DIRECTIVA ADMINISTRATIVA N° 320 -MINSA/OGTI-2021

DIRECTIVA ADMINISTRATIVA QUE ESTABLECE LOS MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN EN LA RECETA ELECTRÓNICA PARA TELEMEDICINA

I. FINALIDAD

Contribuir a la mejora de la calidad de la atención de salud, a través de mecanismos de seguridad referidos a la integridad, confidencialidad y disponibilidad de la información de la receta electrónica en Telemedicina.

II. OBJETIVO

2.1 Objetivo General

Establecer los mecanismos de seguridad de la información en la receta electrónica a usarse en Telemedicina

2.2 Objetivos Específicos

- Establecer las medidas de seguridad de la información de la receta electrónica en los servicios de Telemedicina relacionada con la prescripción.
- Establecer las medidas de seguridad de la información de la receta electrónica en los servicios de Telemedicina relacionada con la dispensación.

III. ÁMBITO DE APLICACIÓN

La presente Directiva Administrativa es de aplicación obligatoria para las dependencias del Ministerio de Salud, Gobiernos Regionales, a través de las Direcciones Regionales de Salud, Gerencias Regionales de Salud o las que hagan sus veces, las Direcciones de Redes Integradas de Salud, los Gobiernos Locales, EsSalud, las Sanidades de las Fuerzas Armadas y de la Policía Nacional del Perú, así como para los establecimientos de salud y oficinas farmacéuticas, a nivel nacional que se encuentren involucrados en los procesos de prescripción y dispensación de la receta electrónica en el marco de la Telemedicina.

IV. BASE LEGAL

- Ley N° 26842, Ley General de Salud, y sus modificatorias.
- Ley Nº 27269, Ley de Firmas y Certificados Digitales, y sus modificatorias.
- Ley N° 29733, Ley de protección de datos personales, y su modificatoria.
- Ley N° 29459, Ley de los Productos Farmacéuticos, Dispositivos Médicos y Productos Sanitarios, y sus modificatorias.
- Ley N° 30096, Ley de Delitos Informáticos, y sus modificatorias.
- Ley N° 30421, Ley Marco de Telesalud, y sus modificatorias.
- Ley Nº 30895, Ley que fortalece la función rectora del Ministerio de Salud.
- Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud, y sus modificatorias.

- Decreto Legislativo N°1303, Decreto Legislativo que optimiza procesos vinculados a Telesalud.
- Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses, y su modificatoria.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 013-2006-SA, que aprueba el Reglamento de Establecimientos de Salud y Servicios Médicos de Apoyo, y sus modificatorias.
- Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales, y sus modificatorias.
- Decreto Supremo N° 014-2011-SA, que aprueba el Reglamento de Establecimientos Farmacéuticos, y sus modificatorias.
- Decreto Supremo N° 070-2011-PCM, que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N° 681 y ampliatorias.
- Decreto Supremo N° 105-2012-PCM, que establece disposiciones para facilitar la puesta en marcha de la firma digital y modifica el Decreto Supremo N° 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, y su modificatoria.
- Decreto Supremo N° 026-2016-PCM que aprueba medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el sector público y privado.
- Decreto Supremo N° 008-2017-SA, que aprueba el Reglamento de Organización y Funciones del Ministerio de Salud, y sus modificatorias.
- Decreto Supremo N° 019-2017-JUS, que aprueba el Reglamento del Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses, y sus modificatorias.
- Decreto Supremo N° 050-2018-PCM, que aprueba la definición de la Seguridad Digital en el Ámbito Nacional.
- Decreto Supremo N° 021-2019-PCM, que aprueba el Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública y sus modificatorias.
- Decreto Supremo N° 005-2021-SA, Decreto Supremo que aprueba el Reglamento de la Ley Nº 30421, Ley Marco de Telesalud, y del Decreto Legislativo Nº 1490, Decreto Legislativo que fortalece los alcances de la Telesalud.
- Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisito y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición", en todas las entidades integrantes del sistema nacional de informática.
- Resolución Ministerial N° 004-2016-PCM, que 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. 2a. Edición", en todas las entidades integrantes del sistema nacional de informática, y sus modificatorias.

- Resolución Ministerial N° 431-2015/MINSA, que aprueba el Documento Técnico "Política de Seguridad de la Información del Ministerio de Salud".
- Resolución Ministerial N° 116-2018/MINSA, que aprueba la Directiva Administrativa N° 249-MINSA/2018/DIGEMID, Gestión del Sistema Integrado de Suministro Público de Productos Farmacéuticos, Dispositivos Médicos y Productos Sanitarios – SISMED, y su modificatoria.
- Resolución Ministerial N° 117-2020-MINSA, que aprueba la Directiva Administrativa 285-MINSA/2020/DIGTEL, Directiva para la implementación y desarrollo de los servicios de telemedicina síncrona y asíncrona.
- Resolución Ministerial N° 146-2020-MINSA, que aprueba la Directiva Administrativa N° 286-MINSA/2020/DIGTEL, Directiva Administrativa para la Implementación y Desarrollo de los Servicios de Teleorientación y Telemonitoreo.
- Resolución Ministerial N° 688-2020/MINSA, que aprueba la Directiva Administrativa N° 294-MINSA/2020/OGTI, "Directiva Administrativa que establece el tratamiento de los datos personales relacionados con la salud o datos personales en salud".
- Resolución Ministerial N° 1010-2020-MINSA, que aprueba el Plan Nacional de Telesalud del Perú 2020-2023.
- Resolución Ministerial N° 052-2021/MINSA, que aprueba Directiva Administrativa N° 300-MINSA/2021/DIGTEL, Directiva Administrativa: Lineamientos para la organización del personal asignado para telesalud.
- Resolución Directoral N° 019-2013-JUS/DGPDP, que aprueba la Directiva de Seguridad de la Información Administrada por los bancos de datos personales, emitida por la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos.

V. DISPOSICIONES GENERALES

5.1 DEFINICIONES OPERATIVAS

Para la aplicación de la presente Directiva Administrativa se consideran las siguientes definiciones operativas:

5.1.1 **Activo de Información:** Es cualquier información o elemento relacionado con el tratamiento de la misma (software, equipos de cómputo y telecomunicaciones, servicio de correo electrónico, servicio de internet, archivadores) que tenga valor para la organización. Comprende los recursos con los que cuenta un Sistema de Seguridad de la Información, para que la organización funcione y alcance los objetivos planteados por los niveles de conducción. Estos activos que tienen valor para la organización incluyen a:

- Activos de información pura (datos digitales).
- Activos tangibles, activos intangibles, software de aplicación, sistemas operativos.
- Activos físicos (infraestructura, hardware).

5.1.2 **Agente automatizado:** Son los procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.

5.1.3 **Certificado digital:** El certificado digital es el documento credencial electrónico generado y firmado digitalmente por una entidad de certificación,

que vincula un par de claves con una persona natural o jurídica confirmando su identidad. El ciclo de vida de un certificado digital podría comprender: a) La suspensión, que consiste en inhabilitar la validez de un certificado digital por un período de tiempo establecido en el momento de la solicitud de suspensión. Dicho período no puede superar la fecha de expiración del certificado digital; b) La modificación de la información contenida en un certificado sin la reemisión de sus claves; y, c) La reemisión consiste en generar un nuevo par de claves y un nuevo certificado, correspondiente a una nueva clave pública pero manteniendo la mayor parte de la información del suscriptor contenida en el certificado a expirar.

5.1.4 **Clave privada:** Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.

5.1.5 **Confidencialidad:** Es la cualidad que indica que la información no está disponible y no es revelada a individuos, entidades o procesos sin autorización.

5.1.6 **Confidencialidad de la Información:** Es un atributo que se le asigna a la información por la naturaleza de su contenido o por los principios que rigen a quien accede a esa información, eso hace que el contenido solo pueda ser accedido por personas autorizadas o tomen conocimiento en ejercicio de su labor, quienes tienen el deber de reservar dicha información y no comentar o divulgar la misma fuera del ámbito estrictamente profesional o para la prestación de servicios. La organización o entidad garantiza que la información será protegida para que sea conocida sólo por usuarios autorizados.

5.1.7 **Control:** Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

5.1.8 **Control de acceso:** Son los medios para garantizar que el acceso a los activos esté autorizado y restringido según el negocio y la seguridad.

5.1.9 **Controles Criptográficos:** Es el conjunto de técnicas que hacen posible el intercambio de mensajes por la red de manera segura, que garantiza que los mensajes sólo puedan ser leídos por las personas a quienes van dirigidos.

5.1.10 **Credenciales de autenticación:** Son los criterios establecidos para la verificación de la identificación cierta de un individuo sobre la base de sus credenciales usuario y contraseña, para el acceso a determinado sistema de información.

5.1.11 **Custodio de la Información:** Es la persona o la entidad que tiene la responsabilidad de aplicar y mantener los niveles de protección adecuados en base a las especificaciones dadas por el Responsable de la Información. El rol será asumido generalmente por los administradores de red o el personal que sea contratado para resguardar activos de información.

5.1.12 **Datos personales:** Es toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

5.1.13 **Datos sensibles:** Son los datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular, datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical e información relacionada a la salud o a la vida sexual. Asimismo, aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida efectiva o familiar, los

hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten a su intimidad.

5.1.14 **Disponibilidad de Información:** Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones, es decir, garantizar el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

5.1.15 **Firma digital:** Es la firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no pueden derivar de ella la clave privada.

5.1.16 **Firma electrónica:** Es cualquier símbolo basado en medios electrónicos utilizados o adoptado por una parte con la intención precisa de vincularse, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita. Se incluye dentro de esta definición a la firma o signatura informática.

5.1.17 **Firewall:** Es un dispositivo de seguridad de la red que monitorea el tráfico de red: entrante y saliente; y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad.

5.1.18 **HIPS**: Sistema de prevención de intrusiones basado en el host, protege el sistema contra malware y actividades no deseadas que intentan perjudicar el equipo.

5.1.19 **IDS:** Es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas.

5.1.20 **IOFE:** Es la Infraestructura Oficial de Firma Electrónica del Perú, que está compuesta por los prestadores de servicios de certificación digital cuya competencia técnica y administrativa ha sido oficialmente reconocida.

5.1.21 **IPS**: Es un software que se utiliza para proteger a los sistemas de ataques e intrusiones, su actuación es preventiva.

5.1.22 **Integridad de la Información:** Es el atributo de la información de ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina.

5.1.23 **Log´s:** Son archivos de registro (o archivos de log) que contienen mensajes sobre el sistema.

5.1.24 **PIN:** Es un tipo de contraseña que permite identificarse a la persona y obtener acceso al sistema como la tarjeta SIM, teléfono móvil o el cajero automático.

5.1.25 **Prescripción:** Acto profesional que resulta de un proceso lógico-deductivo, mediante el cual el profesional de salud prescriptor autorizado a partir del conocimiento adquirido de los síntomas presentados por el paciente y el examen físico realizado, concluye una orientación diagnóstica y toma una decisión terapéutica. Está decisión implica indicaciones farmacológicas y/o no farmacológicas que son plasmadas en una receta médica, ciñéndose por la normatividad correspondiente.

5.1.26 **Prescriptor de la Receta electrónica:** Es el profesional de salud autorizado para prescribir, que previamente ha sido designado como usuario activo de

los servicios de información asistenciales de Telemedicina, y usa su firma digital en una receta electrónica. Se incluye al personal de farmacia para el proceso de dispensación.

5.1.27 **Principio de equivalencia funcional:** Es aquel principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndolos sustituir para todos los efectos legales. De conformidad con lo establecido en la Ley y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

5.1.28 **Dispensación**: Acto profesional del Químico Farmacéutico de proporcionar uno o más productos farmacéuticos, dispositivos médicos y productos sanitarios a un paciente o usuario, generalmente en atención a la presentación de una receta elaborada por un profesional autorizado. En este acto el profesional Químico Farmacéutico informa y orienta al paciente o usuario sobre el uso adecuado del producto farmacéutico, reacciones adversas interacciones medicamentosas y las condiciones de conservación del producto o dispositivo.

