

## SUPLEMENTO

### SUMARIO

Instituto Ecuatoriano de Seguridad Social:

Resoluciones

C.D. 521

Expídense las políticas que regulan las actividades relacionadas con el uso de tecnologías de la información y comunicaciones

C.D. 524

Expídense las disposiciones de aplicación interna del Acuerdo de seguridad Social entre la República de Colombia y la República del Ecuador

### CONTENIDO

#### No. C.D. 521

#### CONSEJO DIRECTIVO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL

Considerando:

Que, la Constitución de la República del Ecuador en el Art. 370 establece que el Instituto Ecuatoriano de Seguridad Social, entidad autónoma regulada por la ley, será responsable de la prestación de las contingencias del seguro universal obligatorio a sus afiliados, en concordancia de lo dispuesto en los artículos 16, 17 y 18 de la Ley de Seguridad Social;

Que, con la vigencia del Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, contenido la Resolución N° C.D. 457 de 8 de agosto de 2013, reformada con Resoluciones N° C.D. 483 y N° C.D. 497 de 13 de abril y 18 de septiembre de 2015 respectivamente, se establece la estructura organizacional de la institución, con las responsabilidades y funciones de los diversos órganos de gestión, operativas y de apoyo administrativo entre otras, la Dirección Nacional de Tecnología de la Información, encargada de la planificación, coordinación y dirección de las actividades referentes a los procesos de gestión tecnológica de información y comunicaciones;

Que, la Procuraduría General del IESS, sobre la aprobación a nivel nacional de las políticas y procedimientos inherentes a Tecnología de la Información, emite el criterio jurídico constante en memorando N° IESS-PG-2014- 1479-M de mayo 30 de 2014, concluyendo que la Dirección General del IESS "... no tiene facultad legislativa...", y por lo tanto "... tales políticas y procedimientos deberán ser presentados al Consejo Directivo.";

Que, el Director General del IESS, a través de memorando N° IESS-DG-2015-0669-M de 26 de marzo de 2015, pone en conocimiento de la Dirección Nacional de Tecnología de la Información el cumplimiento inmediato de las recomendaciones contenidas en el informe de evaluación constante en el oficio N° 05632-DATI de 6 de marzo de 2015, realizadas por la Contraloría General del Estado dentro del examen especial a los procesos de seguridad en los servidores de correo, base de datos y sistema operativo de la plataforma del Instituto Ecuatoriano de Seguridad Social, por el periodo comprendido entre el 1 de enero de 2013 al 31 de diciembre de 2014, entre otras, para la Coordinación General de Gestión Estratégica y la Dirección Nacional de Tecnología de la Información, recomendaron: "N° 25. Dispondrá la actualización e implementación de normas, políticas estándares, procedimientos e instructivos que regulen las actividades relacionadas con TI, gestionará su aprobación ante la máxima autoridad; y, realizará el seguimiento y monitoreo de su cumplimiento.; y, N° 26. Validará, actualizará, gestionará la aprobación, difundirá y vigilará el estricto cumplimiento de las normas, políticas, estándares, procedimientos e instructivos que regulen las actividades relacionadas con TI que incluirán: tareas, periodicidad, responsables, acciones por incumplimiento, procedimientos de supervisión, control y monitoreo.";

Que, la Contraloría General del Estado, en el Informe General aprobado del examen especial a los procesos de seguridad en los servidores de correo, base de datos y sistema operativo de la plataforma del Instituto Ecuatoriano de Seguridad Social, por el periodo comprendido entre el 1 de enero de 2013 al 31 de diciembre de 2014, recomienda al Consejo Directivo del IESS lo siguiente: "9. Aprobará las políticas que regulen las actividades relacionadas con: plataforma y servicios tecnológicos, procesos de gestión TI y seguridad de la información, dispondrá su difusión y cumplimiento.";

Que, las Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos, dentro de la Norma 410 TECNOLOGIA DE LA INFORMACION, la 410-04 Políticas y procedimientos, establece: "La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

La Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.

Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.

Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización.

Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.

Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos.

La Unidad de Tecnología de Información deberá promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información.”.

Que, mediante Memorando No. IESS-PG-2016-0661-M de 19 de abril de 2019 el Procurador General manifiesta que “...El Proyecto de Resolución que contiene las Políticas que regulan las actividades relacionadas con el uso de las Tecnologías de la Información y Comunicaciones no contraviene norma legal alguna y se considera que debe ser conocido por el Consejo Directivo del IESS para su aprobación”; y,

En uso de las atribuciones que le confiere el artículo 27 letra f) y c) de la Ley de Seguridad Social; el artículo 4 del Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, y demás ordenamiento jurídico invocado, el Consejo Directivo,

Resuelve:

Expedir las Políticas que regulan las actividades relacionadas con el uso de Tecnologías de la Información y Comunicaciones, que se detallan a continuación:

## TÍTULO I GENERALIDADES

Art. 1.- Finalidad.- Las Políticas de Tecnología de la Información y Comunicación tienen como finalidad el proteger la información, a la Institución y buscar un aumento en la seguridad y aprovechamiento de la tecnología, lo que contribuye de manera determinante a aumentar la eficiencia en el trabajo y garantizar la continuidad de las operaciones de la Institución.

Art. 2.- Ámbito.- Las Políticas de Tecnología de la Información y Comunicación serán aplicadas de manera obligatoria por las y los funcionarios, servidores y trabajadores que integran el IESS a nivel nacional, que utilicen el hardware, software y comunicaciones, para el cumplimiento de sus actividades diarias.

La Dirección Nacional de Tecnología de la Información será la encargada de administrar y ejecutar estas políticas a través de procedimientos, asimismo las políticas deben cumplirse a nivel nacional por las dependencias que tienen a su cargo el uso de recursos tecnológicos de forma desconcentrada.

La Subdirección Provincial de Apoyo a la Gestión Estratégica representará a la Dirección Nacional de Tecnología de la Información en las Direcciones Provinciales del IESS a nivel nacional y, será la responsable de velar por el cumplimiento de estas políticas.

Art. 3.- Recursos Tecnológicos.- Las Políticas de Tecnología de la Información regularán y estandarizarán el uso de los recursos informáticos que el IESS pone a disposición de todo el personal para desarrollar sus actividades y cumplir con la misión de la Institución.

Art. 4.- Términos.- Se definen los siguientes términos:

**TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.-** Equipo de cómputo personal y centralizado, software y dispositivos de impresión que serán utilizadas para almacenar, procesar, convertir, proteger, transferir y recuperar: información, datos, voz, imágenes y video.

**DOS.-** Denegación de Servicios, por sus siglas en Inglés (Denial of services).

**SOFTWARE (DE APLICACIÓN).-** Componentes lógicos (intangibles) de un computador. Programas de computadora que sirven para interactuar y controlar el sistema operativo, proporcionando control sobre el hardware y dando soporte a otros programas. Es una herramienta que realiza tareas de mantenimiento, soporte para la construcción y ejecución de programas.

**HARDWARE.-** Componente físico de un computador y dispositivos externos.

**INFORMACIÓN.-** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

**USUARIOS.-** Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

**SEGURIDAD INFORMÁTICA.-** Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

**INTEGRIDAD.-** Se refiere a la corrección y complementación de los datos en una base de datos.

**CONFIDENCIALIDAD.-** La información solo debe accesible únicamente a personal autorizado.

**DISPONIBILIDAD.-** Debe estar disponible cuando se necesita, es decir, accesible.

**IRREFUTABILIDAD (No repudio).-** El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que usuario no puede negar dicha acción.

ÁREA INFORMÁTICA.- Es el lugar donde se lleva a cabo el procesamiento de información (programación, análisis y diseño de sistemas de información, ingreso de datos, procesos de back-ups, etc.).AMENAZA.- Es un evento que pueden desencadenar en un incidente en el organismo, produciendo daños materiales o pérdidas inmateriales en sus activos.

IMPACTO.- Medir la consecuencia al materializarse una amenaza.

VULNERABILIDAD.- Posibilidad de ocurrencia que mediante una exploración se viole la seguridad del sistema.

ATAQUE.- Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

BACKUP.- Respaldo de información.

PASSWORDS.- Clave que se le asigna a los usuarios.

FILESYSTEMS.- Punto de montaje de sistemas UNIX.

RETENCIÓN.- Tiempo que vigencia de un respaldo.

DIRECCIÓN MAC.- Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.

DIRECCIÓN IP.- Es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, Tablet, Laptop, Smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

PC.- Computador personal.

CD.- Disco compacto para almacenar información.

URL.- Dirección web.

TI.- Tecnologías de la Información.

SHAREWARE.- Modalidad de distribución de software, en la que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso o con restricciones en las capacidades finales.

FREEWARE.- Tipo de software que se distribuye sin costo, disponible para su uso y por tiempo ilimitado.

QA.- Equipo de trabajo de Control de Calidad perteneciente a la Dirección Nacional de Tecnología.

## TÍTULO II

### POLÍTICA PARA EL USO ADECUADO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Art. 5.- Generales.- Los usuarios internos para el uso adecuado de los recursos tecnológicos tomarán en cuenta lo siguiente:

Para el hardware (equipos, impresoras, escáneres, servidores y demás recursos tecnológicos) de propiedad del IESS, de conformidad con el Reglamento Orgánico del Instituto Ecuatoriano de Seguridad Social, la Dirección Nacional de Tecnología de la Información es la única autorizada para realizar las actividades de soporte técnico, mantenimiento y cambios de configuración en el equipo de cómputo. En el caso de actividades de mantenimiento efectuadas por terceros, éstas serán previamente aprobadas por la Dirección Nacional de Tecnología de la Información.

La Subdirección Provincial de Apoyo a la Gestión Estratégica de cada Dirección Provincial o el área que haga sus veces, podrá efectuar labores de soporte técnico, con personal técnico de planta del IESS o, de ser el caso, a través de terceros, previa coordinación con la Dirección Nacional de Tecnología de la Información.

En caso de equipos de cómputo en esquema de arrendamiento, la empresa arrendadora es la única autorizada a realizar las labores de mantenimiento y cambio de hardware o en su caso autorizar dichas labores, previa coordinación con la Dirección Nacional de Tecnología de la Información o la Subdirección Provincial de Apoyo a la Gestión Estratégica en cada provincia.

El acceso al área de infraestructura informática es restringido y únicamente ingresará personal autorizado.

Se restringirá el acceso a los equipos tecnológicos, a aquellos usuarios que no cuenten con una autorización previa de su superior inmediato para laborar fuera de horario.

La información de trabajo se almacenará en los discos de red asignados por usuario, garantizando así la integridad de la información.

Las y los usuarios autorizados de los sistemas informáticos del IESS, no harán uso indebido, suministro, manejo, de la información institucional, datos en general y datos considerados como confidenciales.

Las bases de datos de la Institución estarán centralizadas en el Data Center de la Dirección Nacional de Tecnología de la Información, de existir bases de datos aisladas o no compatibles con la infraestructura tecnológica se implementarán proyectos de integración y/o migración de aplicativos y base de datos a cargo de la Dirección Nacional de Tecnología de la Información con participación de las unidades de negocio involucradas.

Los sistemas de información desarrollados internamente o adquiridos a terceros, estarán instalados en la infraestructura disponible en la Dirección Nacional de Tecnología de la Información (licenciamiento, software, código fuente, hardware.).

Previo al acceso a las bases de datos del IESS, se contará con la autorización de las Unidades de Negocio y la definición del tipo de acceso a otorgarse.

La entrega de información a entidades externas gubernamentales o privadas, contará con la autorización de las unidades de negocio dueñas de la información.

De no especificar permisos a direcciones web o a direcciones específicas, se proporcionará acceso solamente a la página web institucional y a su intranet.

La identidad de los usuarios externos y los derechos de acceso otorgados, se mantendrán en un repositorio central, en un documento que contenga al menos los siguientes campos como: nombres y apellidos, número de cédula de ciudadanía/identidad, empresa o entidad en la que labora, nombre del proyecto, nombre del responsable del proyecto, fecha de solicitud de los permisos, fecha de expiración de los permisos, sitios a los que se otorgó el acceso, dirección IP de la máquina desde donde se realiza el acceso, dirección MAC de la máquina desde donde se realiza el acceso, nombre de la persona que autoriza el acceso y de la persona que otorga el acceso, notas.

Se prohíbe a los usuarios utilizar los permisos otorgados para fines distintos a los especificados en la solicitud de acceso, así como también se prohíbe el intercambio de direcciones IP con otros usuarios que no consten en la solicitud.

En caso de que el usuario tenga la sospecha que sus accesos han sido comprometidos, solicitará inmediatamente su bloqueo a la Dirección Nacional de Tecnología de la Información o a la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel provincial.

