) Indicar el RUC en el caso de Servicios por Terceros.

DNI |_|_|_|_|_|_|_|_| USUARIO *(3) RUC |_|_|_|_|_|_|_|_|_|_|_| USUARIO

BLOQUEO/CANCELACIÓN/ANULACIÓN DE CUENTAS DE USUARIO

USUARIO: ..... ÁREA O UNIDAD: .....

Deberá ser solicitado por el jefe inmediato del Área, Unidad o Dirección Ejecutiva.

V°B° RESPONSABLE DE ÁREA OUNIDAD	V°B°	USUARIO

OBSERVACIONES:

.....

.....

.....

.....