5.1.29 **Receta electrónica:** Receta médica en formato digital que cumple con lo establecido en las normas legales vigentes y que resulta de la prescripción que realiza un profesional de salud autorizado directamente en un programa informático, y a través de dispositivos electrónicos de transmisión de datos (Computadora personal, tablet, y otros). Incluye la firma digital como respaldo del acto prescriptivo.

5.1.30 **Teleatiendo:** Es un sistema de información asistencial del Ministerio de Salud basado en web para el registro de atenciones de Telemedicina realizado por los profesionales de salud de los establecimientos de salud.

5.1.31 **Telemedicina:** Provisión de servicios de salud a distancia en los componentes de promoción, prevención, diagnóstico, tratamiento, recuperación, rehabilitación y cuidados paliativos, prestados por personal de la salud que utiliza las TIC, con el propósito de facilitar el acceso a los servicios de salud a la población.

5.1.32 **Teleconsulta:** Es la consulta a distancia que se realiza entre un profesional de la salud, en el marco de sus competencias, y una persona usuaria mediante el uso de las TIC, con fines de promoción, prevención, diagnóstico, tratamiento, recuperación, rehabilitación y cuidados paliativos según sea el caso, cumpliendo con las restricciones reguladas a la prescripción de medicamentos y demás disposiciones que determine el Ministerio de Salud.

5.1.33 **Teleinterconsulta:** Es la consulta a distancia mediante el uso de las TIC, que realiza un personal de salud a un profesional de la salud para la atención de una persona usuaria, pudiendo ésta estar o no presente; con fines de promoción, prevención, diagnóstico, tratamiento, recuperación, rehabilitación y cuidados paliativos según sea el caso, cumpliendo con las restricciones reguladas a la prescripción de medicamentos y demás disposiciones que determine el Ministerio de Salud.

5.1.34 **Telemonitoreo:** Es la monitorización o seguimiento a distancia de la persona usuaria, en las Instituciones Prestadoras de Servicios de Salud, en las que se transmite la información clínica de la persona usuaria, y si el caso lo amerita según criterio médico los parámetros biomédicos y/o exámenes auxiliares, como medio de control de su situación de salud. Se puede o no incluir la prescripción de medicamentos de acuerdo al criterio médico y según las competencias de otros profesionales de la salud.

prescripción de medicamentos de acuerdo al criterio médico y según las competencias de otros profesionales de la salud.

5.1.35 **Responsable de la Información:** Para cada órgano o unidad orgánica, es la persona que dirige a dicha instancia, y que tiene la responsabilidad de definir el tratamiento y los niveles de seguridad que se implementarán en la información de su Unidad.

5.1.36 **Riesgo:** Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias.

5.1.37 **Seguridad de la Información:** Es el conjunto de acciones para preservar la confidencialidad, intangibilidad, integridad y disponibilidad de la información, además de otras características como la autenticación, responsabilidad, no repudio y fiabilidad.

5.1.38 **Sesión activa:** Es el tiempo configurado en el sistema de información para que el usuario haga uso de éste y cumpla con su rol establecido.

5.1.39 **Sistema de Información:** Es el conjunto de elementos que interactúan para el tratamiento y administración de datos e información generada que debe cubrir una necesidad o un objetivo, así como estar organizada y disponible para su uso posterior. En el sector salud se incluye los Sistemas de Información Asistenciales y los Sistemas de Información Administrativas.

5.1.40 **Usuario de los servicios de salud:** Es la persona que requiere y hace uso de los servicios de salud intramurales y extramurales de una IPRESS. No implica necesariamente que esté enfermo. Podría ser que use servicios orientados a la prevención de enfermedades, o la promoción de la salud o de estilos de vida saludables, o algún servicio de tipo administrativo.

5.2 ACRÓNIMOS

5.2.1	**ANM**	: Autoridad Nacional de Productos Farmacéuticos, Dispositivos Médicos y Productos Sanitarios
5.2.2	**DIGEMID**	: Dirección General de Medicamentos, Insumos y Drogas
5.2.3	**DIRESA**	: Dirección Regional de Salud
5.2.4	**DIRIS**	: Direcciones de Redes Integradas de Salud
5.2.5	**DPS**	: Datos personales de salud
5.2.6	**GERESA**	: Gerencia Regional de Salud
5.2.7	**IPRESS**	: Instituciones Prestadoras de Servicios de Salud
5.2.8	**MINSA**	: Ministerio de Salud
5.2.9	**OGTI**	: Oficina General de Tecnologías de la Información
5.2.10	**PIN**	: Número de identificación personal
5.2.11	**TIC**	: Tecnologías de la Información y Comunicación
5.2.12	**TUPA**	: Texto Único de Procedimientos Administrativos

5.3 Las IPRESS utilizan la receta electrónica en el servicio de Telemedicina, a través de la Teleconsulta, Teleinterconsulta, Telemonitoreo y otras modalidades que apruebe el Ministerio de Salud.

5.4 Las IPRESS que brindan los servicios de Telemedicina, deben contar con los equipos y herramientas informáticas necesarias para la generación de la receta electrónica, la misma que debe cumplir con la normatividad vigente; así como con el acceso e interoperabilidad a los sistemas de información seguros que garanticen el cumplimiento de las Buenas Prácticas de Prescripción y Dispensación.

5.5 Los profesionales de la salud autorizados para prescribir por la Ley N° 26842, Ley General de Salud, sólo pueden hacer uso de la receta electrónica durante su sesión activa en el sistema de información de Telemedicina, a la cual han ingresado haciendo uso de sus credenciales de autenticación.

5.6 Los profesionales de la salud prescriptores autorizados por Ley que generan una receta electrónica en el servicio de Telemedicina refrendan el acto prescriptivo con su firma digital, haciendo uso de los dispositivos electrónicos disponibles en la IPRESS en la cual brindan servicios.

5.7 En las IPRESS públicas, en tanto se implemente la receta electrónica con firma digital, los profesionales de la salud autorizados para prescribir pueden utilizar en los servicios de Telemedicina la receta electrónica y refrendarla con su firma electrónica siempre que cuente con el respaldo de seguridad de la firma digital generada con un certificado digital de agente automatizado. Por ningún motivo se expide o dispensa la receta electrónica con imagen digital o impresa, careciendo de valor estas presentaciones.

5.8 Los profesionales prescriptores autorizados que brindan los servicios de Telemedicina están impedidos de expedir la receta electrónica en imagen digital, a fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

5.9 En las IPRESS del sector público que brindan servicios de Telemedicina, para la utilización de la receta electrónica con respaldo de firma electrónica, las mismas deben tener implementado el certificado digital de agente automatizado en sus servidores.

5.10 En tanto, las IPRESS de las DIRIS, DIRESA o GERESA no implementen el certificado digital de agente automatizado para Telemedicina en sus servidores, el MINSA brinda el servicio para suscribir la receta electrónica en el Sistema de Información Asistencial "Tele atiendo".

5.11 El MINSA, a través de la Oficina General de las Tecnologías de la Información, debe implementar los mecanismos de seguridad de la información de la receta electrónica del sistema de información asistencial "Tele atiendo".

5.12 La IPRESS asegura que los sistemas de cómputo y sus respectivas bases de datos destinados a Telemedicina estén sincronizados a través de servidores de tiempo que permitan acceder a la fecha y hora oficial del Perú en que se realizó una operación electrónica, tal como lo contempla el artículo 30 del Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece las disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el proceso administrativo, aprobado por Decreto Supremo N° 029-2021-PCM.

5.13 El establecimiento farmacéutico solo puede acceder a la receta electrónica mediante el sistema de información que los articule. Dicho acceso se realiza a través de las credenciales de autenticación otorgadas por el sistema de información asistencial de Telemedicina.

5.14 El Director o jefe de la Red de Salud o IPRESS faculta al coordinador de Telesalud o al responsable de Recursos Humanos o quien haga sus veces, para la creación/generación y asignación de roles a los prescriptores de la receta electrónica.

5.15 Para la implementación de la receta electrónica con firma digital o firma electrónica con certificado digital de agente automatizado del profesional prescriptor autorizado, la IPRESS de la DIRIS, DIRESA o GERESA debe realizar un análisis de riesgo, el cual define la factibilidad de la implementación de la referida receta electrónica. (Según Anexo N° 01); para la elaboración de este análisis se recomienda el acompañamiento de un especialista en seguridad de la información, seguridad digital o ciberseguridad.

5.16 Concluido el análisis de riesgo, los formatos SEG-FOR-3 (Formato de Matriz de Riesgos), SEG-FOR-4 (Formato de Plan de Tratamiento de Riesgos) y SEG-FOR-5 (Formato de Aceptación de Riesgos), contenidos en el Anexo N° 01, se remiten a la OGTI-MINSA para la opinión técnica de los especialistas en seguridad de la información.

VI. DISPOSICIONES ESPECÍFICAS

6.1 DE LOS MECANISMOS DE SEGURIDAD DURANTE LA PRESCRIPCIÓN DE LA RECETA ELECTRÓNICA UTILIZADA EN LOS SERVICIOS DE TELEMEDICINA

6.1.1 De la receta electrónica con firma digital del profesional prescriptor autorizado

a) El prescriptor de la receta electrónica en los servicios de telemedicina habilitado para hacer uso de su certificado digital con función de firma generada bajo la Infraestructura Oficial de Firma Electrónica – IOFE, no requiere mecanismos adicionales para conservar la información contenida en la Receta Electrónica a salvo de adulteraciones y asegurar el cumplimiento del principio de equivalencia funcional y la integridad del contenido del documento electrónico.

b) La IPRESS promueve la gestión y adquisición de los certificados digitales para sus profesionales de la salud.

c) El prescriptor de la receta electrónica debe mantener la reserva a la información relativa a su clave privada. Conforme lo prevé la Ley N° 27269, Ley de Firmas y Certificados Digitales, sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

6.1.2 De la receta electrónica con firma electrónica del profesional prescriptor autorizado con respaldo de certificado digital de agente automatizado

Para que el profesional prescriptor autorizado firme electrónicamente la receta electrónica es necesario lo siguiente:

a) Firma electrónica del profesional prescriptor autorizado

b) Firma digital generada con un certificado digital de agente automatizado.

c) Haber aceptado los términos y condiciones del servicio para dicho fin (Ver Anexo N° 02)

Firma electrónica del profesional prescriptor autorizado

1. La IPRESS que ofrece servicios de Telemedicina es responsable de asegurar que sus sistemas de información permitan la gestión del PIN, la misma que incluye la generación, actualización y recuperación del mismo; cumpliendo los siguientes mecanismos de seguridad:

- Generación obligatoria de un PIN para cada profesional prescriptor autorizado que debe tener vinculación activa con la IPRESS en la cual se utiliza dicho PIN.
- El responsable de Recursos Humanos de la IPRESS valida la referida vinculación activa del profesional prescriptor autorizado.
- Recuperación del PIN: Cuando el prescriptor de la receta electrónica en los servicios de telemedicina olvide su PIN, o se encuentre bloqueado su uso luego de un número de intentos fallidos que no debe superar los 3 intentos, para recuperarlo el Sistema de Información de Telemedicina debe tener implementado un mecanismo para recuperar el PIN, como: envío por correo electrónico o mensaje de texto a su celular con un código de recuperación, el cual debe ingresar acompañado de otros datos que solo es de conocimiento del profesional prescriptor como: la nueva contraseña, la fecha de nacimiento y el dígito verificador del Documento Nacional de Identidad (para los peruanos) o el último dígito del Carnet de Extranjería (para los extranjeros), el cual permite habilitar el nuevo PIN.