Para el caso de conexiones inalámbricas, por defecto se otorgará un acceso a la red pública de la Institución. Si se especifican accesos puntuales, se otorgará acceso a una red específica de acuerdo a sus necesidades.

Se mantendrá un inventario actualizado de los recursos tecnológicos.

Todos los computadores de las unidades administrativas y médicas del IESS a nivel nacional, se sujetarán a la versión del software antivirus institucional, que determine la Dirección Nacional de Tecnología de la Información. Este software tendrá activada la protección en tiempo real al sistema operativo y mantendrá instalada la última definición de virus o una que haya estado vigente en los últimos 15 días. La actualización de las definiciones de antivirus se realizará de manera automática. Si por alguna razón no se dispone del servicio de actualización automática, se las instalará manualmente, si fuera el caso.

Bajo ninguna circunstancia las y los funcionarios/as, servidores/as y trabajadores/as de la Institución, podrán utilizar los recursos informáticos para realizar actividades prohibidas por las políticas establecidas o por las disposiciones jurídicas nacionales o internacionales.

**Art. 6.- Hardware.-** El hardware de propiedad del IESS o arrendado, se utilizará únicamente para actividades relacionadas con los objetivos y metas de la Institución, para lo cual se observará lo siguiente:

Para el correcto funcionamiento del hardware se realizará mantenimiento preventivo, de acuerdo al plan de mantenimiento preventivo del equipo de cómputo anual, elaborado por los técnicos informáticos de cada dependencia, mismo que deberá ser notificado al titular de la Dirección Nacional de Tecnología de la Información a principio de cada ejercicio.

La Dirección Nacional de Adquisiciones, Bienes y Servicios en coordinación con la Dirección Nacional de Tecnología de la Información es la responsable de la asignación y distribución del hardware institucional. A nivel provincial serán las Subdirecciones Provinciales de Apoyo a la Gestión Estratégica y de Servicios Corporativos, o las áreas que hagan sus veces.

La adquisición de bienes tecnológicos y la contratación de servicios de soporte técnico y/o mantenimiento se llevarán a cabo de acuerdo con los lineamientos, especificaciones técnicas que emita la Dirección Nacional de Tecnología de la Información a nivel nacional, basándose en la necesidad institucional y en la normativa vigente sobre la materia.

Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa al hardware del IESS, se notificará de inmediato a la Dirección Nacional de Adquisiciones, Bienes y Servicios, a nivel provincial a la Subdirección Provincial de Apoyo a la Gestión Estratégica o, al área que haga sus veces.

Solamente el personal del IESS autorizado por la Dirección Nacional de Tecnología de la Información o Subdirección Provincial de Apoyo a la Gestión Estratégica en las provincias, está facultado para abrir los gabinetes de las computadoras personales o de cualquier otro equipo de cómputo propiedad institucional, que NO cuenten con la garantía técnica vigente. Para los equipos cuya garantía técnica aún se encuentre vigente, lo efectuará únicamente el personal técnico calificado de la Contratista, previa coordinación con la o el Administrador de Contrato designado. Para los equipos de cómputo en esquema de arrendamiento, la empresa arrendadora es la única autorizada para abrir los gabinetes de dichos equipos o en su caso consentirá la apertura de ellos, previa coordinación con la o el Administrador de Contrato del IESS.

**Art. 7.- Centro de Cómputo.-** En el Centro de Cómputo del IESS se alojarán los servidores y equipos de comunicaciones necesarias para la operación de las actividades informáticas de la Institución y se observará lo siguiente:

El acceso a los centros de cómputo institucionales es restringido y sólo personal autorizado por la Dirección Nacional de Tecnología de la Información o la máxima autoridad de la dependencia en donde se encuentran ubicados, puede tener acceso a él.

El acceso a los servidores de los centros de cómputo institucionales, ya sea usando la consola de administración local o una consola de administración remota es restringido al personal autorizado por la Dirección Nacional de Tecnología de la Información o la máxima autoridad de la dependencia en donde se encuentran ubicados. El intento de conexión por alguna persona no autorizada a cualquier consola de administración de los servidores se considera una violación de las políticas de seguridad.

Art. 8.- Propiedad de la información.- Las y los usuarios de cualquier equipo de cómputo del IESS deben estar informados y conocer que los datos que ellos crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico, durante el desarrollo normal de sus actividades laborales, son de propiedad y responsabilidad del IESS, para lo cual se respetará lo siguiente:

Los derechos patrimoniales de un programa de computación, hojas de cálculo, archivos de Word, macros, etc., y su documentación, creados por uno o varios empleados en el ejercicio de sus actividades laborales corresponden al IESS.

Los respaldos que contengan información del IESS y que fueron realizados o solicitados por el usuario del equipo de cómputo, se tendrán exclusivamente bajo resguardo, de biendo entregarlos al jefe inmediato al finalizar su relación laboral con la institución, mediante la respectiva acta de entrega recepción.

Art. 9.- Usos inadecuados.- Las siguientes actividades están prohibidas:

Violar los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia de uso adecuada adquirida por el IESS (Políticas de Uso de Software).

Difundir información identificada como confidencial a través de medios que involucren el uso de la Tecnología de Información.

Introducir software malicioso en la red o en los servidores (virus, gusanos, troyanos, ráfagas de correo electrónico no solicitado, etc.).

Utilizar la infraestructura de tecnología de información del IESS para conseguir o transmitir material con ánimo de lucro.

Utilizar el sistema de comunicaciones del IESS con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.

Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios del IESS.

Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.

Monitorear puertos o realizar análisis del tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. El personal de la Dirección Nacional de Tecnología de la Información, responsable de la Seguridad Informática puede realizar estas actividades siempre y cuando cuente con la aprobación por parte del Director.

Burlar mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

Interferir o negar el servicio a usuarios autorizados con el propósito de lesionar la prestación o, deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet, Intranet).

Usar comandos o programas para el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet, Intranet).

Instalar cualquier tipo de software en los equipos de cómputo del IESS sin la previa autorización de la Dirección Nacional de Tecnología de la Información o la Subdirección Provincial de Apoyo a la Gestión Estratégica.

Modificar la configuración del software antivirus, firewall personales o políticas de seguridad en general implantadas en los equipos de cómputo del IESS sin consultar previamente con la Dirección Nacional de Tecnología de la Información o la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel provincial, la que analizará la viabilidad de los cambios solicitados.

Queda estrictamente prohibido compartir un repositorio de información con derecho a todos. El área de informática puede cambiar permisos de recursos compartidos por los usuarios si detecta que éstos no cumplen con las mejores prácticas definidas.

Reproducir música de cualquier formato que no esté ubicada en el disco duro de la PC del usuario o en CD. No se permite la reproducción de archivos de música si éstos están ubicados en recursos compartidos de la red privada del IESS o en cualquier URL de Internet (aplicable para los usuarios que hacen uso del servicio de Internet).

Art. 10.- Excepción.- Para propósitos de mantenimiento de la red y de seguridad, por excepción el personal debidamente autorizado, podrá estar exento de seguir algunas de las restricciones anteriores, debido a las responsabilidades bajo su cargo o a eventos programados. Estos privilegios de accesos deberán ser solicitados a la Dirección Nacional de Tecnología de la Información anexando la justificación respectiva, vía correo electrónico y/o de manera escrita.

### TÍTULO III POLÍTICA DE CONTRASEÑAS

Art. 11.- Generales.- El cumplimiento de la política de contraseñas por parte de las y los usuarios internos (funcionarios, servidores y trabajadores) del IESS, es extremadamente importante ya que constituyen la primera línea de defensa para garantizar que el acceso a los aplicativos informáticos sólo sea ejecutado por personal autorizado. Tanto equipos, sistemas y datos utilizan mecanismos de contraseñas para controlar el acceso, como al inicio de sesión en la computadora, ingreso a la red institucional, para utilizar sistemas internos y externos, etc. No existe ninguna tecnología que pueda prevenir el acceso no autorizado a la información si un usuario viola esta política.

Art. 12.- Administración.- Se acatará lo siguiente:

Todos los usuarios internos del IESS requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo que tiene asignado y servicios de red como correo electrónico, impresión, archivos compartidos, Intranet, Internet etc.

Todas las contraseñas son personales e intransferibles. Se prohíbe a los usuarios dar a conocer a terceras personas su contraseña, quien así lo hiciere debe considerar que sigue siendo el único responsable de las actividades que se realicen con su identificación de usuario y contraseña.

Todas las contraseñas del sistema (cuentas de administrador, cuentas de aplicaciones, etc.), se cambiarán con una periodicidad de al menos cada seis meses.

Todas las contraseñas del usuario (cuentas de usuario, cuentas de servicios web, etc.) se cambiarán al menos cada seis meses.

En caso de que el usuario sospeche que su contraseña ha sido comprometida deberá cambiar su contraseña o solicitar al responsable informático de cada dependencia.

En caso de olvido o bloqueo de su contraseña, el usuario deberá coordinar el restablecimiento de la misma con el responsable informático de cada dependencia.

Las contraseñas de los usuarios deben cumplir con ciertos requerimientos de seguridad los cuales definirá la Dirección Nacional de Tecnología de la Información con el objeto de evitar que los usuarios elijan contraseñas débiles. No se utilizarán contraseñas que resulten obvias, fáciles de adivinar o descubrir, o predecibles para un atacante: (el mismo identificador de usuario, palabras de diccionario, fechas o nombres de personas allegadas, secuencias de números repetidos o consecutivos).

Las contraseñas para acceso al correo electrónico deberán ser modificadas por el usuario la primera vez que acceda a su cuenta. 9. Las contraseñas de los sistemas internos contarán con contraseñas independientes de la utilizada para iniciar sesión en la red institucional. La administración funcional, incluyendo creación de usuarios y contraseñas de los sistemas internos serán ejecutadas por la Unidad de Negocio a cargo del mismo.

Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única.

Los derechos de acceso al correo electrónico, red institucional, servidores de archivos y otros servicios provistos por la Dirección Nacional de Tecnología de la Información, deben ser solicitados por el jefe de la dependencia del usuario y estarán alineados con necesidades de negocio definidas firmadas, con requerimientos de trabajo.

Los usuarios internos del IESS, deberán negar la opción de recordar contraseñas que se presentan en los navegadores a fin de evitar la autenticación automática de acceso a los sistemas informáticos que operan en la intranet como en el Internet.

Cuando un usuario se desvincule de la Institución o se le asigne un rol diferente para el que tiene permisos de acceso, el Jefe inmediato deberá notificar a la Dirección Nacional de Tecnología de la Información para suspender los usuarios de la red institucional, sistemas especializados, etc. De la misma manera, la Dirección Nacional de Gestión de Talento Humano, reportará de forma mensual a la Dirección Nacional de Tecnología de la Información el listado de traspasos, renunciaciones, y otros movimientos de personal con el fin de coordinar la cancelación de los derechos de acceso a servicios e información que dispongan dichos usuarios.

Las y los funcionarios, servidores y trabajadores, deberán suscribir un compromiso de responsabilidad en seguridad y uso de usuario y claves de acceso a la información de recursos tecnológicos administrados por la Dirección Nacional de Tecnología de la Información.

Art. 13.- Prohibiciones.- Las actividades que se detallan a continuación están prohibidas:

Revelar o compartir su contraseña de cualquier forma.

Escribir la contraseña o almacenarla en archivos sin que sean encriptados, comunicarla en el texto de mensajes de correo electrónico, o en cualquier otro medio de comunicación electrónica.

Comunicar las contraseñas en conversaciones telefónicas.

#### TÍTULO IV

#### POLÍTICA DE USO DE CORREO ELECTRÓNICO

Art. 14.- Lineamientos Generales.- El Correo Electrónico (email) es un recurso que la institución pone a disposición de las y los funcionarios, servidores y demás trabajadores del IESS, como una herramienta de comunicación, colaboración e intercambio de información oficial, se observará lo siguiente:

El acceso a estos recursos, estará condicionado a la aceptación de la presente Política de Uso.

El acceso a este servicio, se lo realiza por medio de la página web institucional (<https://correo.iess.gob.ec>), cliente de correo o a través de la intranet.

Las comunicaciones institucionales efectuadas por correo electrónico, solo podrán ser realizadas por las cuentas institucionales creadas en la Dirección Nacional de Tecnología de la Información.

Las cuentas de correo asignadas a los funcionarios y demás personal de cada área, deberán ser utilizadas sólo para actividades laborales que estén relacionadas con los propósitos y funciones institucionales.

Los buzones de correo electrónico, creados para las y los funcionarios, servidores y demás trabajadores del IESS, y toda la información contenida en los mismos, son de exclusiva propiedad de la Institución.

La Dirección Nacional de Tecnología de la Información se reserva el derecho para modificar las condiciones de uso establecidas cuando lo considere necesario. También podrá modificar o bloquear servicios relacionados al servicio de correo electrónico cuando sea necesario, por razones administrativas, de mantenimiento, por causas de fuerza mayor o por necesidad institucional.

La Dirección Nacional de Tecnología de la Información puede, en cualquier momento, cancelar o inhabilitar la cuenta de cualquier usuario sin previo aviso e incluso eliminar ésta por falta de uso, o bien; si considera que el usuario ha contravenido las reglas aquí mencionadas; en tales casos la Dirección Nacional de Tecnología de la Información no se hace responsable de la información ni de eventuales repercusiones por dicha cancelación o inhabilitación.

Art. 15.- Tipos de Cuentas.- Son:

Cuentas Personales: El personal del IESS, contará con una cuenta de correo, en el servidor de la Institución con capacidad de bandeja asignada, cuya dirección electrónica estará formada por la inicial del nombre, el apellido y la inicial del segundo apellido; salvo sus debidas excepciones ([xapellidox@iess.gob.ec](mailto:xapellidox@iess.gob.ec)).

Cuentas Temporales: Estas cuentas se crearán bajo propósitos específicos, que serán detallados en el campo de texto "Notas" al momento de crearla. Además se especificará el tiempo de validez, para que sea borrada una vez que ya no se la necesite. El formato para este tipo de cuenta será el siguiente: [proposito@iess.gob.ec](mailto:proposito@iess.gob.ec).

Cuentas Departamentales: Estas cuentas serán creadas, con el objetivo de comunicación a todos los miembros de una determinada dirección o lista de usuarios específica, el formato para este tipo de cuentas será el siguiente: [nombredirecciónlista@iess.gob.ec](mailto:nombredirecciónlista@iess.gob.ec).

Art. 16.- Responsabilidad.- Son:

Los servicios de correo electrónico serán administrados por la Dirección Nacional de Tecnología de la Información y será la responsable de velar por el correcto funcionamiento y operación de dichos servicios.

La Dirección Nacional de Gestión de Talento Humano deberá comunicar a la Dirección Nacional de Tecnología de la Información, sobre el personal que haya ingresado a laborar en la Institución, así como el personal que ha dejado de laborar, para la activación o desactivación de las cuentas de correo respectivas.

Los usuarios son los únicos responsables de todas las actividades realizadas, desde sus cuentas de acceso y buzones.

La información transmitida mediante el servicio de correo electrónico, es responsabilidad única y exclusiva de cada usuario. La Dirección Nacional de Tecnología de la Información no garantiza la veracidad, integridad o calidad del contenido de los mensajes enviados mediante este servicio.

La cuenta de correo es intransferible, por lo que la información correspondiente al inicio de sesión (usuario, contraseña) no debe proporcionarse a otras personas.

La información que se recibe de manera personal y confidencial por correo electrónico, no se puede reenviar a otra persona, sin la autorización del remitente.

Art. 17.- Gestión del buzón de correo.- El usuario deberá:

Velar por que la gestión de la información contenida en su cuenta de correo electrónico sea adecuada. Para lo cual debe revisar periódicamente sus bandejas de correo. En este sentido, se recomienda eliminar los mensajes que no deban conservarse y archivar el resto en la carpeta o subcarpeta apropiada.

Respalidar periódicamente la información contenida en su buzón de correo, para lo cual podrán solicitar soporte a la Dirección Nacional de Tecnología de la Información para la gestión de sus respaldos.

Resguardar la seguridad del buzón de correo, por lo cual deberán evitar la recepción de correo cuando se desconozca al remitente ya que en ocasiones este puede ser un mensaje con contenido potencialmente peligroso o un virus. La Dirección Nacional de Tecnología de la Información definirá el espacio y los servicios asignados para cada buzón de correo, de acuerdo a las necesidades institucionales.

Art. 18.- Uso Inaceptable.- Se considera como mal uso del correo electrónico las siguientes actividades:

Utilizar el correo electrónico para actividades comerciales ajenas a la institución.

Participar en la propagación de cadenas, esquemas piramidales y otros similares de envío con el correo institucional.

Enviar o reenviar mensajes con contenido difamatorio, ofensivo, racista u obsceno.

Enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.

Utilizar mecanismos y sistemas, que intenten ocultar o suplantar la identidad del emisor del correo electrónico.

Distribuir mensajes con contenidos definidos como inapropiados y/o lesivos que atenten contra la moral o las buenas costumbres. Son considerados contenidos inadecuados todo aquello que constituya complicidad con hechos delictivos, por ejemplo: apología del terrorismo, uso y/o distribución de programas piratas, todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento, lenguaje obsceno, virus o código hostil, en general.

La saturación y falta de mantenimiento del buzón electrónico por parte del usuario.

8. Apropiarse de alguna(s) cuenta(s) de correo diferente a la asignada a su persona.

9. Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado, "spam".

10. Dirigir a un usuario o al propio sistema de correo electrónico, mensajes que tengan el objetivo de paralizar el servicio por saturación de las líneas, de la capacidad del servidor de correo, o del espacio en disco del usuario.

## TÍTULO V

### POLÍTICA DE USO DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

Art. 19.- Generales.- Las y los usuarios internos cumplirán las siguientes recomendaciones:

Si no va a estar cerca de su estación de trabajo, bloquee el equipo o active el protector de pantalla. Se recomienda activar el bloqueo automático de la pantalla del computador para que cuando detecte inactividad no pueda ser utilizado, sin el ingreso de una contraseña.

Si va dejar su equipo encendido por periodos extendidos, el usuario deberá asegurarse de no dejar aplicaciones con su usuario activo en los sistemas de la Institución (Correo, Correspondencia, Aplicaciones de Administración de equipos y/o sistemas).

No modificar las configuraciones de dirección IP, DNS, hora, nombre de equipos y demás. En caso de requerir un cambio deberán notificar a los técnicos informáticos de su dependencia.

No modificar las configuraciones del equipo como fondo de pantalla y protector de pantalla, así como la configuración de software y hardware establecidos por la Dirección Nacional de Tecnología de la Información. Si en su equipo se han realizado modificaciones, debe notificar a los técnicos informáticos de su dependencia, para que se realice la re-configuración del mismo.

Está prohibido instalar aplicaciones, programas, utilitarios, que no sean aprobados por su línea de supervisión o que difieran del software base determinado por la Dirección Nacional de Tecnología de la Información, que no tengan licencias o que para su uso se deba romper la seguridad de licenciamiento del mismo.

En caso de funcionarios y/o servidores que tengan a su cargo computadores portátiles, estos deberán permanecer con el candado de seguridad durante todo el tiempo que el computador esté sin supervisión de dichos funcionarios y/o servidores. En caso de no disponer del candado, se deberá gestionar la adquisición del mismo a través de la Dirección a la que pertenece.

Para evitar pérdida de información, la o el usuario es responsable de respaldar su máquina periódicamente en medios magnéticos externos y verificar que los respaldos generados se encuentren disponibles, e íntegros para su uso de ser requerido.

No pueden moverse los equipos o reubicarlos sin permiso. En caso de que necesite movilizar un equipo fuera de la Institución se requiere autorización del Director de la Dependencia por escrito.

Está prohibido poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios y/o dañar o alterar los recursos informáticos.

Todo el personal que accede a los sistemas de información del IESS debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de uso.

Art. 20.- Compromiso de Confidencialidad.- Las y los servidores de las institución deberán firmar compromisos de confidencialidad y de no-divulgación de información de conformidad con lo dispuesto en la Constitución, las leyes y las necesidades de protección de información de la institución.

La Dirección Nacional de Gestión de Talento Humano será la encargada de controlar que los compromisos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción, gestionar la custodia de los compromisos firmados, en los expedientes, físicos o electrónicos, de cada funcionario y/o servidor, y controlar que la firma de los compromisos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios y/o servidores a la institución, sin excepción.

El personal de otras entidades públicas o privadas; deberán de igual manera suscribir el compromiso de confidencialidad previo a acceder a la información.

Art. 21.- Responsables de la seguridad.- Los responsables de la seguridad informática de los activos bajo su custodia serán la Dirección Nacional de Tecnología de la Información y la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial, y los responsables de la seguridad de la información serán las Unidades de Negocio hasta que se conforme y formalice la Unidad de Seguridad de la Información Institucional.

Art. 22.- Responsables de la Información.- Los responsables de la información se definen para asegurar adecuadamente la pertenencia, custodia y salvaguarda de los recursos, teniendo en cuenta una correcta distribución de funciones, que se diferencian entre:

Responsables Directos: Los Responsables Directos de la información son aquellos que por la naturaleza de su posición en la Institución conocen el tipo de información que se genera o comunica o ingresen en los diversos sistemas o aplicativos, pueden ser las Gerencias, Seguros Especializados, Direcciones Nacionales, Direcciones Provinciales, Jefaturas o aquellos designados por el Director General o su delegado para dicha actividad, son responsables de:

La clasificación directa de la información, de la organización y autorización del acceso a la información.

Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.

Monitoreo del uso de la información por parte de personal a su cargo

Asignar a los responsables del uso y manejo de la información.



Monitorear el uso de la información por parte de los Responsables Directos: Los Responsables Directos de la información por tener una relación directa en el manejo de la información serán responsables de monitorear el uso que le dé el personal a su cargo.

Responsables Secundarios: Los Responsables Secundarios de la información son aquellos que por la naturaleza de su cargo en la organización deben acceder, modificar o almacenar información. Son responsables de:

Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.

Custodios: Los Custodios de la información son aquellos que por la naturaleza de su cargo en la organización deben custodiar, respaldar o almacenar la información. Se convierten en custodios el personal que tenga acceso a bases de información. Entre sus responsabilidades constan:

El manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.

Mantener la disponibilidad e integridad de la información custodiada.

Mantener el acceso y permisos de acceso a la información custodiada.

Brindar soporte para evaluar e identificar la información para su clasificación.

Art. 23.- Clasificación de la Información.- Los Responsables Directos de la información deberán clasificar adecuadamente la información que manejan y deben asegurarse de que se respete el acceso a la misma por parte del personal a su cargo.

Los activos de información de la organización deben ser clasificados en una de las categorías definidas en el punto Niveles de Clasificación de Información de la Política de Seguridad de la Información.

Para clasificar la información dentro de uno de los niveles determinados o cambiar su categoría, se deben utilizar los criterios de clasificación de información mencionados en el punto Criterios de Clasificación de la Política de Seguridad de la Información.

La información será rotulada claramente con la clasificación que le sea otorgada. Esta rotulación debe ser clara y visible.

Toda la información generada en la organización y que no se le dé una clasificación específica, mantendrá el nivel de PRIVADA y deberá ser tratada como tal.

Criterios de Clasificación.- Son:

Valor: Es el principal criterio de clasificación, está basada en el valor del activo desde el punto de vista del negocio (valor propio del activo o producto del mismo).

Edad: Donde la clasificación de cierta información puede cambiar si el valor de la información se reduce con el tiempo.

Vida útil: Cuando la información se vuelve obsoleta en base a nueva información generada, cambios organizacionales u otros motivos.

Niveles de clasificación de la Información.- Son:

PÚBLICA: Es la información que por su naturaleza, puede ser visible o divulgada por el personal general de la organización, clientes o el público en general, sin riesgo de que su contenido pueda afectar en ningún sentido la integridad o economía de la organización.

Esta información puede ser, entre otras, publicaciones, anuncios de prensa o medios de comunicación, página web Institucional, etc.

Nivel de visualización y acceso: Este tipo de información debe obtener su clasificación por niveles autorizados.

SENSIBLE: Solo para uso interno, destinada al uso exclusivo por parte de los empleados de la organización en el desarrollo rutinario de los procesos de negocio. La divulgación y visibilidad de la misma dentro de la organización es segura.

Esta información debe ser mantenida dentro de la organización, pues su divulgación fuera de la misma puede tener un impacto leve o moderado a la privacidad del personal o causar un daño leve al negocio o la imagen de la organización. Esta información puede ser, entre otras, memorandos, avisos, comunicaciones, informativos, etc.

Nivel de visualización y acceso: Todo el personal de la organización, tiene acceso a esta información para su visualización. La modificación de la misma debe darse por el dueño de la información o por autorización escrita.

c) **RESTRINGIDA:** Información por su naturaleza es destinada solo para uso exclusivo de la organización. Esta información debe ser accedida y visualizada solo por el personal de la organización que cuente con la autorización y extenderse a las dependencias del IESS en general.

La divulgación o visualización no autorizada dentro de la organización o fuera de ella podría violar la privacidad de personas, reducir la ventaja competitiva de la organización o causar un daño significativo al negocio o la imagen de la organización.