2. El prescriptor de la receta electrónica en los servicios de Telemedicina debe ingresar una clave que contiene 8 dígitos numéricos, acompañada de la fecha de nacimiento y el dígito verificador de su Documento Nacional de Identidad (para los peruanos) o el último dígito del Carné de Extranjería (para los extranjeros), para respaldar su autenticación personal.
3. El prescriptor de la receta electrónica en los servicios de telemedicina debe realizar de manera obligatoria la actualización del PIN cada 2 meses. Para la actualización del PIN se debe consignar la clave anterior y proponer una clave nueva distinta a la anterior.
4. El prescriptor de la receta electrónica en los servicios de Telemedicina, adicionalmente, puede actualizar su PIN en el momento que crea conveniente, haciendo uso de las funcionalidades que el sistema de información asistencial de Telemedicina tiene habilitado para dicho fin.

Firma digital generada con un certificado digital de agente automatizado

El MINSA, la DIRIS, la DIRESA/GERESA o la IPRESS, para hacer uso de la firma digital generada con un certificado digital de agente automatizado, debe implementar, como mínimo, los siguientes controles de seguridad a los componentes que forman parte del proceso de la firma digital:

1. **Servidor físico:** Se debe contar con un análisis de vulnerabilidades, aplicando las contramedidas necesarias; los sistemas operativos deben estar actualizados; sólo deben estar abiertos aquellos puertos de comunicación para el consumo de la interface de la firma. Asimismo, debe estar protegido contra malware/ransomware y mediante una seguridad perimetral adecuada (firewall, IPS/IDS).

   El acceso al servidor físico debe estar limitado al administrador, de acuerdo con la política de gestión de accesos. (Ver Anexo N° 03).

2. **Servidor virtualizado:** Se deben incluir controles de seguridad proactiva disponibles, tales como HIPS (Sistema de prevención de intrusiones basado en el host) con prevención automática contra exploits y control de aplicaciones con marcado dinámico en lista blanca; se deben actualizar las versiones de las plataformas de virtualización; el acceso a la plataforma debe estar limitado únicamente al administrador del servidor, de acuerdo a la política de gestión de accesos. (Ver Anexo N° 03)
3. **Base de datos:** Se debe contar con un análisis de vulnerabilidades, luego del cual se aplican las contramedidas que corresponden; deben estar activos los log´s de auditoría; el acceso a la plataforma debe estar limitado al administrador de la base de datos, de acuerdo a la política de gestión de accesos.
4. **Log´s centralizados:** Son parte del proceso de la firma digital; deben estar en una fuente centralizada (servidor o carpeta) con la finalidad de ser auditables.
5. **Equipo de cómputo del prescriptor de la receta electrónica dentro de la red institucional:** Debe estar protegido con antivirus, sistema operativo actualizado, además debe estar custodiado con seguridad perimetral.
6. **Equipo de cómputo del prescriptor de la receta electrónica fuera de la red institucional:** Deben estar protegidos con antivirus y sistema operativo actualizado.
7. **Equipos móviles del prescriptor de la receta electrónica:** Deben contar con la última versión del sistema operativo; se verifica que esté correctamente instalada la aplicación informática para la generación de la firma digital.

6.2 DE LOS MECANISMOS DE SEGURIDAD DURANTE LA DISPENSACIÓN DE LA RECETA ELECTRÓNICA UTILIZADA EN LOS SERVICIOS DE TELEMEDICINA

6.2.1. La Farmacia del Establecimiento de Salud/Oficina Farmacéutica autorizada para la dispensación de lo requerido en una receta electrónica cumple con las Buenas Prácticas de Dispensación aprobadas por la DIGEMID como ANM.

6.2.2. El usuario de los servicios de salud, para solicitar la dispensación de una receta electrónica generada en los servicios de Telemedicina debe presentar en la farmacia del establecimiento de salud/oficina farmacéutica, su documento de identidad físico con el cuál se registró para su atención en el servicio de Telemedicina.

6.2.3. Para los casos en que el usuario de los servicios de salud, cuente con un representante, éste debe presentar en la farmacia del establecimiento de salud/oficina farmacéutica, su documento de identidad y la del usuario de los servicios de salud.

6.2.4. La farmacia del establecimiento de salud/oficina farmacéutica, para acceder a la visualización de la receta electrónica, debe ingresar el número del documento de identidad del usuario de los servicios de salud y la fecha de emisión del mismo.

6.2.5. La farmacia del establecimiento de salud/oficina farmacéutica registra la entrega parcial o total de los productos requeridos en la receta electrónica, a través del ingreso del número de documento físico (boleta de venta, ticket o nota de salida) que evidencia la entrega de los mencionados productos al usuario de los servicios de salud o su representante. La boleta de venta, ticket o nota de salida debe contar con la firma manuscrita del usuario de los servicios de salud o representante legal como constancia de la recepción de los productos.

6.2.6. El establecimiento farmacéutico debe mínimamente cumplir con lo siguiente:

- Los equipos de cómputo deben estar protegido con antivirus y sistema operativo actualizado; además, debe estar custodiado con seguridad perimetral.
- Los equipos móviles deben contar con sistema operativo actualizado.
- Contar con acceso a internet.
- Contar con las credenciales de autenticación proporcionadas por el responsable de Recursos Humanos de la IPRESS, para el uso de Sistema de Información Asistencial de Telemedicina.
- El personal designado para el uso del Sistema de Información asistencial de Telemedicina debe tener el rol de farmacia.
- Los accesos al Sistema de Información asistencial de Telemedicina son de exclusiva responsabilidad del personal designado, ya que dichos accesos son únicos e intransferibles.

VII. RESPONSABILIDADES

7.1 NIVEL NACIONAL

El Ministerio de Salud, a través de la Oficina General de Tecnologías de la Información, es responsable de difundir la presente Directiva Administrativa, supervisar su implementación y cumplimiento, así como brindar la asistencia técnica que se requiera en el marco de sus competencias.

7.2 NIVEL REGIONAL

Las DIRIS, DIRESA o GERESA, a través de sus Oficinas de Informática, Tecnologías de la Información o las que hagan sus veces, son responsables de implementar la presente Directiva Administrativa, así como supervisar y brindar la asistencia técnica que se requiera a las demás unidades orgánicas.

7.3 NIVEL LOCAL

Las IPRESS o establecimientos farmacéuticos de las DIRIS, DIRESA o GERESA a nivel nacional son responsables de la aplicación de la presente Directiva Administrativa.

Los profesionales de la salud prescriptores y dispensadores son responsables del cumplimiento de las Buenas Prácticas de Prescripción y Buenas Prácticas de Dispensación, así como de la aplicación de la presente Directiva Administrativa, en lo que corresponda.

VIII. ANEXOS

8.1 Anexo N° 01: Sistema de Gestión de Seguridad de la Información - Metodología de Gestión de Riesgos

8.2 Anexo N° 02: Modelo referencial de Términos y Condiciones para la suscripción de la receta electrónica con firma electrónica del profesional prescriptor autorizado con respaldo de certificado digital de agente automatizado, en el Sistema de Información Asistencial para Telemedicina

8.3 Anexo N° 03: Política de gestión de accesos.

ANEXO N°01 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN METODOLOGÍA DE GESTIÓN DE RIESGOS

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

METODOLOGÍA DE GESTIÓN DE RIESGOS

1. OBJETIVO
2. ALCANCE
3. TERMINOS Y DEFINCIONES
4. RESPONSABILIDADES
5. DESARROLLO DE LA METODOLOGIA
6. FORMATOS Y SUBANEXOS

1. OBJETIVO

Establecer un método estandarizado para realizar actividades de identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información, en el que la participación del personal del Ministerio de Salud (MINSA), las IPRESS, DIRIS, DIRESAS o GERESAS involucrados en el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) es fundamental.

2. ALCANCE

Aplica al proceso definido dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

3. TÉRMINOS Y DEFINICIONES

Se utilizan los términos y definiciones de la Norma ISO 27000:2014, tales como:

- **Aceptación de Riesgos.-** Decisión informada para tomar un riesgo en particular.
  Nota 1: La aceptación del riesgo puede ocurrir sin el tratamiento del riesgo o durante el proceso de tratamiento de riesgos.
  Nota 2: Riesgos aceptados están sujetos a supervisión y revisión.
- **Amenaza.-** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.
- **Análisis de Riesgo.-** Proceso de comprender la naturaleza del riesgo y determinar el nivel de riesgo.
  Nota 1: El análisis de riesgos proporciona las bases para la evaluación del riesgo y para tomar las decisiones sobre el tratamiento del riesgo.
  Nota 2: El análisis de riesgo incluye la estimación del riesgo.
- **Confidencialidad.-** Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.
- **Consecuencia.-** Resultado de un evento que afecta a los objetivos.
  Nota 1: Un evento puede conducir a una serie de consecuencias.
  Nota 2: Una consecuencia puede ser cierta o incierta, y puede tener efectos positivos o negativos sobre la consecución de los objetivos.
  Nota 3: Las consecuencias pueden ser expresadas cualitativa o cuantitativamente.
  Nota 4: Las consecuencias iniciales pueden convertirse en reacciones en cadena.
- **Comunicación y Consulta de Riesgos.-** Procesos continuos e iterativos que realiza una organización para proporcionar, compartir u obtener información, y para establecer el diálogo con las partes interesadas en relación con la gestión del riesgo.
  Nota 1: La información puede corresponder a la existencia, la naturaleza, la forma, la probabilidad, la importancia, la evaluación, aceptabilidad y tratamiento de la gestión del riesgo.

Nota 2: La consulta constituye un proceso de comunicación informada de doble sentido entre una organización y sus partes interesadas, sobre un tema antes de tomar una decisión o determinar una orientación sobre dicha cuestión: La consulta es:

- Un proceso que impacta sobre una decisión a través de la influencia más que por la autoridad; y
- Una contribución para una toma de decisión, y no una toma de decisión conjunta.

- **Control.-** Medida que modifica un riesgo.

  Nota 1: Los controles incluyen cualquier proceso, la política, dispositivo, práctica, u otras acciones que modifiquen un riesgo.

  Nota 2: Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.

- **Criterios de Riesgo.-** Términos de referencia respecto a los que se evalúa la importancia del riesgo.

  Nota 1: Los criterios de riesgo se basan en los objetivos de la organización, y el contexto externo e interno.

  Nota 2: Los criterios de riesgo se pueden obtener de normas, leyes, políticas y otros requisitos.

- **Disponibilidad.-** Propiedad de ser accesible y utilizable por petición de una entidad autorizada.
- **Evaluación del Riesgo.-** Proceso de la comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable.

  Nota: La evaluación de riesgos ayuda a la decisión sobre el tratamiento del riesgo.

- **Gestión de Riesgos.-** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del Riesgo.-** Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos.

  Nota 1: La identificación de riesgos consiste en la identificación de las fuentes de riesgo, eventos/sucesos, sus causas y sus consecuencias potenciales.

  Nota 2: La identificación de riesgos puede implicar datos históricos, análisis teórico, opiniones informadas y de expertos; así como necesidades de las partes interesadas.

- **Integridad.-** Propiedad de exactitud y lo completo.
- **Nivel de Riesgo.-** Magnitud de un riesgo, expresados en términos de la combinación de las consecuencias y de su probabilidad.
- **Probabilidad.-** Posibilidad de que algún hecho se produzca.
- **Proceso de Gestión de Riesgos.-** Aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación, consulta, estableciendo el contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgo.

  Nota 1: ISO / IEC 27005 se utiliza el término "proceso" para describir la gestión del riesgo global. Los elementos dentro del proceso de gestión de riesgos se denominan «actividades».

- **Propietario del Riesgo.-** Persona o entidad que tiene la responsabilidad y la autoridad para gestionar un riesgo.
- **Riesgo.-** Efecto de la incertidumbre sobre la consecución de los objetivos.

  Nota 1: Un efecto es una desviación de lo esperado - positiva o negativa.

  Nota 2: La incertidumbre es el estado, aunque sea parcial, de la carencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia, o la probabilidad.

  Nota 3: El riesgo se caracteriza a menudo por referencia a los eventos potenciales y consecuencias, o una combinación de éstos.

  Nota 4: El riesgo se expresa a menudo en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad asociada de ocurrencia.

  Nota 5: En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden ser expresados como efecto de la incertidumbre en los objetivos de seguridad de la información.

  Nota 6: El riesgo para la seguridad de información se asocia con la posibilidad de que las amenazas explotarán vulnerabilidades de un activo de información o un grupo de activos de información, y por lo tanto causan daño a la organización.
- **Riesgo Residual.-** Riesgo que queda después del tratamiento del riesgo.

  Nota 1: El riesgo residual puede contener riesgos no identificados.

  Nota 2: El riesgo residual también puede ser conocido como " riesgo retenido".
- **Seguridad de la Información.-** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

  Nota: Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.
- **Tratamiento del Riesgo.-** Proceso para modificar el riesgo.

  Nota 1: El tratamiento del riesgo puede implicar:
  - Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo;
  - Tomar el aumento del riesgo con el fin de perseguir una oportunidad;
  - Eliminación de la fuente de riesgo;
  - El cambio de la probabilidad;
  - El cambio de las consecuencias;
  - Compartir el riesgo con la otra parte o partes (incluyendo los contratos y la financiación del riesgo);
  - Retener el riesgo por elección informada.

  Nota 2: Tratamientos de riesgo que tienen que ver con las consecuencias negativas se refieren a veces como "riesgo mitigación", "eliminación de riesgos", "prevención de riesgos" y "reducción del riesgo".

  Nota 3: El tratamiento del riesgo puede crear nuevos riesgos o modificar los riesgos existentes.

- **Valoración del Riesgo.-** Proceso general de la identificación del riesgo, el análisis de riesgo y la evaluación del riesgo.
- **Vulnerabilidad.-** Debilidad de un activo o de control que puede ser explotado por una o más amenazas.

4. RESPONSABILIDADES

4.1. Propietario de los Activos de Información

- Participar en los talleres de identificación de activos de la información.

4.2. Propietarios del Riesgo

- Definir los niveles de riesgos así como los criterios de aceptación de riesgos.
- Mantener actualizado el inventario de activos de la información que se encuentra bajo su responsabilidad.
- Promover la participación activa del personal en la evaluación y tratamiento de riesgos de seguridad de la información.
- Conformar el equipo de trabajo.
- Aprobar, de forma conjunta con el Presidente del Comité de Seguridad de la Información o Comité de Gobierno Digital, la información documentada correspondiente a la gestión de riesgos del Sistema de Gestión de Seguridad de la Información, entre ella: Ficha de Evaluación de Riesgos, Inventario de Activos de Información, Matriz de Riesgos, Mapa de Riesgos, Plan de Tratamiento de Riesgos, Aceptación de Riesgos.

4.3. Comité de Seguridad de la Información o Comité de Gobierno Digital

- Promover la participación del personal en el proceso de evaluación y tratamiento de riesgos de seguridad de la información.
- Aprobar, a través del Presidente del Comité de Seguridad de la Información o del Comité de Gobierno Digital, la información documentada correspondiente a la gestión de riesgos, entre ella: Inventario de Activos de Información, Matriz de Riesgos, Mapa de Riesgos, Plan de Tratamiento de Riesgos, Aceptación de Riesgos, Declaración de Aplicabilidad.

4.4. Responsable de Seguridad de la Información

- Verificar el cumplimiento del presente documento.
- En coordinación con los propietarios del riesgo, convocar y conformar al equipo de trabajo.
- Capacitación en la identificación, análisis y evaluación de riesgos de seguridad de la información al equipo de trabajo.
- Liderar los talleres a desarrollarse para la identificación, análisis y evaluación de riesgos de seguridad de la información.
- Liderar las reuniones a desarrollarse para el tratamiento de riesgos de seguridad de la información.

- Revisar y presentar a los Propietarios del Riesgo y al Comité de Seguridad de la Información los resultados de la evaluación y tratamiento de riesgos de seguridad de la información.

4.5. Equipo de Trabajo

- Desarrollar la identificación, análisis y evaluación de riesgos de seguridad de la información.
- En coordinación con el Propietario del Riesgo y el Responsable de Seguridad de la Información, identificar a los responsables de la implementación de los planes de acción.

4.6. Responsables de la Implementación

- Implementar los planes de acción a su cargo, definidos en el plan de tratamiento de riesgos.

5. DESARROLLO DE LA METODOLOGÍA

5.1. Condiciones Generales

- El proceso de identificación, análisis y evaluación de riesgos de seguridad de la información se realiza una vez al año o cuando ocurran cambios en los activos y/o proceso que forma parte del alcance del SGSI.
- El proceso de tratamiento de riesgos de seguridad de la información se realiza posterior a la culminación del proceso de evaluación de riesgos de seguridad de la información.

5.2. Marco de Trabajo

- El proceso de evaluación de riesgos de seguridad de la información se realiza mediante talleres con el equipo de trabajo.
- Para la definición del marco de trabajo del proceso de evaluación de riesgos de seguridad de la información el responsable de seguridad de la información convoca al propietario del riesgo y personal involucrado en el proceso como parte del alcance del SGSI, que se considere. Los propietarios de riesgo determinan los niveles de riesgos, así como los criterios de aceptación de riesgos.

  Esta actividad es registrada en el documento **SEG-FOR-1** Formato de Ficha de Evaluación de Riesgos, el cual consta de las siguientes partes:

5.2.1. Número (N°)

El responsable de seguridad de la información debe asignar un número correlativo en el campo "N°".

5.2.2. Fecha

El responsable de seguridad de la información debe detallar la fecha de la elaboración de la ficha en el campo "FECHA".

5.2.3. Área

El responsable de seguridad de la información debe detallar el nombre del área dueña del proceso, en el campo "ÁREA".

5.2.4. Proceso

El responsable de seguridad de la información debe detallar el nombre del proceso en el campo "PROCESO".

5.2.5. Documentos Relacionados al Proceso

El propietario del riesgo debe detallar los documentos relacionados al proceso en el campo "DOCUMENTOS RELACIONADOS AL PROCESO".

5.2.6. Áreas (Personal Clave) y Terceros Involucrados

El propietario del riesgo debe detallar el personal clave y las áreas a las que pertenecen dentro del Ministerio de Salud (MINSA), las IPRESS, DIRIS, DIRESAS o GERESAS y, el personal y/o las organizaciones externas involucradas en el proceso en el campo "ÁREAS (PERSONAL CLAVE) Y TERCEROS INVOLUCRADOS".

5.2.7. Requisitos Normativos, Legales y/o Contractuales

El propietario del riesgo debe detallar los requisitos normativos, legales y/o contractuales aplicables al proceso en el campo "REQUISITOS NORMATIVOS, LEGALES Y/O CONTRACTUALES".

5.2.8. Equipo de Trabajo

El propietario del riesgo con el apoyo del responsable de seguridad de la información, debe detallar los nombres y apellidos, cargo/rol y área/organización externa del equipo de trabajo en el campo "EQUIPO DE TRABAJO".

5.2.9. Propietario de los Riesgos

El responsable de seguridad de la información debe detallar el propietario de los riesgos en el campo "PROPIETARIO DE LOS RIESGOS".

5.2.10. Herramientas

El responsable de seguridad de la información debe detallar las herramientas que se utilizan en el campo "HERRAMIENTAS".

5.2.11. Fuentes de Información

El responsable de seguridad de la información, con el apoyo del propietario del riesgo, debe detallar las fuentes de información en el campo "FUENTES DE INFORMACIÓN".

El responsable de seguridad de la información del MINSA realiza una charla de capacitación al equipo de trabajo y propietarios del riesgo, con el fin de explicar la presente metodología y los formatos a utilizar, así como dar a conocer los niveles de riesgo, criterios de aceptación de riesgos, niveles de riesgo aceptables y, los criterios para la realización de las evaluaciones de riesgos de seguridad de la información.

5.3. Inventario de Activos de Información

Para la identificación de activos de información del proceso se utiliza el documento **SEG-FOR-2** Formato de Inventario de Activos de Información, el cual consta de las siguientes partes:

5.3.1. Área

El responsable de seguridad de la información debe detallar el nombre del área dueña del proceso.

5.3.2. Proceso

El responsable de seguridad de la información debe detallar el nombre del proceso al que pertenecen los activos de información identificados.

5.3.3. Fecha

El responsable de seguridad de la información debe detallar la fecha de la identificación de activos de información.

5.3.4. Código del Activo

El responsable de seguridad de la información debe asignar un código correlativo.

5.3.5. Nombre del Activo

El Equipo de Trabajo detallará el nombre del activo de información identificado.

5.3.6. Detalle del Activo

El equipo de trabajo describe un breve detalle del activo. Ejemplo: Manual del Proceso ABC, Manual de Usuario del Sistema XYZ, Manual Técnico del Sistema XYZ, Reporte ABC, etc.

5.3.7. Propietario del Activo

El equipo de trabajo detalla el nombre del propietario del activo de información identificado; bajo el concepto que éste es el responsable de controlar la producción, desarrollo, mantenimiento, uso y seguridad del activo de información, tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo.

5.3.8. Tipo y Categoría del Activo

El equipo de trabajo, teniendo en cuenta el Subanexo N° 1: "Lista General de Activos de Información" detallan el tipo del activo y categoría del activo.

Tener en cuenta que si se identifica un activo que no se encuentra en el Subanexo N° 1: "Lista General de Activos de Información" se debe registrar en el documento SEG-FOR-2 Formato de Inventario de Activos de Información, para su posterior actualización en el citado Subanexo.

5.3.9. Clasificación de Información

El Equipo de Trabajo coloca la clasificación del activo de información identificado, la cual se define de la siguiente manera:

- **SECRETA (S):** De acuerdo al artículo 15 del Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo N° 021-2019-JUS, la información expresamente clasificada como secreta, es aquella que se sustente en razones de seguridad nacional y tenga como base fundamental garantizar la seguridad de las personas y cuya revelación originaría riesgos para la integridad territorial y/o subsistencia del sistema democrático, así como respecto a las actividades de inteligencia y contrainteligencia dentro del marco que establece el Estado de Derecho en función de las situaciones.

  Restricción: No pueden ser copiados, fotocopiados, extraídos o reproducidos interna y/o externamente, los documentos originales cuya información esté clasificada como Secreta.

- **RESERVADA (R):** De acuerdo al artículo 16 del texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo N° 021-2019-JUS, es aquella que por razones de seguridad nacional en el ámbito del orden interno cuya revelación originaría riesgo a la integridad territorial y/o la subsistencia del sistema democrático. En consecuencia, se considera reservada la información que tiene por finalidad prevenir y reprimir la criminalidad en el país y cuya revelación puede entorpecerla.

  Restricción: No pueden ser reproducidos por personas ajenas al MINSA, las IPRESS, DIRIS, DIRESAS o GERESAS o al Sector Salud, los documentos originales cuya información esté clasificada como Reservada.

- **CONFIDENCIAL (C):** De acuerdo al numeral 5 del artículo 17 del Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo N° 021-2019-JUS, es considerada información confidencial a la referida a los datos personales cuya publicidad constituye una invasión de la intimidad personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal. En este caso, sólo el juez puede ordenar la publicación sin perjuicio de lo establecido en el inciso 5 del artículo 2 de la Constitución Política del Estado.
  Restricción: Esta información no puede ser reproducida por personas ajenas al Ministerio de Salud (MINSA), las IPRESS, DIRIS, DIRESAS o GERESAS o al Sector Salud.

- **USO INTERNO (I):** Activos de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno de la Institución y que sólo pueden ser divulgados a terceras partes teniendo firmado un acuerdo de confidencialidad, siempre y cuando su divulgación no impacte a la Institución.

- **PÚBLICA (P):** La información pública es información cuyo contenido no es sensible, de acceso público y que su divulgación no genera impacto en la Institución.

5.3.10. Ubicación Específica

El Equipo de Trabajo colocará la ubicación específica del activo de información identificado.