Nivel de visualización y acceso: Departamentos, Áreas, Seguros o personas con autorización en base a la tabla de autorizaciones. La autorización debe ser explícita para visualización y/o para modificación.

d) **CONFIDENCIAL:** Es la información considerada como sensible y está destinada a uso solamente interno y por parte del personal específico que debe tener permisos y autorización para su visualización y/o manejo. La divulgación o visualización no autorizada causaría violación de la privacidad de las personas, reduciría la ventaja competitiva de la organización o produciría un daño grave o irreparable al negocio o la imagen de la organización.

Esta información puede ser, pero no limitarse a: Información de decisión de negocio, información secreta de Afiliados, Pensionistas, Empleadores (pines, contraseñas, historial, etc.),

Información de productos nuevos, información de negocios nuevos, etc.

Nivel de visualización y acceso: El acceso, modificación o visualización de la misma es permitido solo para los dueños de la información y para personal expresamente autorizado de forma escrita por los mismos.

Acceso a recursos y privilegios.- Los usuarios deberán tener el nivel necesario de privilegios para acceso a las aplicaciones, configuración de perfil o acceso a recursos para cumplir con las actividades de su cargo.

Gestión de Incidentes de Seguridad.- La gestión de incidentes de seguridad debe realizarse considerando los siguientes tres objetivos básicos:

Responder rápida y eficientemente.

Contener y reparar el daño causado por los incidentes.

Prevenir daños futuros.

Segregación Funcional.- Ningún proceso crítico debe ser conocido y ejecutado por una sola persona o que una misma persona tenga privilegios o accesos en diferentes fases de un proceso. Los distintos procesos del negocio deben ser claramente descritos, de tal forma que cualquier persona de la organización pueda ser capaz de asumir los roles y responsabilidades de otra.

Prevención y Entrenamiento Continuo.- Las políticas, reglamentos y normas referentes a Seguridad de Información deberán ser conocidos por todos los miembros de la organización y para el efecto, la Institución proveerá recursos necesarios para realizar capacitaciones a los diferentes usuarios de aplicaciones, personal técnico y demás personal de la institución en general.

Art. 24.- Almacenamiento.- La información obtenida de cualquiera de los servicios y que sea almacenada localmente en el equipo de cómputo del usuario y de propiedad institucional, no podrá ser distribuida o transmitida por la red institucional, o por otros medios de comunicación sin la autorización del inmediato superior

Es responsabilidad del usuario solicitar de forma periódica a la Dirección Nacional de Tecnología de la Información y/o informáticos de cada dependencia, el respaldo de dicha información.

La Dirección Nacional de Tecnología de la Información revisará el aprovechamiento óptimo de los recursos compartidos en la red para mantener la integridad y para asegurar que los usuarios utilicen los recursos de manera responsable.

Art. 25.- Transmisión de datos.- A fin de garantizar la integridad y confidencialidad de la información obtenida de los sistemas y aplicativos informáticos de la institución y en razón de que los dispositivos móviles, magnéticos y los soportes extraíbles generan vulnerabilidades como divulgación no autorizada de datos, robo de datos, datos dañados o comprometidos, por la facilidad de uso, alta movilidad y capacidad de almacenamiento, la Dirección Nacional de Tecnología de la Información y la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial, de forma programada y bajo pedido de las unidades administrativas, procederá a salvaguardar la información que mantiene la institución, proporcionando el mecanismo tecnológico de encriptación y des encriptación a las Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial. Y las unidades administrativas de forma programada y bajo pedido solicitarán a las Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial la encriptación y/o des encriptación de la información digital.

Art. 26.- Propiedad y Derechos de contenidos.- La información disponible en Internet, incluyendo textos, software, música, sonido, fotografía, video, gráficos u otro material contenido, está protegida por copyright, marcas registradas, patentes u otros derechos de propiedad y leyes. Sólo se permite el uso de este material bajo autorización expresa del autor.

El bajar, cargar, archivar, copiar, imprimir o enviar cualquier material debe ser realizado solamente bajo la autorización del autor.

Los usuarios no deben descargar ni instalar ningún tipo de software comercial, shareware o freeware en las unidades de disco o en cualquier disco, sin la autorización de los técnicos informáticos de cada dependencia.

Art. 27.- Conducta del Usuario Interno.- El Usuario Interno observará lo siguiente:

El usuario es el único responsable del contenido de transmisiones a través de cualquier servicio.

El usuario debe cumplir con las leyes de transmisión de datos técnicos de los países desde los cuales y hacia donde se envían los mensajes de correo electrónico.

El usuario no debe usar el servicio para propósitos ilegales o de entretenimiento.

El usuario debe cumplir con todas las regulaciones, políticas y procedimientos del uso del internet en la Institución.

La comunicación de los usuarios se debe conducir con respecto y consideración, evitando los abusos y el uso del lenguaje inapropiado.  
6. Se prohíbe el acceso a cualquier fuente de información cuyo contenido no se encuentre relacionado con las actividades del IESS o con las actividades del usuario.

Art 28.- Respaldo de la información tecnológica.- La Dirección Nacional de Tecnología de la Información y la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial, así como las unidades negocio, propietarias de la información como correspondan, determinarán el procedimiento de resguardo y contención de la información obtenida de los sistemas y/o aplicativos informáticos, considerando al menos los siguientes ítems:

Etiquetado de las copias de respaldo, contenido, periodicidad y retención.

Extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución.

Vida útil recomendada por el proveedor y la destrucción de estos medios magnéticos.

Guardado de los respaldos en un sitio lejano, a una distancia suficiente para evitar cualquier daño debido a desastres en la sede principal de la institución.

Grado apropiado de protección física y ambiental.

Eventos regulares de verificación y restauración de los medios de respaldo para garantizar sean confiables para uso de emergencia.

Protección de la información confidencial por medio de encriptación.

Generación de respaldos a discos y en el mismo sitio si se tiene suficientes recursos, ya que en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

## TÍTULO VI

### POLÍTICA DE USO DE SOFTWARE

Art. 29.- Administración.- La Dirección Nacional de Tecnologías de la Información será la única dependencia encargada, a nivel nacional, de la administración, instalación, soporte y funcionamiento del software instalado en el IESS. Dentro de las responsabilidades de la administración e instalación de software se describen las siguientes:

Mantener el resguardo de las licencias de uso de software de la Institución.

Mantener actualizado el catálogo de software de la Institución, desinstalar el software de las computadoras que no posean licencias o que no estén aprobadas por la Dirección Nacional de Tecnología de la Información.

Revisar periódicamente la vigencia de uso de las licencias adquiridas.

Generación de estándares de software institucional.

Establecer los procedimientos para el uso de software.

Realizar el análisis de necesidades y requerimientos de negocio, con la finalidad de planificar la adquisición o desarrollo de una solución de software.

Efectuar el registro de derechos de autor de los sistemas del IESS, desarrollados directamente o a través de terceros (contratados), en cumplimiento con las disposiciones de la Ley de Propiedad Intelectual.

Art. 30.- Uso/Instalación de Software.- Para el uso e instalación de software se observará lo siguiente:

La Dirección Nacional de Tecnología de la Información es la única autorizada, así como responsable, de realizar la instalación de software y proporcionar soporte técnico del mismo en las computadoras de la Institución.

El software utilizado por la Institución, deberá ajustarse a las especificaciones técnicas y arquitectura de la plataforma tecnológica disponible en la Dirección Nacional de Tecnología de la Información. Se exceptuarán los casos debidamente justificados mediante informe técnico del área de desarrollo de software.

El software adquirido debe cumplir con los procesos formales de recepción, validación técnica y pruebas, previos a la aceptación técnica del producto.

Art. 31.- Restricciones.- Se prohíbe la instalación y/o uso del software en los siguientes casos:

Copias ilegales de cualquier sistema informático, software o programa.

Software descargado de Internet.

Software que no se haya identificado como institucional.

Instalaciones no autorizadas o que no hayan sido solicitadas a la Dirección Nacional de Tecnología de la Información.

Software adquirido para uso personal del usuario (sin fines institucionales).

Software de entretenimiento o que no tenga relación con las actividades institucionales.

Software sin licencia.

Art. 32.- Requerimientos de Software.- Todo usuario interno que requiera la instalación de un determinado software deberá solicitarlo a la Dirección Nacional de Tecnología de la Información de acuerdo al procedimiento y formatos que para el efecto se establezcan.

La Dirección Nacional de Tecnología de la Información determinará, de acuerdo a las características del software solicitado, si existe disponibilidad de licencias para atender la petición o, en su caso, si se cuenta con el software adecuado para atender a las necesidades del usuario.

En caso de ser necesaria la adquisición de nuevo software la Dirección Nacional de Tecnología de la Información será la encargada de remitir al usuario las especificaciones técnicas generales y específicos de dicho software. Para la continuación del trámite respectivo, el usuario será el encargado de realizar los estudios completos (incluye estudio de mercado) y demás documentación de sustento para

el procedimiento de contratación de conformidad con la Ley Orgánica del Sistema Nacional de Contratación Pública, su Reglamento General, Resoluciones del Servicio Nacional de Contratación Pública y del IESS.

## TÍTULO VII POLÍTICA DE DESARROLLO DE SOFTWARE

Art. 33.- Generales- Para el desarrollo de software se requiere:

Toda solicitud de desarrollo, evaluación o modificación de programas informáticos deberá empezar con el pedido formal a la Dirección Nacional de Tecnología de la Información, para su análisis y aprobación.

La unidad requirente será la responsable de contar con la siguiente documentación, previa al inicio del proceso de desarrollo:

Proceso oficializado y aceptado por la unidad requirente y la Dirección Nacional de Procesos.

Documentación del flujo de procesos, procedimientos y actividades.

Formularios relacionados con el proceso.

Reglas y excepciones de negocio.

Responsables de las áreas involucradas para el acompañamiento en el proceso de desarrollo.

Documentación adicional que se deba tomar en cuenta para el proceso de desarrollo de software.

Los desarrollos o modificaciones de software deben estar de acuerdo a la arquitectura de aplicaciones definida por la Dirección Nacional de Tecnología de la Información, y deben seguir estándares y buenas prácticas de la industria.

El ciclo de desarrollo de software debe contar con un proceso de aseguramiento de la calidad (QA), que garantice que el producto sea desarrollado cumpliendo con criterios de calidad. Para lo cual, la Dirección Nacional de Tecnología de la Información deberá realizar las pruebas necesarias para garantizar la seguridad, rendimiento y confiabilidad de los aplicativos.

La unidad requirente deberá validar que el software cumpla con las funcionalidades y requerimientos solicitados, previo a la liberación en ambiente de producción.

Todo software desarrollado debe garantizar el registro de pistas de auditoría, donde se evidencien los eventos realizados por un usuario dentro de una aplicación.

Art. 34.- Entorno de Trabajo.- La Dirección Nacional de Tecnología de la Información utilizará los siguientes ambientes para el proceso de desarrollo de software:

Desarrollo. Ambiente utilizado para la construcción de los productos de software. El ambiente es administrado por el área de desarrollo.

Pre producción (Pruebas). Establecido como un ambiente idéntico al de producción, utilizado para control de calidad y pruebas del sistema. El ambiente es administrado por el área de calidad.

Producción. Ambiente utilizado para la operación de los sistemas. El ambiente es administrado por el área de Operaciones y el área de Base de Datos.

La información almacenada en el ambiente de producción no debe ser utilizada, ni visible a los ambientes de pre producción y desarrollo, con el fin de precautelar la confidencialidad de los datos.

Art. 35.- De la implantación de un sistema en ambiente de producción.-

1. El área de desarrollo de software, conjuntamente con el área de QA y el área de operaciones, seguirán el procedimiento determinado y aprobado por la Dirección Nacional de Tecnología de la Información para la implantación o modificación de los sistemas que se encuentran en ambiente de producción.

2. La implantación o modificación de los sistemas desarrollados por la Dirección Nacional de Tecnología de la Información debe ser validada y aprobada formalmente por el área requirente, previamente a la liberación en el ambiente de producción.

## TÍTULO VIII POLÍTICA DE USO DE INTERNET E INTRANET

Art. 36.- Generales.- Los servicios de Internet e Intranet son recursos que la institución pone a disposición de las y los funcionarios, servidores y demás trabajadores del IESS, como una herramienta de consulta de información, investigación y acceso a los sistemas institucionales, facilitando la realización de las labores cotidianas, tomando en cuenta lo siguiente:

El acceso y uso de los servicios de Internet e Intranet está condicionado a la aceptación de las presentes políticas.

El uso del servicio de Internet e Intranet está limitado a la realización de actividades laborales que estén relacionadas con los propósitos y funciones institucionales.

El acceso a estos servicios debe ser solicitado a la Dirección Nacional de Tecnología de la Información, previa autorización del titular de la unidad administrativa o médica a la que pertenezca el usuario.

En caso de que la solicitud sea aprobada, se realizará la configuración necesaria en el equipo del usuario y le asignará un perfil de acceso con un nivel de navegación (acceso a sitios web) determinado, de acuerdo a las actividades que el usuario desempeña dentro de la Institución.

En caso de que el usuario requiera acceder a un sitio web restringido por el nivel de navegación otorgado, deberá solicitar a la Dirección Nacional de Tecnología de la Información la habilitación de dicho sitio, adjuntando las justificaciones necesarias.

En caso de que un usuario externo, ajeno a la Institución, requiera el acceso al servicio de Internet, se le asignará un perfil de acceso limitado, con navegación básica y a través de una conexión de red que no ponga en riesgo la seguridad de los equipos internos de la Institución.

El intercambio de información entre las dependencias administrativas y médicas del IESS se lo realizará a través de red local, Intranet o una conexión privada virtual.

Art. 37.- Responsabilidades.- Los servicios de enlaces de datos y de Internet e Intranet son administrados por el personal de la Dirección Nacional de Tecnología de la Información a través del área de Infraestructura. El proveedor del servicio enlace de datos y de Internet es responsable de garantizar la disponibilidad y los anchos de banda del enlace, de acuerdo a los acuerdos de nivel de servicio contratados, tomando en cuenta lo siguiente:

Los servicios de Internet contratados por las Unidades Administrativas y Médicas a nivel nacional, su uso y administración estarán de acuerdo a los lineamientos o especificaciones que marque la Dirección Nacional de Tecnología de la Información; la Subdirección Provincial de Apoyo a la Gestión Estratégica en las jurisdicciones provinciales solventarán los problemas técnicos y errores de recepción y envío y gestionarán su atención inmediata.

La Dirección Nacional de Tecnología de la Información es responsable de monitorear periódicamente el uso de Internet e Intranet del IESS, con la finalidad de vigilar el cumplimiento de las presentes políticas, manteniendo la confidencialidad de la información.

La información y mensajes que se envíen a través de Internet, serán de completa responsabilidad del usuario emisor. En ningún momento dichos mensajes podrán atentar contra la imagen y reputación de la Institución

El usuario será el único responsable por los sitios web visitados desde su perfil de acceso a Internet, por lo tanto, será también responsable de mantener en privado las credenciales de su cuenta de acceso a Internet.

Art. 38.- Prohibiciones.- Se prohíbe lo siguiente:

Utilizar el Internet como un medio para realizar cualquier actividad comercial o lucrativa de carácter individual o la participación y distribución de actividades o materiales que vayan en contra de la Ley.

Utilizar el Internet para propósitos que puedan influir negativamente en la imagen del IESS, de sus autoridades o funcionarios.

Realizar cualquier actividad que pueda comprometer la seguridad de los servidores y recursos informáticos de la Institución.

Accesos a sitios web que puedan ser percibidos como obscenos, que distribuyan, emitan o promuevan material pornográfico, material ofensivo o con humor inapropiado; que vaya en contra de la moral y buenas costumbres.

Acceso a sitios de juegos y actividades recreativas o de promoción de intereses personales tales como redes sociales, chat, encuestas, concursos, mensajes no solicitados, etc.

Transmitir amenazas, material indecente o de hostigamiento. Así como intimidar, insultar, difamar, ofender, acosar a otras personas o interferir en el trabajo de otros usuarios.

Distribuir por Internet de material que cause daños, como la piratería, el sabotaje, específicamente la distribución de software malicioso.

Descargar e instalar programas o archivos vía Internet. Únicamente se podrá llevar a cabo esta tarea en situaciones previamente convenidas con la Dirección Nacional de Tecnología de la información.

Congestionar, afectar, interferir o paralizar el uso del servicio.

La instalación o uso de programas P2P (este tipo de programas, utiliza una red común para comunicar entre si las computadoras de los usuarios, donde se encuentran los archivos a intercambiar), como por ejemplo: Ares, Torrent, Blubster, Computwin, E-Donkey, Emule, entre otros.

Descargar música, fotos, videos, u otro material que no esté relacionado con las actividades o propósitos laborales.

## TÍTULO IX SANCIONES

Art. 39.- Incumplimiento de las Políticas.- Ante el incumplimiento de las obligaciones contempladas en este instrumento, dependiendo de la gravedad de la infracción cometida, se iniciarán las respectivas acciones y procedimientos administrativos y jurisdiccionales, de conformidad a las normas que las regulan, a fin de que se determine la responsabilidad civil, administrativa y penal, a que haya lugar, en contra de las personas imputables. El Instituto Ecuatoriano de Seguridad Social podrá iniciar las acciones de oficio o a petición de parte, a través de los órganos competentes.

Además de las acciones y procedimientos que se ejerzan en contra de los sujetos responsables de la violación de este instrumento, el Director Nacional de Tecnología de la Información o quien haga sus veces en territorio, dependiendo de la gravedad del incumplimiento y luego de seguir el debido proceso de acuerdo a la normativa legal vigente, en especial a la Ley Orgánica de Servicio Público su reglamento de aplicación y más normativa conexas, calificará motivadamente la falta e impondrá las siguientes acciones:

Ante un incumplimiento leve de las Políticas, se notificará por escrito recordándole la vigencia de las Políticas al usuario responsable de la falta, así como se pondrá en conocimiento del Titular de la dependencia a la que pertenezca el usuario y a la Dirección Nacional de Gestión de Talento Humano para su seguimiento y control.

En el evento de presentarse un incumplimiento moderado en las Políticas, o una reincidencia en un incumplimiento leve, se notificará por escrito al Titular de la dependencia a la que pertenezca la o el servidor y a la Dirección Nacional de Gestión de Talento Humano, así como de considerarlo necesario se podrá disponer la suspensión temporal del servicio a la o el usuario responsable hasta que el Titular del área apruebe por escrito la restauración del servicio.

En caso de presentarse un incumplimiento grave de las Políticas, causará el retiro de los equipos, bienes, servicios y herramientas informáticas.

Sin perjuicio de lo expuesto, el Director Nacional de Tecnología de la Información o su delegado, remitirá el expediente al Director Nacional de Gestión de Talento Humano o quien haga sus veces en territorio para determinar o solicitar el ejercicio de la responsabilidad administrativa, civil o penal a que hubiere lugar, a través de las autoridades competentes.

## DISPOSICIONES GENERALES

PRIMERA.- El Director General del IESS estará facultado para aprobar los procedimientos y estándares específicos que se requieran para la aplicación de las presentes Políticas que regulan las actividades relacionadas con el uso de Tecnologías de la Información y Comunicaciones

SEGUNDA.- Encárguese al Director General del IESS, al Coordinador General de Gestión Estratégica, al Director Nacional de Tecnología de la Información, la aplicación, control, seguimiento, monitoreo de su cumplimiento y la difusión de las políticas que regulan las actividades relacionadas con el uso de Tecnologías de la Información contenidas en la presente Resolución, a través de la Dirección Nacional de Gestión Documental.

TERCERA.- La Dirección Nacional de Tecnología de la Información con el apoyo de la Dirección Nacional de Procesos, presentará a la Dirección General del IESS, en un término no mayor de ciento ochenta (180) días, los procedimientos para la aplicación de las políticas que regulan las actividades relacionadas con el uso de Tecnologías de la Información y Comunicaciones del IESS, contenidas en la presente Resolución.

CUARTA.- La Dirección Nacional de Tecnología de la Información se encargará de realizar los trámites necesarios para el registro e inscripción en el Instituto Ecuatoriano de Propiedad Intelectual, del software de propiedad del IESS presente y futuro, de conformidad con lo dispuesto en la Ley de Propiedad Intelectual y su Reglamento. La Dirección Nacional de Gestión Financiera otorgará los recursos económicos para el cumplimiento de dicho fin.

Disposición Final.- Esta resolución entrará en vigencia a partir de la presente fecha, sin perjuicio de su publicación en el Registro Oficial

COMUNÍQUESE.- Quito, Distrito Metropolitano, a los 28 días del mes de abril del 2016.

f.) Richard Espinosa Guzmán, B.A., Presidente, Consejo Directivo.

f.) Ing. Felipe Pezo Zúñiga, Representante Empleadores.

f.) Dr. Luis Clavijo Romero, Representante Asegurados

f.) Geovanna León Hinojosa, Directora General, Secretaria del Consejo Directivo.

Certifico.- Que la presente Resolución fue aprobada por el Consejo Directivo del Instituto Ecuatoriano de Seguridad Social en una discusión, en sesión celebrada el 28 de abril de 2016.

f.) Geovanna León Hinojosa, Directora General, Secretaria del Consejo Directivo.

Instituto Ecuatoriano de Seguridad Social.- Es fiel Copia del original.- Lo certifico.- f.) Abg. David García S., Prosecretario, Consejo Directivo.

Certificado que es fiel copia del Original.- f.) Ing. Patricio Prócel I.- Dirección Nacional de Gestión Documental del IESS.

### No. C.D. 524

#### EL CONSEJO DIRECTIVO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL

Considerando:

Que, el 11 de diciembre de 2012, en la ciudad de Tulcán – Ecuador, se suscribió el “Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador”;

Que, la Corte Constitucional declaró mediante Dictamen 030-13-DTI-CC de 5 de noviembre de 2013, que el “Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador”, mantiene conformidad con la Constitución de la República del Ecuador;

Que, el Pleno de la Asamblea Nacional en sesión de 20 de mayo de 2014, resolvió “APROBAR EL ACUERDO DE SEGURIDAD SOCIAL ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR”;

Que, el Econ. Rafael Correa, Presidente de la República del Ecuador, mediante Decreto Ejecutivo No. 345 de 4 de junio de 2014, ratificó el "Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador"; el cual fue publicado en el Suplemento del Registro Oficial No. 273 de 23 de junio de 2014;

Que, mediante Nota Diplomática Nro. S-GTAJI14-064881, de 9 de septiembre de 2014, el Ministerio de Relaciones Exteriores de Colombia informa que el Acuerdo de Seguridad Social suscrito entre Ecuador y Colombia entró en vigor el 1 de agosto de 2014.

Que, el numeral 3 del artículo 9 del Acuerdo de Seguridad Social suscrito entre Ecuador y Colombia, determina que: "Así mismo los Organismos de Enlace podrán completar y perfeccionar los procedimientos administrativos establecidos en este Acuerdo para lograr una mejor aplicación del mismo.";

Que, el Organismo de Enlace y de aplicación del Acuerdo de Seguridad Social entre las Repúblicas de Ecuador y Colombia, en el Ecuador es el Instituto Ecuatoriano de Seguridad Social de conformidad a lo establecido en la letra B) del artículo 5 del referido Acuerdo;

Que, es necesario sistematizar, difundir y aplicar a nivel nacional las disposiciones del "Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador";

Que, mediante Memorando No. IESS-DNAC-2016- 0456-M de 5 de mayo de 2016 y Memorando No. IESSDNAC- 2016-0542 de 23 de mayo de 2016, la Directora de Afiliación y Cobertura remite el proyecto de resolución enfatizando que el mismo contiene las disposiciones de aplicación interna del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador;

Que, mediante Memorando No. IESS-PG-2016-0782-M de 20 de mayo de 2016 el Procurador General señala que el proyecto deberá ser remitido al Consejo Directivo para su aprobación conforme lo estipula el ordenamiento jurídico, y;

En ejercicio de las funciones y atribuciones que le confiere el artículo 27, literales c) y f) de la Ley de Seguridad Social y el artículo 4 del Reglamento Orgánico Funcional del Instituto de Seguridad Social, el Consejo Directivo,

Resuelve:

**EXPEDIR LAS DISPOSICIONES DE APLICACIÓN  
INTERNA DEL ACUERDO DE SEGURIDAD  
SOCIAL ENTRE LA REPÚBLICA DE COLOMBIA  
Y LA REPÚBLICA DEL ECUADOR**

Artículo 1.- La Dirección del Sistema de Pensiones será la responsable de otorgar las prestaciones contributivas del Seguro General Obligatorio, en lo que se refiere al Seguro de Invalidez, Vejez y Muerte que incluye pensiones de supervivencia a viudas y huérfanos y el auxilio de funerales, con sujeción a las disposiciones del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador.

Artículo 2.- La Dirección Nacional de Afiliación y Cobertura, funcionará como Oficina de Enlace Nacional para la aplicación operativa del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador, cumpliendo entre otras las siguientes actividades:

Informará sobre la aplicación del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador y entregará los formularios requeridos según corresponda.

Receptará las solicitudes de prestaciones en los formularios acordados conjuntamente con la documentación requerida, debidamente verificados y certificados; y, las remitirá a los Organismos de Enlace de Colombia.