5.3.11. Valor del Activo

El equipo de trabajo coloca el valor del activo de información identificado, la cual se define de la siguiente manera:

- **Alto:** Activo importante para la Institución. Su disponibilidad es necesaria para los procesos críticos de la Institución.
- **Medio:** Constituye un soporte para los activos importantes de la Institución. La información puede estar replicada en varias fuentes o existen medios alternos. No compromete los procesos críticos de la Institución.
- **Bajo:** Activos secundarios, que constituyen información para la toma de decisiones de un área específica. No compromete ningún proceso crítico de la Institución.

5.4. Identificación, Análisis y Evaluación de Riesgos

Una vez concluido el Inventario de Activos de Información, se inicia la identificación, análisis y evaluación de riesgos. Sólo los activos de valor "Alto", son los considerados en esta etapa.

Para esta actividad se utiliza el documento SEG-FOR-3 Formato de Matriz de Riesgos, el cual consta de las siguientes partes:

5.4.1. Área

El responsable de seguridad de la información debe detallar el nombre del área dueña del proceso.

5.4.2. Proceso

El responsable de seguridad de la información debe detallar el nombre del proceso.

5.4.3. Fecha

El responsable de seguridad de la información debe detallar la fecha de la identificación, análisis y evaluación de riesgos.

5.4.4. Nombre del Activo

El responsable de seguridad de la información coloca el nombre de los activos de valor "Alto" que se identificaron en el Inventario de Activos de Información.

En el Inventario de Activos de Información, los activos de información son identificados en forma independiente; sin embargo, cuando estos han sido tasados y son similares pueden ser agrupados como por ejemplo: XP24000, EVA6300, son 2 activos Storage - Disk Array, en la matriz de riesgos aparecerá agrupado de la siguiente forma: Storage - Disk Array (XP24000, EVA6300).

5.4.5. Amenaza

El equipo de trabajo para la identificación de las amenazas utiliza el Subanexo N° 2: "Tabla de Amenazas", bajo el concepto que amenaza es un evento que potencialmente puede causar daño.

5.4.6. Vulnerabilidad

El equipo de trabajo, para la identificación de las vulnerabilidades utiliza el Subanexo N° 3: "Tabla de Vulnerabilidades", bajo el concepto que vulnerabilidad es una debilidad de la Institución que puede ser explotada por una amenaza.

5.4.7. Evaluación del Criterio CID

El equipo de trabajo, para poder determinar cómo la amenaza afecta la Confidencialidad (C), Integridad (I) y Disponibilidad (D) del activo, evalúa cada uno de los criterios CID. Se toman los valores según las siguientes tablas:

a) Tabla de Valorización de Confidencialidad

VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA
3	**Alta**	Es la información o recurso que debe ser divulgada sólo a fuentes autorizadas, controladas y debidamente identificadas. Debe ser modificada y leída por un grupo reducido de personas autorizadas y claramente identificadas.	La divulgación no autorizada produce: Uso malicioso en contra de la Institución. - Pérdidas financieras que no pueden ser absorbidas por la Institución. - Demandas legales que dañan la imagen y confianza pública de la Institución.
2	**Media**	Es la información que debe ser divulgada sólo al personal de las áreas que la manejan y modificada sólo por personas autorizadas e individualizadas.	La divulgación no autorizada produce: - Uso malicioso en contra de la imagen o situaciones puntuales. - Pérdidas financieras que pueden ser absorbidas por la Institución. - No se producen demandas legales.
1	**Baja**	Es la información que puede ser divulgada a público general, pero que sólo puede ser modificada por personas autorizadas.	La divulgación no autorizada no representa perjuicio para la Institución.

b) Tabla de Valorización de Integridad

VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA
3	**Alta**	Es la información o recurso que, al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de gran magnitud.	La falta de integridad produce daños de gran magnitud, los que se pueden expresar como: - Pérdidas económicas (pérdida, incumplimiento de metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo más allá de lo estimado como manejable). - Daño de la imagen de la Institución (daño a nivel nacional e internacional que no se puede reparar en el corto plazo). - Pérdida de la confianza de los usuarios.
2	**Media**	Es la información o recurso que, al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de mediana magnitud.	La falta de integridad produce daños de mediana magnitud, los que se pueden expresar como: - Pérdidas económicas (menor ganancia, incumplimiento de metas en menor escala). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un periodo de tiempo que está en el límite superior de lo estimado como manejable). - Daño de la imagen de la Institución (daño a nivel nacional, se puede reparar en el corto plazo). - No se pierde la confianza de los usuarios.
1	**Baja**	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de pequeña magnitud.	La falta de integridad produce daños de pequeña magnitud los que se pueden expresar como: - Pérdidas económicas (no impacta las ganancias, se cumplen las metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo pero este es manejable). - Daño de la imagen de la Institución (daño a nivel nacional que puede no ser percibido y se puede reparar prontamente). - No se pierde la confianza de los usuarios.

c) Tabla de Valorización de Disponibilidad

VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA
3	**Alta**	Es información o activo indispensable para la continuidad de la Institución. El recurso principal y el alternativo no pueden faltar por un período prolongado de tiempo en horarios críticos.	La falta de disponibilidad por períodos prolongados produce: - Incumplimiento a los acuerdos de nivel de servicio. La transición entre el recurso principal y el alternativo no debe impactar el acuerdo de servicio. - Perjuicios legales que afectan la imagen de la Institución. - Perjuicios económicos que no pueden ser absorbidos por la Institución.
2	**Media**	La disponibilidad de la información es necesaria para la continuidad de la Institución, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable. El recurso principal y el alternativo pueden quedar fuera de servicio por un periodo mínimo de tiempo en horarios críticos.	La falta de disponibilidad produce: - Que los niveles de servicio acordados se puedan ver afectados en la transición entre el medio principal y el alternativo. - Perjuicios legales que no comprometen la imagen de la Institución. - Perjuicios económicos que pueden ser absorbidos por la Institución.
1	**Baja**	Es información o activos de apoyo o secundarios para la institución. La información se encuentra duplicada en varias fuentes. Si no está disponible no compromete procesos operativos importantes.	La falta de disponibilidad produce: - Que los niveles de servicio acordados para los procesos operativos importantes, no se vean afectados. - Problemas administrativos y operativos no significativos. - Perjuicios económicos que no son significativos. - No hay perjuicios legales.

5.4.8 Valor CID

El Equipo de Trabajo calcula el valor CID de acuerdo a la siguiente tabla:

a) Tabla de Valorización

ASPECTO DE SEGURIDAD AFECTADO POR EL RIESGO			VALOR CID
C	I	D	

1	1	1	No Significativo
1	1	2	Bajo
1	1	3	Alto
1	2	1	Bajo
1	2	2	Mediano
1	2	3	Alto
1	3	1	Alto
1	3	2	Alto
1	3	3	Extremo
2	1	1	Bajo
2	1	2	Mediano
2	1	3	Alto
2	2	1	Mediano
2	2	2	Mediano
2	2	3	Alto
2	3	1	Alto
2	3	2	Alto
2	3	3	Extremo
3	1	1	Alto
3	1	2	Alto
3	1	3	Extremo
3	2	1	Alto
3	2	2	Alto
3	2	3	Extremo
3	3	1	Extremo
3	3	2	Extremo
3	3	3	Extremo

5.4.9 Impacto

El Equipo de Trabajo determina el impacto de acuerdo a la siguiente tabla.

a) Tabla de Valorización del Impacto del Riesgo

NIVEL	DESCRIPCIÓN	IMPACTO
5	**Extremo**	Impacta en forma severa en la Institución al punto de comprometer la confidencialidad o integridad de información crítica y/o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a toda la Institución y su efecto repercute en todo el personal involucrado.

4	**Alto**	Impacta en forma grave a un área o servicio específico de la Institución, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves por un tiempo considerable. Su efecto está limitado dentro de la Institución.
3	**Mediano**	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	**Bajo**	El impacto es leve y se puede prescindir del mismo en un tiempo limitado.
1	**No Significativo**	No representa un impacto importante para la Institución.

5.4.10 Probabilidad

El Equipo de Trabajo determina la probabilidad de ocurrencia de acuerdo a la siguiente tabla:

a) Tabla de Valoración de la Probabilidad de Ocurrencia

VALOR	CLASIFICACIÓN	DEFINICIÓN
1	**Muy Baja**	El evento no ocurre nunca o casi nunca. Ha ocurrido al menos 1 vez al año.
2	**Baja**	Si bien el evento puede ocurrir el periodo entre uno y otro evento puede ser muy grande. Al menos 2 veces al año.
3	**Moderada**	Es posible que ocurra el evento con una frecuencia baja. 3 o 4 veces al año.
4	**Alta**	Existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo pero la frecuencia no es alta. 1 vez al mes.
5	**Muy Alta**	El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta. 1 vez a la semana o más.

5.4.11 Nivel de Riesgo

El riesgo efectivo es la medida del daño probable causado por una amenaza, que se materializa en un activo. Con el valor obtenido del producto del impacto por la probabilidad, el equipo de trabajo obtiene el nivel de riesgo de acuerdo a la siguiente tabla:

a) Tabla de Valorización del Riesgo

TABLA DE VALORIZACIÓN DE RIESGOS					
IMPACTO		**PROBABILIDAD**		**NIVEL DE RIESGO**	

Extremo	5	Muy Alta	5	Extremo	25
Alto	4	Muy Alta	5	Extremo	20
Mediano	3	Muy Alta	5	Extremo	15
Bajo	2	Muy Alta	5	Alto	10
No Significativo	1	Muy Alta	5	Mediano	5
Extremo	5	Alta	4	Extremo	20
Alto	4	Alta	4	Extremo	16
Mediano	3	Alta	4	Alto	12
Bajo	2	Alta	4	Mediano	8
No Significativo	1	Alta	4	Bajo	4
Extremo	5	Moderada	3	Extremo	15
Alto	4	Moderada	3	Alto	12
Mediano	3	Moderada	3	Alto	9
Bajo	2	Moderada	3	Mediano	6
No Significativo	1	Moderada	3	Bajo	3
Extremo	5	Baja	2	Alto	10
Alto	4	Baja	2	Mediano	8
Mediano	3	Baja	2	Mediano	6
Bajo	2	Baja	2	Bajo	4
No Significativo	1	Baja	2	No Significativo	2
Extremo	5	Muy Baja	1	Mediano	5
Alto	4	Muy Baja	1	Bajo	4
Mediano	3	Muy Baja	1	Bajo	3
Bajo	2	Muy Baja	1	No significativo	2
No Significativo	1	Muy Baja	1	No significativo	1

Los riesgos son clasificados de acuerdo a niveles, según su grado de exposición, lo cual realizará el equipo de trabajo según la siguiente tabla:

b) Tabla de Nivel de Riesgo

RANGO DE RIESGO	NIVEL DE RIESGO	DESCRIPCIÓN DE LAS CONSECUENCIAS
De 15 a 25	**Extremo**	Puede afectar seriamente a la Institución, en términos de paralización de las operaciones. Requiere acción correctiva inmediata más allá del tiempo tolerable, pérdidas considerables o demandas legales y daño considerable.

De 9 a 12	**Alto**	Puede afectar los niveles de operación y servicio de la Institución, incumplimiento de metas, y divulgación no autorizada de información fuera de la Institución. Requiere una acción correctiva sujeta a la discreción de los propietarios del riesgo en términos de plazos y compromisos.
De 5 a 8	**Mediano**	Afecta a los activos de información de soporte a los activos principales, puede afectar la disponibilidad en áreas específicas de la Institución. La divulgación no autorizada no representa perjuicio importante para la Institución. Su aceptación está sujeta a la revisión de los propietarios del riesgo.
De 3 a 4	**Bajo**	No causa un efecto considerable en la Institución. Usualmente son aceptados sin revisión.
De 1 a 2	**No Significativo**	El efecto para la Institución es insignificante. Usualmente no se les considera para la gestión de riesgos.

5.4.12 Nombre del Riesgo

El responsable de seguridad de la información asigna un nombre para el riesgo que sirva para identificarlo respecto de otros.

5.4.13 Código del Riesgo

El responsable de seguridad de la información asigna un código para el riesgo que sirva para identificarlo respecto de otros.