Receptará los formularios y la documentación enviada por los Organismos de Enlace Colombiano; y, remitirá la misma según corresponda a la Dirección General, Direcciones Provinciales o Direcciones de los Seguros Especializados.

Tramitará también las solicitudes de traslados o desplazamientos temporáneos de los afiliados ecuatorianos a la República de Colombia y de los afiliados colombianos a la República del Ecuador.

Notificará a quien corresponda, sobre las resoluciones e información de las prestaciones.

Informará a la Oficina de Enlace Colombiano y a los beneficiarios del Convenio sobre el estado de los trámites.

Certificará y remitirá a la Oficina de Enlace o a las Instituciones Competentes de Colombia, la documentación relacionada con la aplicación del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador.

Mantendrá un registro de los trámites al amparo del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador; debiendo mantener actualizado la base de datos estadísticos como Organismo de Enlace.

Artículo 3.- Las Direcciones Provinciales del IESS, funcionarán en coordinación con la Dirección Nacional de Afiliación y Cobertura, como Oficinas de Enlace Provinciales para la aplicación del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador, desarrollando en su jurisdicción provincial, actividades similares a las de la Oficina de Enlace Nacional.

Las Direcciones Provinciales remitirán la documentación recibida a la Dirección Nacional de Afiliación y Cobertura, para que proceda a emitir el acuerdo respectivo.

Artículo 4.- Las calificaciones de invalidez para aplicación del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador, las realizarán en el Ecuador las Comisiones Provinciales de Valuación de Incapacidades a cargo del Sistema de Pensiones.

**DISPOSICIONES GENERALES**

PRIMERA.- La Dirección General dispondrá a la Dirección del Sistema de Pensiones, a la Dirección Nacional de Tecnología de la Información, a la Dirección Nacional de Afiliación y Cobertura y a las Direcciones Provinciales, la ejecución oportuna y adecuada de la presente Resolución.

SEGUNDA.- Los formularios de implementación del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador con sujeción a lo que dispone el numeral 3 del artículo 9 del referido Acuerdo, son los que se anexan a la presente Resolución y que constan en el siguiente cuadro resumen:

FORMULARIO	DENOMINACIÓN	REFERENCIA ARTÍCULOS DEL ACUERDO
ECU/COL-01	Formulario de Períodos de Seguro Acreditados	Artículos 11, 16 y 21.
ECU/COL-02	Solicitud	Artículos 19, 20 y 21.
ECU/COL-03	Informe Médico Detallado	Artículos 21, 22 y 23.
ECU/COL-04	Certificado de Traslado Temporal	Artículos 14.
ECU/COL-05	Prórroga de Traslado Temporal	Artículo 14, apartado 1, literal b) y d) y Artículo 15, apartado 2.
ECU/COL-06	Ejercicio del Derecho de Opción	Artículo 14, apartado 1, literal i) y j).

TERCERA.- Las solicitudes de traslados o desplazamientos temporarios de los afiliados colombianos a la República del Ecuador y de los afiliados ecuatorianos a la República de Colombia, facultados en el artículo 14 del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador; serán resueltos por la Dirección Nacional de Afiliación y Cobertura.

CUARTA.- Las solicitudes de prórrogas de desplazamientos temporarios de los afiliados colombianos a la República del Ecuador y de los afiliados ecuatorianos a la República de Colombia, facultados en el artículo 14 del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador; serán resueltos por la Dirección General del IESS.

QUINTA.- La Dirección Nacional de Afiliación y Cobertura emitirá de ser el caso, el informe favorable, estableciendo el cumplimiento de la normativa vigente, incluyendo la verificación de que los solicitantes no se encuentren afiliados al IESS, previo a la autorización de prórroga de desplazamiento por parte de la Dirección General del IESS.

SEXTA.- Las solicitudes de prórrogas de desplazamientos se autorizarán con sujeción a las disposiciones establecidas en el Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador.

SÉPTIMA.- Una vez concluido, según el caso, el período establecido por el Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador o el período de prórroga debidamente autorizado, los trabajadores afiliados a la seguridad social de la otra Parte Contratante comprendido en una u otra situación, de continuar laborando en el Ecuador, deberán afiliarse al IESS, con sujeción a las disposiciones de la Constitución de la República, Ley de Seguridad Social; y, demás normativa legal vigente.

OCTAVA.- Las solicitudes de prórroga de desplazamiento se recibirán en el IESS, siempre y cuando su presentación se realice dentro de los plazos determinados en Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador.

NOVENA.- Las Direcciones Provinciales dentro de su jurisdicción, verificarán y dispondrán las acciones correspondientes para que los trabajadores afiliados a la seguridad social de la otra Parte Contratante que laboren en el país por el tiempo establecido en Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador, sin haber obtenido autorización de prórroga, se encuentren afiliados al IESS.

DÉCIMA.- La Dirección del Sistema de Pensiones y la Dirección Nacional de Afiliación y Cobertura remitirán trimestralmente a la Dirección Actuarial la información estadística sobre la aplicación del Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador.

La Dirección Nacional de Afiliación y Cobertura elaborará el informe estadístico anual que la Dirección General remitirá a los Organismos de Enlace correspondientes.

#### DISPOSICIONES TRANSITORIAS

PRIMERA.- La Dirección de Comunicación Social del IESS, difundirá a nivel nacional los beneficios a los cuales pueden acogerse los ciudadanos amparados por el Acuerdo de Seguridad Social entre la República de Colombia y la República del Ecuador, así como los requerimientos para acceder a los mismos.

SEGUNDA.- La Dirección Nacional de Tecnología de la Información implementará los procesos informáticos requeridos para la aplicación de la presente Resolución.

#### DISPOSICIÓN FINAL

Esta Resolución entrará en vigencia a partir de la fecha de su aprobación, sin perjuicio de su publicación en el Registro Oficial.

COMUNÍQUESE.- Quito, Distrito Metropolitano, a los 23 días del mes de mayo de 2016.



f.) Richard Espinosa Guzmán, B.A., Presidente, Consejo Directivo.

f.) Ing. Felipe Pezo Zúñiga, Representante Empleadores.

f.) Dr. Luis Clavijo Romero, Representante Asegurados.

f.) Abg. Geovanna León Hinojosa, Directora General IESS, Secretaria del Consejo Directivo.

Certifico.- Que la presente Resolución fue aprobada por el Consejo Directivo del IESS en sesión de lunes 23 de mayo de 2016.

f.) Abg. Geovanna León Hinojosa, Directora General IESS Secretaria del Consejo Directivo.

Instituto Ecuatoriano de Seguridad Social.- Es fiel Copia del original.- Lo certifico.- f.) Abg. David García S., Prosecretario, Consejo Directivo.

Certificado que es fiel copia del Original.- f.) Ing. Patricio Prócel I.- Dirección Nacional de Gestión Documental del IESS.

ACUERDO ADMINISTRATIVO DE  
SEGURIDAD SOCIAL ENTRE ECUADOR Y COLOMBIA

ECU/COL-01

FORMULARIO DE PERÍODOS DE SEGURO ACREDITADOS

Artículos 11, 16 y 21 del Acuerdo Administrativo.

El presente formulario será cumplimentado en la parte que le afecte, por la Entidad Gestora ante la cual se presente la solicitud y remitido, en duplicado ejemplar, a la Institución de enlace competente de la otra Parte donde el asegurado alega haber cotizado. Ésta devolverá un ejemplar del formulario en el que se certifiquen los períodos efectivos de cotización de acuerdo con su legislación.

Nº de referencia en Ecuador: .....

Fecha de presentación de la solicitud de informe: DD..... MM..... AAA.....

**1** Entidad Gestora destinataria competente.

1.1. Denominación.....  
1.2. Dirección (1).....  
1.3. Correo electrónico.....

**2** Datos relativos al asegurado:

2.1. Primer apellido	Segundo apellido (2)	Nombre
.....	.....	.....
2.2. Apellido de nacimiento (3)	Nombre del padre	Nombre de la madre
.....	.....	.....
2.3. Fecha de nacimiento	Lugar de nacimiento	
Día.....mes.....año.....	.....	
2.4. Sexo: M..... F.....	Nacionalidad (4)	.....
2.5. Estado civil: (5)		.....
Fecha de matrimonio o de la unión marital de hecho: .....		
Fecha del divorcio o de separación si es unión de hecho: .....		
2.6. DNI/NIE. (6).....		
Tipo de documento (C.C., C.E, T.I.R.C .o NUIP) (6) .....	No. de documento.....	
<b>(Por favor anexas fotocopia del documento expedido en Colombia)</b>		
2.7. Domicilio habitual (1)		.....
2.8. Número de afiliación a la Seguridad Social (7)	En Ecuador: .....	
	En Colombia: .....	
2.9. Correo electrónico.....		



**ACUERDO ADMINISTRATIVO DE  
SEGURIDAD SOCIAL ENTRE ECUADOR Y COLOMBIA**

ECU/COL-01

*FORMULARIO DE PERÍODOS DE SEGURO ACREDITADOS*

4	Datos sobre los periodos de seguro.			
4.1	Periodos de seguro acreditados en Ecuador.			
Desde <i>DD/MM/AAA</i>	Hasta <i>DD/MM/AAA</i>	Voluntarios (días)	Obligatorios (días)	Equivalentes (días)
TOTAL:				

**ACUERDO ADMINISTRATIVO DE  
SEGURIDAD SOCIAL ENTRE ECUADOR Y COLOMBIA**

ECU/COL-01

*FORMULARIO DE PERÍODOS DE SEGURO ACREDITADOS*

4.2 Períodos de seguro acreditados en Colombia.

Entidad colombiana donde realizó aportes para pensión	Desde <i>DD/MM/AAA</i>	Hasta <i>DD/MM/AAA</i>	Obligatorios (días)	Equivalentes (días)
<b>TOTAL:</b>				

ACUERDO ADMINISTRATIVO DE  
SEGURIDAD SOCIAL ENTRE ECUADOR Y COLOMBIA

ECU/COL-01

*FORMULARIO DE PERÍODOS DE SEGURO ACREDITADOS*

**Institución de Ecuador.**

Denominación:

.....

Dirección: (1)

.....

.....

Sello:

Fecha:.....

Firma

**Institución de Colombia**

Denominación:

.....

Dirección:

.....

.....

Sello:

Fecha:.....

Firma.....

**ACUERDO ADMINISTRATIVO DE  
SEGURIDAD SOCIAL ENTRE ECUADOR Y COLOMBIA**

**ECU/COL-01**

**FORMULARIO DE PERÍODOS DE SEGURO ACREDITADOS**

**INSTRUCCIONES.**

**El presente formulario se cumplimentará a máquina o en caracteres de imprenta, utilizando únicamente las líneas de puntos.**

**NOTAS.**

1. Para Ecuador, indicar: la dirección del Instituto Ecuatoriano de Seguridad Social.
2. Para nacionales ecuatorianos es imprescindible el segundo apellido.
3. Para las mujeres casadas.
4. En caso de cambio de nacionalidad, indicar a continuación cuándo se produjo dicho cambio.
5. Indicar según los casos: soltero/a, casado/a, viudo/a o divorciado/a, unión marital de hecho
6. Para los nacionales colombianos residentes en Ecuador indicar el número de identidad extranjera (NIE). Para los nacionales colombianos : Cédula de Ciudadanía ( CC ), Cédula de Extranjería ( CE, ) Tarjeta de Identidad (T.I.) Registro Civil o Número Único de Identificación (R.C o NUIP)
7. En Ecuador: Número de cédula de identidad.  
En Colombia Tipo y Número de identificación
8. En Colombia deberá acreditar tiempos servidos en iguales condiciones. La legislación colombiana considera actividades de alto riesgo:
  1. Trabajos en minería que impliquen prestar el servicio en socavones o en subterráneos.
  2. Trabajos que impliquen la exposición a altas temperaturas, por encima de los valores límites permisibles, determinados por las normas técnicas de salud ocupacional.
  3. Trabajos con exposición a radiaciones ionizantes.
  4. Trabajos con exposición a sustancias comprobadamente cancerígenas.
  5. En la Unidad Administrativa Especial de Aeronáutica Civil o la entidad que haga sus veces, la actividad de los técnicos aeronáuticos con funciones de controladores de tránsito aéreo, con licencia expedida o reconocida por la Oficina de Registro de la Unidad Administrativa Especial de Aeronáutica Civil, de conformidad con las normas vigentes.
  6. En los Cuerpos de Bomberos, la actividad relacionada con la función específica de actuar en operaciones de extinción de incendios.
  7. En el Instituto Nacional Penitenciario y Carcelario, Inpec, la actividad del personal dedicado a la custodia y vigilancia de los internos en los centros de reclusión carcelaria, durante el tiempo en el que ejecuten dicha labor. Así mismo, el personal que labore en las actividades antes señaladas en otros establecimientos carcelarios, con excepción de aquellos administrados por la fuerza

ACUERDO ADMINISTRATIVO DE SEGURIDAD SOCIAL ENTRE ECUADOR Y COLOMBIA  
SOLICITUD

VEJEZ       INVALIDEZ       SUPERVIVENCIA

El presente formulario será diligenciado por la Entidad Gestora ante la cual se presente la solicitud de acuerdo con los documentos allegados por el solicitante, y será remitido al Organismo de Enlace competente de la otra parte, donde el asegurado alega haber cotizado.

Artículos 19, 20 y 21 del Acuerdo Administrativo.

Fecha de presentación: Día..... Mes..... Año.....      Nº de referencia en Ecuador:.....

<b>1</b>	<b>Destinatario:</b>
1.1.	Denominación .....
1.2.	Dirección (1) .....
1.3.	Correo Electrónico .....

<b>2</b>	<b>Datos relativos al asegurado o causante fallecido:</b>
2.1.	Primer apellido      Segundo apellido      Nombre
2.2.	Apellidos de nacimiento (2)      Nombre del padre      Nombre de la madre
2.3.	Fecha de nacimiento    Día ..... Mes ..... Año .....      Lugar de nacimiento .....
2.4.	Sexo: <input type="checkbox"/> F <input type="checkbox"/> M      Nacionalidad (3) .....
2.5.	Estado civil: (4) <input type="checkbox"/> Soltero <input type="checkbox"/> Casado <input type="checkbox"/> Divorciado <input type="checkbox"/> Unión libre <input type="checkbox"/> Viudo
	Fecha de matrimonio o de la unión marital de hecho:      Día ..... Mes ..... Año .....
	Fecha del divorcio, o de la separación si es unión libre:      Día ..... Mes ..... Año .....
2.6.	DNI/NIE (5) .....
	Tipo de documento (C.C., C.E., T.I, R.C o NUIP) (6) ..... No. de documento .....
	(Por favor anexas fotocopia del documento expedido en Colombia, en el caso de corresponder)
2.7.	Domicilio habitual (1) .....
2.8.	Número de afiliación a la Seguridad Social (6)
	En Ecuador: .....
	En Colombia: .....
2.9.	Fecha de fallecimiento. Día..... mes..... año.....      Lugar de fallecimiento.....
2.10.	Causa de fallecimiento.....
2.11.	El asegurado (7)
	<input type="checkbox"/> Ejerce <input type="checkbox"/> una actividad asalariada
	<input type="checkbox"/> No ejerce <input type="checkbox"/> una actividad independiente
2.12.	Fecha en la que ha cesado o cesará su actividad laboral . Día ..... Mes ..... Año .....
2.13.	¿Se encuentra afiliado a Salud a una Entidad Promotora de Salud (EPS) en Colombia? (10) <input type="checkbox"/> SI <input type="checkbox"/> NO. (11)
	Cuál? .....
	Cotizante .....
	Beneficiario(s) .....
2.14.	¿Se considera el interesado incapacitado para el trabajo? (8) <input type="checkbox"/> SI <input type="checkbox"/> NO
2.15.	El asegurado (7)
	<input type="checkbox"/> percibe <input type="checkbox"/> no percibe una pensión o renta
	<input type="checkbox"/> ha sido <input type="checkbox"/> no ha sido titular de una pensión o renta
2.16.	En caso afirmativo :
	Institución que concedió la pensión .....
	Importe mensual de la pensión.....
	Número de pagas al año .....
2.17.	Correo electrónico: .....







7.2 En Colombia (13)					
Nombre de la empresa	Dirección, Ciudad, Departamento y Municipio	Nombre de la Administradora de Pensiones	Desde	Hasta	Naturaleza de la actividad

8 Datos sobre los periodos de seguro.					
8.1 Períodos de seguro acreditados en Ecuador.					
Entidad ecuatoriana donde realizó aportes para pensión	Desde <i>DD/MM/AAA</i>	Hasta <i>DD/MM/AAA</i>	Voluntarios (días)	Obligatorios (días)	Equivalentes (días)



**10. Determinación de la prestación a cargo de Ecuador.**

Clase de la prestación.	Fecha de efectos.	Importe anual.	Número de pagas al año.
..... ...	DD.....MM.....AAA.....	.....	.....

10.1. (7)     Por totalización                                   Sin totalización

En caso de liquidación por totalización, número total de días tenidos en cuenta:.....

Coficiente prorrata: .....

10.2. Motivos por los cuales no se abona ninguna prestación.

Sello:

Fecha: .....

.....  
Firma del Funcionario

**10.3. Entidad Gestora de Ecuador.**

Denominación:

Dirección: (1) .....

Teléfono: .....

Correo electrónico: .....

Sello:

Fecha: .....

.....  
Firma



**INSTRUCCIONES.**

El presente formulario se diligenciará a máquina o en caracteres de imprenta, utilizando únicamente las líneas de puntos.

**NOTAS.**

- 1- Para Colombia, indicar: Dirección, Ciudad, Municipio y Departamento.
2. Para las mujeres casadas, apellido de Soltera.
3. En caso de cambio de nacionalidad, indicar a continuación cuándo se produjo dicho cambio.
4. Indicar según los casos: soltero/a, casado/a, viudo/a o divorciado/a, unión libre.
5. Para los nacionales colombianos residentes en Ecuador indicar el número de identidad extranjera (NIE). Para los nacionales colombianos: Cédula de Ciudadanía ( CC ), Cédula de Extranjería ( CE,) Tarjeta de Identidad (T.I.) Registro Civil o Número Único de Identificación (R.C o NUIP)
6. En Colombia: Tipo y Número de identificación
7. Marcar lo que proceda.
8. Marcar lo que proceda, en caso de incapacidad, adjuntar informe médico.
9. Hijos, padres u otros derechohabientes.
10. Indicar SI o NO.
11. Si la persona a la cual se le ha reconocido una pensión en Colombia reside en el exterior y no se encuentra afiliado a ninguna EPS en Colombia se descontará el 1% para el fondo de Solidaridad del Sistema Integral de Seguridad Social en Colombia. Si reside en Colombia deberá aportar el 12% de la mesada pensional y será afiliado obligatorio al Sistema General de Seguridad Social en Salud de Colombia.
12. Si va a cobrar en el exterior, deberá acreditar certificación Bancaria que contenga los datos exigidos en este ítem, adicionalmente el pensionado debe diligenciar la declaración de cambio.
13. Si la persona pide régimen de alto riesgo en Colombia deberá acreditar tiempo de servicio en iguales condiciones en Ecuador Art. 24 del Acuerdo.
14. En los casos de solicitudes de prestaciones de SOBREVIVENCIA por invalidez, el beneficiario deberá presentar el formulario de "INFORME MEDICO DETALLADO".
15. Se diligencia en los casos de solicitud de pensiones de sobrevivientes por hijos menores de edad o con discapacidad, donde se requiere estar representado por un tutor, curador o representante legal.

ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR

**INFORME MÉDICO DETALLADO.**

Artículo 21, 22 y 23 del Acuerdo Administrativo

<b>1.1 Institución a la que se dirige el informe.</b>	
1.1.1 Denominación y/o nombre	.....
1.1.2 Dirección (1)	.....
1.1.3 Referencia:	.....

**1.2 Datos del examinado**

1.2.1	Apellido(s) (2)		.....	
1.2.2	Nombre	Apellido(s) anteriores (3)	Lugar de nacimiento (4)	
1.2.3	Fecha de nacimiento	Sexo: F <input type="checkbox"/> M <input type="checkbox"/>	Nacionalidad	Numero de Identificación ..... (5)
1.2.4	Dirección (1)			
1.2.5	Último empleo			
1.2.6	Niveles de escolaridad			
1.2.7	Correo electrónico			
1.2.8	<input type="checkbox"/> Número de afiliación			
1.2.9	<input type="checkbox"/> Número de Resolución de pensión			
1.2.10	Fecha de presentación de la solicitud de pensión			
1.2.10	Fecha de presentación de la solicitud de revisión de pensión o por Patología progresiva.			
1.2.11	Patología degenerativa / progresiva			
1.2.12	Patología Congénita			
1.2.13	Patología de alto costo / catastrófica			

**1.3 Informe expedido por el médico laboral examinador**

1.3.1	Apellido(s)	Nombre
1.3.2	Dirección (1)	
1.3.3	Nombre del Inspector de la D. Prov. de y/o médico laboral de la Institución Calificadora	

**1.4 Institución que solicita el examen**

1.4.1	Denominación	
1.4.2	Dirección (1)	
1.4.3	Número de referencia del expediente	
1.4.4	Sello	1.4.5 Fecha
		1.4.6 Firma



ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR

**INFORME MÉDICO DETALLADO.**

2. Apellido(s), nombre:	Fecha: Día ..... Mes ..... Año .....
2.1 Dictamen basado en el examen de:	(fecha) Día ..... Mes ..... Año .....
2.2. Dictamen basado en el informe médico	(fecha) Día ..... Mes ..... Año .....

**3. Historial del paciente**

3.1	Historial clínico – Evolución con diagnósticos, estudios clínicos de la o las enfermedades en forma cronológica, incluyendo fechas: ..... ..... .....
3.2	Principales dolencias que alega en la actualidad : ..... ..... .....
3.2.1	El paciente está siendo tratado por el médico – describir si es especialista y/o la Institución ..... ..... .....
3.3	Tratamiento actual ..... ..... .....
3.4	Antecedentes sociales, personales, familiares y carrera profesionales / Cargo/oficio/empleo ..... ..... .....
3.4.1	¿Ejerce el asegurado en la actualidad una actividad remunerada? (6) Sí <input type="checkbox"/> No <input type="checkbox"/> Número de horas de trabajo: ..... Tipo de actividad ..... .....
3.4.2	Accidentes de trabajo / enfermedades profesionales, Fecha y secuelas o daños. ..... ..... .....
3.4.3	Características del último empleo / trabajo u ocupación ..... ..... .....
3.4.4	Incapacidad temporal laboral (6) <input type="checkbox"/> desde el: ..... Cese de la actividad o desvinculación laboral, <input type="checkbox"/> el: .....

**4. Examen Físico**

4.1 Estado General (6)
------------------------

ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR

**INFORME MÉDICO DETALLADO.**

Talla ..... cm	Peso ..... kg
Estado de nutrición:	<input type="checkbox"/> bueno <input type="checkbox"/> exceso de peso <input type="checkbox"/> falta de peso
Membranas mucosas	.....
Piel	.....
Estado mental y emocional	.....
Comentarios:	..... ..... .....
<b>4.2 Cabeza:</b>	
4.2.1 Visión	
4.2.2 Oído	
4.2.3 Otros órganos sensoriales.	
4.2 Cuello (observaciones externas).	
4.3.1 Examen de la glándula tiroides.	
4.3.2 Ganglios linfáticos.	
4.3.3 Otros.	
4.4 Aparato respiratorio:	
4.5 Sistema circulatorio	
4.5.1 Corazón	
4.5.2 Pulso	
4.5.3 Tensión arterial (en reposo)	
4.5.4 Tensión arterial (segunda medición)	
4.5.5 Vasos periféricos	
4.5.6 Edema	
4.5.7 BCG (en reposo)	
4.6. Riñones	
4.7 Abdomen	
4.7.1 Aparato digestivo y órganos intra-abdominales	
4.7.2 Hígado	
4.7.3 Bazo	
4.7.4 Aparato genito-urinario	
4.8 Sistema endocrino	
4.9 Aparato locomotor (en caso necesario, usar el método neutral O, página anterior)	
4.9.1 Columna vertebral	
.....	
4.9.2 Extremidades superiores. (describir amputaciones y grados de limitaciones funcionales de las articulaciones)	
.....	
.....	
4.9.3 Extremidades inferiores. (describir amputaciones y grados de limitaciones funcionales de las articulaciones, acortamientos)	

ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR

INFORME MÉDICO DETALLADO.