5.5. Tratamiento del Riesgo

El MINSA, las IPRESS, DIRIS, DIRESAS o GERESAS reconocen los niveles de riesgos, definidos por los propietarios del riesgo, en la siguiente tabla:

a) Tabla de Nivel de Riesgo

NIVEL DE RIESGO	DESCRIPCIÓN DE LAS CONSECUENCIAS
Extremo	Puede afectar seriamente a la Institución, en términos de paralización de las operaciones. Requiere acción correctiva inmediata más allá del tiempo tolerable, pérdidas considerables o demandas legales y daño considerable.
Alto	Puede afectar los niveles de operación y servicio de la Institución, incumplimiento de metas, y divulgación no autorizada de información fuera de la Institución. Requiere una acción correctiva sujeta a la discreción de los propietarios del riesgo en términos de plazos y compromisos.
Mediano	Afecta a los activos de información de soporte a los activos principales, puede afectar la disponibilidad en áreas específicas de la Institución. La divulgación no autorizada no representa

	perjuicio importante para la Institución. Su aceptación está sujeta a la revisión de los propietarios del riesgo.
Bajo	No causa un efecto considerable en la Institución. Usualmente son aceptados sin revisión.
No Significativo	El efecto para la Institución es insignificante. Usualmente no se les considera para la gestión de riesgos.

- Para la etapa de tratamiento del riesgo:
  - Se consideran como aceptables los riesgos definidos como: "Mediano", "Bajo" y "No Significativo".
  - Para los riesgos de nivel "Extremo" y "Alto" se procede a evaluar las siguientes opciones de tratamiento de riesgo: "Reducir" o "Evitar" o "Transferir" o "Aceptar".

Todo ello según lo especificado en la siguiente tabla:

b) Opciones del Tratamiento del Riesgo

TRATAMIENTO	DETALLES DEL TRATAMIENTO DE RIESGOS
Reducir	Hacer algo para disminuir la probabilidad de ocurrencia de un riesgo y/o disminuir el impacto si se concreta a un umbral aceptable.
Aceptar	No realizar ninguna acción consciente o intencionadamente para hacer frente a un riesgo.
Evitar	Hacer desaparecer el riesgo, eliminar cualquier probabilidad de ocurrencia.
Transferir	Entregarle la administración de un riesgo a un tercero que lo pueda manejar mejor que la Institución.

La decisión sobre el tratamiento de un riesgo se realiza en cada ciclo de evaluación, el cual se efectúa una vez al año o cuando ocurran cambios en el proceso y/o activos de información parte del alcance del SGSI. Los planes de tratamiento de riesgo, son revisados con periodicidad no mayor a un año por parte del Comité de Seguridad de la Información o el Comité de Gobierno Digital, los nuevos riesgos efectivos son medidos y comparados con los riesgos residuales estimados.

Se realiza el tratamiento de los riesgos identificados en el documento SEG-FOR-3 Formato de Matriz de Riesgos, lo cual se plasma en el documento SEG-FOR-4 Formato de Plan de Tratamiento de Riesgos.

Para la aceptación de riesgos identificados, los riesgos que en el documento SEG-FOR-4 Formato de Plan de Tratamiento de Riesgos indiquen opción de tratamiento "Aceptar", se plasman en el documento SEG-FOR-5 Formato de Aceptación de Riesgos.

En la determinación del riesgo residual, cuando ya se han aplicado las medidas de control previstas, los valores a utilizar se hacen sobre la premisa de controles implementados. De forma similar que el riesgo efectivo, para el riesgo residual se utiliza la Tabla de Valorización del Riesgo y Tabla de Nivel de Riesgo.

El riesgo residual se plasma en el documento SEG-FOR-4 Formato de Plan de Tratamiento de Riesgos.

6. FORMATOS Y SUBANEXOS

6.1. Subanexos

- Subanexo N° 1: Lista General de Activos de Información.
- Subanexo N° 2: Tabla de Amenazas.
- Subanexo N° 3: Tabla de Vulnerabilidades.

6.2. Formatos

- SEG-FOR-1 Formato de Ficha de Evaluación de Riesgos.
- SEG-FOR-2 Formato de Inventario de Activos de Información.
- SEG-FOR-3 Formato de Matriz de Riesgos.
- SEG-FOR-4 Formato de Plan de Tratamiento de Riesgos.
- SEG-FOR-5 Formato de Aceptación de Riesgos.

Subanexo N° 1: Lista General de Activos de Información

TIPO	CATEGORIA
Información	Electrónica
	Impresa
	Electrónica e Impresa
Software	Software comercial
	Software de terceros
	Software desarrollado internamente
	Otro software
Físico	Equipo de procesamiento
	Equipo virtual de procesamiento
	Equipo de comunicación
	Instalaciones
	Otro equipo
Personas	Responsables de tomar decisiones (Directores, Jefes, entre otros)
	Otros trabajadores
Servicios	Servicios públicos
	Procesamiento y comunicaciones
	Otros servicios

Subanexo N° 2: Tabla de Amenazas

CÓDIGO	AMENAZA	TIPO
AM1	Incendio	Daño físico
AM2	Daño por agua	
AM3	Contaminación	
AM4	Accidente mayor	
AM5	Destrucción del equipo o los medios	
AM6	Polvo, corrosión, congelación	
AM7	Fenómeno climático	Eventos naturales
AM8	Fenómeno sísmico	
AM9	Fenómeno volcánico	
AM10	Fenómeno meteorológico	

CÓDIGO	AMENAZA	TIPO
AM11	Inundación	
AM12	Fallas del sistema de aire acondicionado o del suministro de agua	**Pérdida de servicios esenciales**
AM13	Pérdida del suministro de electricidad	
AM14	Falla del equipo de telecomunicaciones	
AM15	Radiación electromagnética	**Perturbación debido a radiación**
AM16	Radiación térmica	
AM17	Pulsos electromagnéticos	
AM18	Intercepción de señales de interferencia comprometedoras	**Compromiso de la información**
AM19	Espionaje remoto	
AM20	Interceptación de comunicaciones	
AM21	Robo de medios o documentos	
AM22	Robo de equipos	
AM23	Hallazgo de medios reciclados o descartados	
AM24	Divulgación	
AM25	Datos de fuentes no confiables	
AM26	Adulteración del Hardware	
AM27	Adulteración del software	
AM28	Detección de posición	
AM29	Falla de equipo	**Fallas técnicas**
AM30	Mal funcionamiento del equipo	
AM31	Saturación del sistema de información	
AM32	Mal funcionamiento del software	
AM33	Uso no autorizado del equipo	**Acciones no autorizadas**
AM34	Copia fraudulenta del software	
AM35	Uso de software falsificado o copiado	
AM36	Corrupción de datos	
AM37	Procesamiento ilegal de datos	
AM38	Error en el uso	**Compromiso de funciones**
AM39	Abuso de derechos	
AM40	Falsificación de derechos	
AM41	Negación de acciones	
AM42	Ruptura en la disponibilidad del personal	

CÓDIGO	AMENAZA	TIPO
AM43	Hacking	**Hacker, cracker**
AM44	Ingeniería social	
AM45	Intrusión en el sistema, incursiones	
AM46	Acceso no autorizado al sistema	
AM47	Crimen informático (acoso cibernético)	**Criminal informático**
AM48	Acto fraudulento (reproducción de archivos, suplantación, intercepción)	
AM49	Soborno informático	
AM50	Falsificación o usurpación de la dirección	
AM51	Intrusión en el sistema	
AM52	Bomba/Terrorismo	**Terrorismo**
AM53	Equipo de guerra informática	
AM54	Ataque al sistema (ej. DDOS)	
AM55	Penetración en el sistema	
AM56	Adulteración del sistema	
AM57	Ventaja de defensa	**Espionaje**
AM58	Ventaja política	
AM59	Explotación económica	
AM60	Robo de información	
AM61	Intrusión en la privacidad personal	
AM62	Asalto a un empleado	**Gente dentro de la Institución (empleados mal capacitados, resentidos, maliciosos, negligentes, deshonestos o despedidos)**
AM63	Chantaje	
AM64	Búsqueda de información propietaria	
AM65	Abuso informático	
AM66	Fraude y robo	
AM67	Soborno por información	
AM68	Ingreso de datos falsificados o corruptos	
AM69	Intercepción	
AM70	Códigos maliciosos (ej. Virus, bomba lógica, troyano)	
AM71	Venta de información personal	
AM72	Disfunciones del sistema (bugs)	
AM73	Intrusión en el sistema	
AM74	Sabotaje al sistema	

CÓDIGO	AMENAZA	TIPO
AMXX	Otros que se indiquen en los talleres	**Otros**

Subanexo N° 3: Tabla de Vulnerabilidades

CÓDIGO	VULNERABILIDAD	CATEGORÍA
VU1	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	**Hardware**
VU2	Falta de esquemas de reemplazo periódicos	
VU3	Susceptibilidad a la humedad, al polvo y a la suciedad	
VU4	Sensibilidad a la radiación electromagnética	
VU5	Falta de control eficiente del cambio de configuración	
VU6	Susceptibilidad a variación de voltaje	
VU7	Susceptibilidad a variaciones de temperatura	
VU8	Almacenamiento no protegido	
VU9	Falta de cuidado al descartarlo	
VU10	Equipo desfasado por vigencia tecnológica	
VU11	Pruebas al software inexistentes o insuficientes	**Software**
VU12	Errores conocidos en el software	
VU13	No hacer "logout" cuando se sale de la estación de trabajo	
VU14	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	
VU15	Falta de evidencia de auditoria	
VU16	Asignación equivocada de derechos de acceso	
VU17	Software ampliamente distribuido	
VU18	Aplicar programas de aplicación a datos incorrectos en términos del tiempo	
VU19	Interfaz de usuario complicada	
VU20	Falta de documentación	
VU21	Seteo incorrecto de parámetros	
VU22	Fechas incorrectas	
VU23	Falta de mecanismos de identificación y autentificación como la autentificación de usuarios	
VU24	Tablas de claves no protegidas	
VU25	Mala administración de claves	
VU26	Habilitación de servicios innecesarios	
VU27	Software inmaduro o nuevo	

CÓDIGO	VULNERABILIDAD	CATEGORÍA
VU28	Especificaciones no claras o incompletas para los desarrolladores	
VU29	Falta de control de cambios eficaz	
VU30	Descarga y uso incontrolado de software	
VU31	Falta de copias de respaldo	
VU32	No producir informes de gestión	
VU33	Falta de pruebas de envió o recepción de mensaje	Red
VU34	Líneas de comunicación no protegidas	
VU35	Tráfico delicado no protegido	
VU36	Juntas malas en el cableado	
VU37	Punto de falla única	
VU38	Falta de identificación y autentificación del destinatario	
VU39	Arquitectura de red insegura	
VU40	Transferencia de claves en claro	
VU41	Gestión inadecuada de la red (capacidad de recuperación del ruteo)	
VU42	Conexiones no protegidas de la red publica	
VU43	Ausencia del personal	Personal
VU44	Procedimientos inadecuados del reclutamiento	
VU45	Capacitación de seguridad insuficiente	
VU46	Uso incorrecto del software y hardware	
VU47	Falta de conciencia de seguridad	
VU48	Falta de mecanismos de monitoreo	
VU49	Trabajo no supervisado del personal externo o de limpieza	
VU50	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	
VU51	Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	Sitio
VU52	Ubicaciones en una área susceptible a las inundaciones	
VU53	Red inestable de energía eléctrica	
VU54	Falta de protección física del edificio, puertas y ventanas	
VU55	Falta de un procedimiento formal para el registro y baja de usuarios	Institución
VU56	Falta de proceso formal para revisar el derecho de acceso (supervisión)	

CÓDIGO	VULNERABILIDAD	CATEGORÍA
VU57	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros	
VU58	Falta de procedimientos de monitoreo de instalaciones de procesamiento de la información	
VU59	Falta de auditorías regulares (supervisión)	
VU60	Falta de procedimientos de identificación y evaluación del riesgo	
VU61	Falta de informes de fallas registradas en los registros del administrador y del operador	
VU62	Respuesta inadecuada del mantenimiento del servicio	
VU63	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	
VU64	Falta de procedimiento de control de cambios	
VU65	Falta de procedimiento formal para el control de la documentación de la institución	
VU66	Falta de procedimiento formal para la supervisión del registro de la institución	
VU67	Falta de proceso formal para autorización de información pública disponible	
VU68	Falta de asignación apropiada de responsabilidades de seguridad en la información	
VU69	Falta de planes de continuidad	
VU70	Falta de una política de uso de correos electrónicos	
VU71	Falta de procedimientos para introducir software en sistemas operativos	
VU72	Faltas de registro en los historiales del administrador y del operador	
VU73	Falta de procedimientos para manejo de la información clasificada	
VU74	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos	
VU75	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)	
VU76	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	
VU77	Falta de política formal sobre el uso de computadoras portátiles	
VU78	Falta de control de activos que se encuentran fuera del local	
VU79	Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"	
VU80	Falta de autorización al acceso a las instalaciones de procesamiento de la información	
VU81	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	

CÓDIGO	VULNERABILIDAD	CATEGORÍA
VU82	Falta de revisiones regulares de la gestión	
VU83	Falta de procedimientos para reportar debilidades en la seguridad	
VU84	Falta de procedimientos sobre el cumplimiento de disposiciones respecto de derechos intelectuales	
VUXX	Otros que se indiquen en los talleres	**Otros**

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**Id: SEG-FOR-1**
		Versión: V1 **xx.xx.21**
FICHA DE EVALUACIÓN DE RIESGOS		

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma:	Firma:	Firma:

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
MINSA-SGSI Ficha de Evaluación de Riesgos	1	Primera versión	xx/xx/2021

CLASIFICACIÓN DEL DOCUMENTO

CONFIDENCIAL

DIFUSIÓN LIMITADA

NOTA DE CONFIDENCIALIDAD: La información contenida en este documento es CONFIDENCIAL y sólo puede ser utilizada por el MINSA conforme al apartado CONTROL DE DIFUSIÓN. Es responsabilidad de la(s) IPRESS, DIRIS, DIRESA(s) o GERESA (s) receptora(s) de este documento su distribución interna, en función de la necesidad de conocer la información contenida en el mismo.

CONTROL DE DIFUSIÓN

AUTOR/ES:

DISTRIBUCIÓN:

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**Id: SEG-FOR-1**
		Versión: V1 xx.xx.21
FICHA DE EVALUACIÓN DE RIESGOS		

N°	xx – 20xx	**FECHA**	xx/xx/20xx
ÁREA			
PROCESO			
DOCUMENTOS RELACIONADOS AL PROCESO	•		
ÁREAS (PERSONAL CLAVE) Y TERCEROS INVOLUCRADOS	**Personal y Áreas dentro de la organización:** • • **Personal y/o Organizaciones externas:** •		
REQUISITOS NORMATIVOS, LEGALES Y/O CONTRACTUALES	• •		
EQUIPO DE TRABAJO	**NOMBRES Y APELLIDOS**	**CARGO/ROL**	**ÁREA / ORGANIZACIÓN EXTERNA**
PROPIETARIO DE LOS RIESGOS	•		
HERRAMIENTAS	•		
FUENTES DE INFORMACIÓN	•		

FIRMAS

NOMBRE Y FIRMA DEL PROPIETARIO DEL RIESGO

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**Id: SEG-FOR-2**
		Versión: V1 **xx.xx.21**
INVENTARIO DE ACTIVOS DE INFORMACIÓN		

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma:	Firma:	Firma:

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
MINSA-SGSI Inventario de Activos de Información	1	Primera versión	xx/xx/2021

CLASIFICACIÓN DEL DOCUMENTO

CONFIDENCIAL
DIFUSIÓN LIMITADA
NOTA DE CONFIDENCIALIDAD: La información contenida en este documento es CONFIDENCIAL y sólo puede ser utilizada por el MINSA conforme al apartado CONTROL DE DIFUSIÓN.
Es responsabilidad de la(s) IPRESS, DIRIS, DIRESA(s) o GERESA (s) receptora(s) de este documento su distribución interna, en función de la necesidad de conocer la información contenida en el mismo.

CONTROL DE DIFUSIÓN

AUTOR/ES:

DISTRIBUCIÓN:

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Id: SEG-FOR-2
		Versión: V1 xx.xx.21
INVENTARIO DE ACTIVOS DE INFORMACIÓN		

Área: _____

Proceso: _____

Fecha: _____

CÓDIGO	NOMBRE DEL ACTIVO	DETALLE DEL ACTIVO	PROPIETARIO DEL ACTIVO	TIPO DEL ACTIVO	CATEGORÍA DEL ACTIVO	CLASIFICACIÓN DE INFORMACIÓN	UBICACIÓN ESPECÍFICA	VALOR DEL ACTIVO

FIRMAS

_____

NOMBRE Y FIRMA DEL PROPIETARIO DEL RIESGO

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**Id: SEG-FOR-3**
		Versión: V1 **xx.xx.21**
MATRIZ DE RIESGOS		

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma:	Firma:	Firma:

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
MINSA-SGSI Matriz de Riesgos	1	Primera versión	xx/xx/2021

CLASIFICACIÓN DEL DOCUMENTO

CONFIDENCIAL
DIFUSIÓN LIMITADA
NOTA DE CONFIDENCIALIDAD: La información contenida en este documento es CONFIDENCIAL y sólo puede ser utilizada por el MINSA conforme al apartado CONTROL DE DIFUSIÓN. Es responsabilidad de la(s) IPRESS, DIRIS, DIRESA(s) o GERESA (s) receptora(s) de este documento su distribución interna, en función de la necesidad de conocer la información contenida en el mismo.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**Id: SEG-FOR-3**
		Versión: V1 **xx.xx.21**
MATRIZ DE RIESGOS		

CONTROL DE DIFUSIÓN

AUTOR/ES:
DISTRIBUCIÓN:

Área: _____

Proceso: _____

Fecha: _____

NOMBRE DEL ACTIVO	AMENAZA	VULNERABILIDAD	¿Qué afecta en los activos de información?				RIESGO EFECTIVO				
			C	I	D	VALOR CID	IMPACTO	PROBABILIDAD	NIVEL DE RIEGO	NOMBRE DEL RIESGO	CÓDIGO DEL RIESGO

FIRMAS

_____

NOMBRE Y FIRMA DEL PROPIETARIO DEL RIESGO

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**Id: SEG-FOR-4**
		Versión: V1 **xx.xx.21**
PLAN DE TRATAMIENTO DE RIESGOS		

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma:	Firma:	Firma:

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
MINSA-SGSI Plan de Tratamiento de Riesgos	1	Primera versión	xx/xx/2021

CLASIFICACIÓN DEL DOCUMENTO

CONFIDENCIAL
DIFUSIÓN LIMITADA
NOTA DE CONFIDENCIALIDAD: La información contenida en este documento es CONFIDENCIAL y sólo puede ser utilizada por el MINSA conforme al apartado CONTROL DE DIFUSIÓN. Es responsabilidad de la(s) IPRESS, DIRIS, DIRESA(s) o GERESA (s) receptora(s) de este documento su distribución interna, en función de la necesidad de conocer la información contenida en el mismo.

CONTROL DE DIFUSIÓN

AUTOR/ES:

DISTRIBUCIÓN:

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Id: SEG-FOR-4
		Versión: V1 xx.xx.21
PLAN DE TRATAMIENTO DE RIESGOS		

Área: _____

Proceso: _____

Fecha: _____

CÓDIGO DEL RIESGO	NOMBRE DEL RIESGO	NIVEL DE RIESGO	NOMBRE DE LA ACTIVO	AMENAZA	VULNERABILIDAD	TRATAMIENTO DEL RIESGO	CONTROL REFERENCIA ISO 27001	ACTIVIDAD A REALIZAR PARA LA IMPLEMENTACIÓN DEL CONTROL	RIESGO RESIDUAL			RESPONSABLE DE LA IMPLEMENTACIÓN	ÁREA DEL RESPONSABLE DE LA IMPLEMENTACIÓN	FECHA DE INICIO DE LA IMPLEMENTACIÓN	FECHA FIN DE LA IMPLEMENTACIÓN	ESTADO
									P(X)	IMPACTO	RIESGO RESIDUAL					

FIRMAS

_____

NOMBRE Y FIRMA DEL PROPIETARIO DEL RIESGO

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**Id: SEG-FOR-5**
		Versión: V1 **xx.xx.21**
ACEPTACIÓN DE RIESGOS		

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma:	Firma:	Firma:

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
MINSA-SGSI Aceptación de Riesgos	1	Primera versión	xx/xx/2021

CLASIFICACIÓN DEL DOCUMENTO

CONFIDENCIAL

DIFUSIÓN LIMITADA

NOTA DE CONFIDENCIALIDAD: La información contenida en este documento es CONFIDENCIAL y sólo puede ser utilizada por el MINSA conforme al apartado CONTROL DE DIFUSIÓN. Es responsabilidad de la(s) IPRESS, DIRIS, DIRESA(s) o GERESA (s) receptora(s) de este documento su distribución interna, en función de la necesidad de conocer la información contenida en el mismo.

CONTROL DE DIFUSIÓN

AUTOR/ES:

DISTRIBUCIÓN:

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Id: SEG-FOR-5
		Versión: V1 xx.xx.21
ACEPTACIÓN DE RIESGOS		

Área: _____

Proceso: _____

Fecha: _____

El Propietario de Riesgos, del Ministerio de Salud (MINSA), la(s) IPRESS, DIRIS, DIRESA(s) o GERESA (s) declara:

- Que la aceptación de los riesgos es una decisión tomada con entera responsabilidad, en forma totalmente voluntaria y sin presiones.
- Un riesgo aceptado podría provocar daños graves a futuro en la Institución, sin embargo, asumimos la responsabilidad personal de aceptar el(los) riesgo(s) aquí descritos y el impacto que estos puedan tener en el (MINSA), la(s) IPRESS, DIRIS, DIRESA(s) o GERESA (s).
- La responsabilidad personal no significa que somos financieramente responsables de las pérdidas que pueden ocurrir como resultado de la aceptación de riesgos. La responsabilidad personal significa que la aceptación de estos riesgos puede comprometer los recursos, y los sistemas.
- También entendemos que la aceptación de estos riesgos y sus responsabilidades expira en un año a partir de la fecha de firma de este documento.
- La aceptación actual de este riesgo no significa que con un cambio de las condiciones actuales en que se encuentre estos riesgos pueden ser mitigados en un futuro con las condiciones financieras técnicas y administrativas adecuadas.
- He leído la declaración y estoy de acuerdo en aceptar los siguientes riesgos:

N°	CÓDIGO DEL RIESGO	NOMBRE DEL RIESGO	NIVEL DE RIESGO
1			
2			
3			

FIRMAS

_____

NOMBRE Y FIRMA DEL PROPIETARIO DEL RIESGO

DIRECTIVA ADMINISTRATIVA N° 320 -MINSA/OGTI-2021
DIRECTIVA ADMINISTRATIVA QUE ESTABLECE LOS MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA RECETA ELECTRÓNICA EN TELEMEDICINA

ANEXO N° 02: MODELO REFERENCIAL DE TÉRMINOS Y CONDICIONES PARA LA SUSCRIPCIÓN DE LA RECETA ELECTRÓNICA CON FIRMA ELECTRÓNICA DEL PROFESIONAL PRESCRIPTOR AUTORIZADO CON RESPALDO DE CERTIFICADO DIGITAL DE AGENTE AUTOMATIZADO, EN EL SISTEMA DE INFORMACIÓN ASISTENCIAL PARA TELEMEDICINA

1. **PRESENTACIÓN**
   - El (nombre de la entidad a cargo), en adelante LA ENTIDAD, con tipo y número de documento de identidad, con domicilio, pone a disposición de sus usuarios del sistema de información asistencial (SIA).
   - Breve descripción del servicio que ofrece el SIA
   - Nombre del banco o bancos de datos personales donde se registrarán los datos personales, así como el número de registro en el RNPDPD de ser el caso.
   - Objeto de los Términos y Condiciones

2. **USO DE DATOS PERSONALES**

Los datos personales expresados a continuación son los necesarios para la suscripción de la receta electrónica en **el Sistema de Información Asistencial para telemedicina denominado** ....., de conformidad con lo señalado en la Directiva Administrativa Nº 301-2021-MINSA, Directiva Administrativa que aprueba la trama estandarizada de datos para la prescripción y dispensación de medicamentos, aprobada mediante Resolución Ministerial N° 053-2021-MINSA.
Los datos personales solicitados a **EL USUARIO** son de carácter obligatorio. En caso **EL USUARIO** no proporcione los datos obligatorios, no podrá suscribir la receta electrónica.
El USUARIO no podrá oponerse o cancelar los datos obligatorios solicitados para la suscripción de la receta electrónica, dispuestos en la Directiva Administrativa Nº 301-2021-MINSA, Directiva Administrativa que aprueba la trama estandarizada de datos para la prescripción y dispensación de medicamentos, aprobada mediante Resolución Ministerial N° 053-2021-MINSA, mientras mantenga el vínculo contractual o laboral con la IPRESS.

a) **Datos de EL USUARIO en la receta electrónica:**
   - **Datos obligatorios para profesional de práctica general**

     Datos personales
     - Tipo y número de documento de identidad
     - Nombres y apellidos
     - Celular
     - Correo electrónico

     Datos profesionales
     - Profesión
   - **Datos adicionales de carácter obligatorio para profesional de práctica especializada**

     Datos profesionales
     - Colegiatura
     - Especialidad
     - RNE

b) **Bancos de datos de acceso público**
La ENTIDAD propietaria del Sistema de Información Asistencial para telemedicina..... accede a los siguientes bancos de datos de acceso público para contar con la información de **EL USUARIO** descritos en el anterior literal a) en la receta electrónica.
- Registro Nacional del Personal de la Salud – INFORHUS
- Registro de Información Migratoria – RIM - MIGRACIONES
- Registro Único de Identificación de Personales Naturales – RUIPN - RENIEC

Al ser bancos de datos personales de INFORHUS, MIGRACIONES y RENIEC, en caso **EL USUARIO** requiera la actualización, rectificación, supresión o cancelación de algunos de estos datos personales deben ser solicitados ante las entidades que administran dichos bancos de datos.

c) **Finalidad**
Los datos personales señalados tienen por finalidad la identificación del profesional que suscribirá la receta electrónica a través del **Sistema de Información Asistencial para telemedicina**.....
La suscripción mediante la firma electrónica y firma digital de agente automatizado permite la generación de la receta electrónica.

d) **Flujo transfronterizo**
Indicar países en los cuales se realizaría flujo transfronterizo de ser el caso y las finalidades de la transferencia.

e) **Ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición - ARCO**
Para el ejercicio de los derechos de **Acceso, Rectificación, Cancelación y Oposición – ARCO debe dirigir correspondencia a xxxxx@entidad.gob.pe donde un profesional del derecho designado por la ENTIDAD absolverá sus consultas**.

3. **OBLIGACIONES DEL USUARIO**
Serán obligaciones de **EL USUARIO**, las contenidas en la legislación peruana y los presentes **TÉRMINOS Y CONDICIONES**:

- **EL USUARIO** está obligado a respetar los **TÉRMINOS Y CONDICIONES** de uso actuales y futuras actualizaciones establecidas por **LA ENTIDAD PÚBLICA**, en calidad de propietaria del **Sistema de Información Asistencial para telemedicina**.....
- Generar el PIN y firmar electrónicamente mediante los procedimientos señalados por **LA ENTIDAD PÚBLICA**, en estos **TÉRMINOS Y CONDICIONES**.
- **EL USUARIO** será notificado cuando se requieran nuevos datos personales y fines adicionales, para el tratamiento de sus datos personales en la receta electrónica. Además, se solicitará la autorización respectiva o informará, según sea el caso, siguiendo las indicaciones de lo establecido en la Ley N° 29733, Ley de Protección de Datos Personales.
- **EL USUARIO** es responsable de la prescripción de la medicación que realiza en la receta electrónica dentro del área de su profesión, así como del contenido de la misma.
  EL USUARIO está obligado a hacer uso responsable de su PIN para realizar la firma electrónica, como requisito indispensable para invocar al servicio de la firma digital de agente automatizado.
  El PIN es:
  - Exclusivo: solo **El USUARIO** puede hacer uso del mismo, no pudiendo transferirlo, compartirlo, cederlo u otro acto de disposición, ante otros.
  - Reservado: **El USUARIO** mantiene el control y la reserva del PIN, no pudiendo ser divulgado, ni puesto en conocimiento a otros, bajo su responsabilidad.
- Se prohíbe hacer uso del PIN y por ende generar firmas electrónicas permitidas mediante el **Sistema de Información Asistencial para telemedicina**....., en los siguientes casos:
  - No cuente con las competencias profesionales para los actos que vaya a suscribir.
  - No tenga relación contractual o laboral vigente con alguna IPRESS que sea usuaria del **Sistema de Información Asistencial para telemedicina**..... / **EL USUARIO** solo hace uso de las firmas electrónicas incluyendo el uso del PIN, mientras cuente con contrato o vínculo laboral vigente con la IPRESS usuaria del **Sistema de Información Asistencial para telemedicina**....., siendo el **USUARIO** el único responsable por este incumplimiento.

  Si Usted no cuenta con las competencias profesionales para la prescripción de medicamentos y por error ha tenido acceso a un PIN, comunicarse inmediatamente a soporte_aplicativos@example.gob.pe (particularizar la extensión de acuerdo a la entidad), o acudir al responsable de recursos humanos de la IPRESS de su jurisdicción, para la baja correspondiente de esta facultad, bajo responsabilidad.
- El **USUARIO** como propietario del PIN está obligado, bajo responsabilidad, a cambiar su PIN al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:
  a) Exposición, puesta en peligro o uso indebido del PIN.
  b) Deterioro, alteración o cualquier otro hecho u acto que afecte el PIN.
  c) Riesgo de vulneración de los datos personales del USUARIO.

5. Cláusula de propiedad intelectual
6. Cláusula de prohibiciones de uso en eso SIA, delitos informáticos
7. Legislación y jurisdicción aplicable

ANEXO N°03: POLÍTICA DE GESTIÓN DE ACCESOS

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**Id: SEG-POL-4**
		Versión: V1 **xx.xx.21**
POLÍTICA DE GESTIÓN DE ACCESOS		

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma:	Firma:	Firma:

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
MINSA-SGSI Política de Gestión de Accesos	1	Primera versión	xx/xx/2021

CLASIFICACIÓN DEL DOCUMENTO

CONFIDENCIAL
DIFUSIÓN LIMITADA
NOTA DE CONFIDENCIALIDAD: La información contenida en este documento es CONFIDENCIAL y sólo puede ser utilizada por el MINSA conforme al apartado CONTROL DE DIFUSIÓN. Es responsabilidad de la(s) IPRESS, DIRIS, DIRESA(s) o GERESA (s) receptora(s) de este documento su distribución interna, en función de la necesidad de conocer la información contenida en el mismo.

CONTROL DE DIFUSIÓN

AUTOR/ES:

DISTRIBUCIÓN:

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Id: SEG-POL-4
		Versión: V1 xx.xx.21
POLÍTICA DE GESTIÓN DE ACCESOS		

1. GESTIÓN DE ACCESO

1.1. Objetivos

a) Segmentar, limitar y asignar los privilegios correspondientes para el acceso de la información, primando el "menor privilegio".
b) Controlar y monitorear la gestión, manejo y uso de la información del MINSA.
c) Prevenir los riesgos de perdida, eliminación y sustracción de información, mitigando las amenazas.

1.2. Política

1.2.1. Requisitos para el control de acceso

Los accesos a los recursos de información y las plataformas informáticas del MINSA son de acuerdo a las funciones y actividades del usuario o que estén desinadas por el jefe inmediato, debiéndose tomar en cuenta lo siguiente:

- Los requerimientos de seguridad de cada aplicación y sistemas de información.
- Mapeo de toda la información con relación a las aplicaciones, parametrizando esta, su impacto y valorando el riego.
- Detallar y ser claro en las políticas de control de acceso y la clasificación de la información.
- Revisión periódica y auditoria permanente de los controles de acceso.
- Revocación de los derechos de acceso.

1.2.1.1. La OGTI:

a) Establece procedimientos de autorización y control para proteger el acceso a la red de datos, previo requerimiento de los jefes inmediatos o responsables de estos datos, definiendo los permisos mínimos y necesarios para el desempeño de las funciones del usuario.
b) Brinda las credenciales de usuario (UserID) único y personalizado para acceder a la infraestructura tecnológica y activos de información de la institución, este será de uso exclusivo para quien fue creado.
c) Procede a la creación de las cuentas y accesos a las diferentes plataformas tecnológicas, cuando el personal inicie un vínculo laboral con el MINSA y sea notificado por la OGGRRH; para el caso de los prestadores de servicios personales, será desde la emisión de la orden de servicio, previa notificación de la OGA al área usuaria.
d) Verifica periódicamente que los usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios para los que fueron autorizados.
e) Realiza cambios de privilegios (permisos y responsabilidades) de los usuarios previa solicitud del jefe inmediato o superior.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Id: SEG-POL-4
		Versión: V1 xx.xx.21
POLÍTICA DE GESTIÓN DE ACCESOS		

1.2.2. Gestión de acceso de usuario

Los responsables de los órganos, direcciones, áreas, oficinas autorizan y solicitan a la OGTI los niveles de accesos, permisos y privilegios a los sistemas, plataformas de información y aplicativos para el personal, proveedores de servicios, indicando los niveles de acceso o privilegios.

1.2.2.1. OGGRRHH:

a. Solicita a la OGTI la baja de las cuentas de acceso del personal cuando finalicen su contrato laboral.

1.2.2.2. La OGTI

b. Coordina con la OGGRRHH la relación contractual antes de otorgar las credenciales según corresponda a los sistemas de información.
c. Cancela las cuentas de acceso una vez finalizada las labores del personal cesado, terceros y proveedores, teniendo un día hábil de plazo como máximo a partir de la comunicación de los responsables de los órganos y dependencias.
d. Coordina la cancelación de las cuentas de acceso de los administradores de los sistemas de información antes de su cese.
e. Lleva un registro del personal que cumple el rol de administrador de los sistemas de información.

El Oficial de Seguridad de la Información revisa periódicamente en coordinación con los responsables de los Sistemas de información, las cuentas de acceso del personal.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Id: SEG-POL-4
		Versión: V1 xx.xx.21
POLÍTICA DE GESTIÓN DE ACCESOS		

1.3. Responsabilidades de los usuarios

1.3.1. Uso de información de autentificación secreta

Los usuarios de los sistemas de información:

- Mantener la confidencialidad de su contraseña (no compartirlas) y cambiar la misma si tiene algún indicio de su vulnerabilidad.
- Los usuarios cambian su contraseña cada 90 días en el directorio activo de forma obligatoria.

1.4. Control de acceso a los sistemas y aplicaciones

Los administradores de los sistemas de información configuran a los sistemas considerando lo siguiente:

- Obligar a los usuarios que cambien su contraseña cuando se ingrese por primera vez.
- Bloquear el acceso luego de 3 intentos fallidos, reestableciéndose luego de 5 minutos.
- Obligar a los usuarios a cambiar su contraseña cada 90 días.
- Se debe guardar los registros de intentos fallidos y exitosos de acceso. (dependiendo de la capacidad de almacenamiento, se van depurando los registros).

1.4.1. La OGTI:

- Los desarrolladores aseguran que no se guarden en la pantalla las contraseñas ingresadas, asimismo deshabilitar el recordar campos de contraseña.

FIRMAS

NOMBRE Y FIRMA DEL PROPIETARIO DEL RIESGO