4.10 Presencia de ganglios linfáticos.
4.11 Comprobaciones neurológicas (6)
4.11.1 Movimiento (potencia y tono) <input type="checkbox"/> normal <input type="checkbox"/> rápido <input type="checkbox"/> lento <input type="checkbox"/> débil
4.11.2 Marcha <input type="checkbox"/> normal <input type="checkbox"/> deficiencia / derecha <input type="checkbox"/> deficiencia / izquierda
4.11.3 Reflejos osteotendinosos y cutáneo-mucosos:
4.11.4 Síntomas neurovegetativos:
4.11.5. Síntomas extrapiramidales:.....Escala de Webster.....
4.12 Aparato Psíquico: (antecedente de tratamientos, internaciones, presentación de certificación por especialista, manifestación de síntomas o sospecha de patología psiquiátrica deberá realizarse examen psiquiátrico según arte).
4.13 Otros (alergias, etc)

5 Pruebas funcionales y fechas de realización (en caso necesario)

5.1 Función pulmonar (Indicar: espirómetros post Broncodilatador VEF1 y CCVF y grado de disnea según escala de MCR_ATS).
5.2 Función cardíaca/ECG de esfuerzo (Señalar conforme la clasificación funcional NYHA, signos de falla Cardíaca).
5.3 Ecografía Doppler (corazón y vasos)
5.4 Estudios por formación de imágenes (indicar fecha)
5.4.1 Resultados del examen radiográfico por rayos X de hoy
5.4.2 Resultados de anteriores exámenes radiográficos por rayos X realizados en otra parte



ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR  
INFORME MÉDICO DETALLADO.

6. Hoja complementaria reservada a las observaciones de otros especialistas (a completar únicamente en caso necesario).

Formulario para observaciones de otros especialistas. El área contiene líneas de texto preformateadas para facilitar la entrada de información.

**ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR  
INFORME MÉDICO DETALLADO.**

**7. Diagnóstico indicando la causa de la incapacidad**

7.1 Diagnóstico Principal: / Deficiencias Motivos de Valoración: indicando afecciones, Grado o Estadio, Porcentajes de incapacidad laboral acorde con normativa vigente (barcno).

.....  
 .....  
 .....

7.2 Diagnóstico secundario:

.....  
 .....

**8 FUNDAMENTO TÉCNICO: (Describir los datos que determinan el Grado y Porcentaje de las afecciones)**

( Consignar las restricciones que le está generando la deficiencia en su desarrollo de su desempeño laboral y su autosuficiencia económica; en el aprendizaje y aplicación del conocimiento; Comunicación; Movilidad; Cuidado personal; Vida doméstica, con base a los estándares Internacionales - CIF - OMS. )

.....  
 .....  
 .....

**Evolución de la enfermedad**

.....  
 .....  
 .....

**Perjuicio para la salud**

.....  
 .....  
 .....

**Déficits funcionales**

.....  
 .....  
 .....

Comparación con el informe anterior (fecha Día..... Mes ..... Año .....) (6)

Mejora  Empeoramiento  Sin Cambios

ACUERDO DE SEGURIDAD SOCIAL  
 ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR  
**INFORME MÉDICO DETALLADO.**

**9. El asegurado sigue siendo capaz de realizar de forma regular un trabajo (6)**

Pesado <input type="checkbox"/>	Medio <input type="checkbox"/>	Ligero <input type="checkbox"/>
---------------------------------	--------------------------------	---------------------------------

**10. Deberán tenerse en cuenta las siguientes restricciones**

10.1 Se evitará el trabajo: (6)	
En lugar húmedo <input type="checkbox"/>	En lugar frío <input type="checkbox"/>
En lugar a alta temperatura <input type="checkbox"/>	En lugar con ruidos <input type="checkbox"/>
En lugar con humo, gases, vapores <input type="checkbox"/>	
Por turnos <input type="checkbox"/>	En turno de noche <input type="checkbox"/>
En tareas que obligan frecuentemente <input type="checkbox"/>	
Al asegurado a encorvarse, elevar o transportar objetos que requiera el uso de rampas, escaleras, escalerillas <input type="checkbox"/>	
Peligro de caída <input type="checkbox"/>	
10.2 La actividad deberá desarrollarse únicamente: (6)	
Sentado <input type="checkbox"/>	Con pausas adicionales <input type="checkbox"/>
En sitios cerrados <input type="checkbox"/>	(además de las pausas habituales) número y duración de las pausas
Con una postura corporal variada <input type="checkbox"/>	Un trabajo que requiera andar, estar sentado y de pie <input type="checkbox"/>
Por turnos <input type="checkbox"/>	En turno de noche <input type="checkbox"/>
Sin presión especial por límites de tiempo <input type="checkbox"/>	

ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR

**INFORME MÉDICO DETALLADO.**

10.3 El rendimiento en el trabajo se ve reducido porque el asegurado tiene un uso restringido de sus órganos sensoriales, manos, etc  
.....  
.....  
Es alérgico a:  
.....  
.....

**11. Preguntas complementarias**

11.1 ¿ Puede el asegurado realizar un trabajo en pantalla de video? (6)  
SI  NO   
En caso negativo, especificar la causa:  
.....  
.....

11.2 ¿ Puede el asegurado trabajar sin la ayuda de otra persona en el lugar de trabajo? (6)  
SI  NO   
En caso negativo, especificar la causa:  
.....  
.....

11.3 ¿ Puede el asegurado trabajar a domicilio sin la ayuda de otra persona? (6)  
SI  NO   
En caso negativo, especificar la causa:  
.....  
.....

11.4 ¿ Puede el asegurado trabajar a tiempo completo en su último puesto de trabajo? (6)  
SI  NO   
En caso negativo, especifíquese el tiempo máximo de trabajo (en horas o porcentajes de día laboral):  
.....  
.....

11.5 ¿ Puede el asegurado realizar trabajo adaptado? (6)  
SI  NO   
En caso afirmativo, citar algunos ejemplos de trabajo adaptado:  
.....  
.....

11.6 ¿ Puede el asegurado realizar un trabajo adaptado a tiempo completo? (6)  
SI  NO   
En caso negativo, especificar el tiempo máximo de trabajo (en horas o porcentajes de una jornada laboral):  
.....  
.....

11.7 La invalidez o grado de pérdida de capacidad laboral (Incapacidad Permanente Parcial), para el último puesto es, en virtud de la legislación del país de residencia (6)  
 Total  Parcial  Grado de invalidez o porcentaje de la pérdida de capacidad laboral



ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR

**INFORME MÉDICO DETALLADO.**

11.8 Grado de invalidez o porcentaje de la pérdida de capacidad laboral para cualquier otro tipo de trabajo en relación con las aptitudes del interesado, en virtud de la legislación del país de residencia.

.....  
.....

11.9 Categoría de invalidez en virtud de la legislación del país de residencia.  
(A rellenar únicamente si el reconocimiento médico se llevó a cabo con el fin de determinar si se admite na solicitud de pensión de invalidez o de incapacidad (indemnización por incapacidad permanente parcial (subsidio por incapacidad).

.....  
.....

Las restricciones establecidas:

- (a) Han sido permanentes desde.....  
(b) Son temporales, del..... al .....

11.10 ¿Es posible mejorar el estado de salud actual? (6)

SI  NO  No es posible responder

En caso negativo, indíquese las medidas y si hay lugar a aplicar el subsidio por incapacidad (colombiano):

.....  
.....

11.11 ¿Puede mejorarse la capacidad de trabajo mediante (6)

Formación Sanitaria  Formación profesional?

SI  NO  No es posible responder

12. ¿Será necesario realizar un nuevo reconocimiento? (6)

SI  NO  En caso afirmativo, indíquese la fecha

.....

13. REEXAMEN: //(REVISIÓN DE LAS PENSIONES DE INVALIDEZ)

Antes del tercer año  A los 3 años  Fecha .....

Firma de la autoridad competente para calificar la invalidez

Sello

CERTIFICO QUE ES FIEL  
COPIA DEL ORIGINAL

ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR  
**INFORME MÉDICO DETALLADO.**

**INSTRUCCIONES**

El presente formulario se cumplimentará a máquina o en caracteres de imprenta, utilizando únicamente las líneas de puntos.

**NOTAS**

- (1) Para Ecuador indicar: calle, número, código postal, localidad y provincia.
  - (2) Para nacionales colombianos es imprescindible el segundo apellido.
  - (3) Para las mujeres que están o han estado casadas, indicar el apellido de nacimiento.
  - (4) Indicar localidad y país. \_\_\_\_\_
  - (5) Para los ecuatorianos número del identificación personal
  - (6) Para los nacionales colombianos : Cédula de Ciudadanía ( CC ), Cédula de Extranjería ( CE,) Tarjeta de Identidad (T.I.)  
Registro Civil o Número Único de Identificación (R.C o NUIP).
  - (7) Marcar la casilla que corresponda.
-

ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR

**INFORME MÉDICO DETALLADO.  
FORMULARIO PARA EL COBRO DE SEGURO O SUBSIDIO**

(Indemnización por incapacidad permanente parcial)

Apellido(s),Nombre:	Fecha:
---------------------	--------

**1 El asegurado sigue siendo capaz de realizar de forma regular un trabajo (6)**

Pesado	<input type="checkbox"/>	Medio	<input type="checkbox"/>	Ligero	<input type="checkbox"/>
--------	--------------------------	-------	--------------------------	--------	--------------------------

**2 Deberán tenerse en cuenta las siguientes restricciones**

<b>2.1 Se evitará el trabajo: (6)</b>
En lugar húmedo <input type="checkbox"/> En lugar frío <input type="checkbox"/>
En lugar a alta temperatura <input type="checkbox"/> En lugar ruidoso <input type="checkbox"/>
En lugar con humo, gases, vapores <input type="checkbox"/>
Por turnos <input type="checkbox"/> En turno de noche <input type="checkbox"/>
En tareas que obligan frecuentemente <input type="checkbox"/>
Al asegurado a encorvarse, elevar o transportar objetos que requiera el uso de rampas escaleras, escalerillas <input type="checkbox"/>
Peligro de caída <input type="checkbox"/>
<b>2.2 La actividad deberá desarrollarse únicamente: (6)</b>
Sentado <input type="checkbox"/> Con pausas adicionales <input type="checkbox"/>
En sitios cerrados <input type="checkbox"/> (además de las pausas habituales) número y duración de las pausas.....
Con una postura corporal variada <input type="checkbox"/> Un trabajo que requiera andar, <input type="checkbox"/> estar sentado y de pie
Sin presión especial por límites de tiempo <input type="checkbox"/>
<b>2.3 El rendimiento en el trabajo se ve reducido porque el asegurado tiene un uso restringido de sus órganos sensoriales, manos, etc.</b>
.....
.....
Es alérgico
a:.....
...

ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR

**INFORME MÉDICO DETALLADO.**

**3 Preguntas complementarias**

3.1	¿Puede el asegurado realizar un trabajo en pantalla de video? (6)
	SI <input type="checkbox"/> NO <input type="checkbox"/>
	En caso negativo, especificar la causa.....
3.2	¿Puede el asegurado trabajar sin la ayuda de otra persona en el lugar de trabajo? (6)
	SI <input type="checkbox"/> NO <input type="checkbox"/>
	En caso negativo, especificar la causa:.....
3.3	¿Puede el asegurado trabajar a domicilio sin la ayuda de otra persona? (6)
	SI <input type="checkbox"/> NO <input type="checkbox"/>
	En caso negativo, especificar la causa:.....
3.4	¿Puede el asegurado trabajar a tiempo completo en su último puesto de (6).....
	SI <input type="checkbox"/> NO <input type="checkbox"/>
	En caso negativo, especifíquese el tiempo máximo de trabajo (en horas o porcentajes de día laboral).....
3.5	¿Puede el asegurado realizar trabajo adaptado? (6)
	SI <input type="checkbox"/> NO <input type="checkbox"/>
	En caso afirmativo, citar algunos ejemplos de trabajo adaptado.....
3.6	¿Puede el asegurado realizar un trabajo adaptado a tiempo completo? (6)
	SI <input type="checkbox"/> NO <input type="checkbox"/>
	En caso negativo, especificar el tiempo máximo de trabajo (en horas o porcentajes de una jornada laboral).....
3.7	El grado de pérdida de capacidad laboral (Incapacidad permanente parcial), para el último puesto es, en virtud de la legislación Del país de residencia (6)
	<input type="checkbox"/> Total <input type="checkbox"/> Parcial <input type="checkbox"/> Grado de invalidez o porcentaje de la pérdida de capacidad laboral
3.8	Grado y porcentaje de la pérdida de capacidad laboral para cualquier otro tipo de trabajo en relación con las aptitudes del interesado, en virtud de la legislación del país de residencia
	.....

**ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR**

CERTIFICADO DE TRASLADO TEMPORAL  
(Artículo 14 del Acuerdo)

**A CUMPLIMENTAR POR EL EMPLEADOR O TRABAJADOR ASALARIADO O INDEPENDIENTE**

**1. DATOS DEL TRABAJADOR:**  **ASALARIADO O DEPENDIENTE**     **CUENTA PROPIA O INDEPENDIENTE**

Apellido (s): .....

Nombre (s): .....

Fecha de nacimiento: D D M M A A A A A A      Nacionalidad: .....

--	--	--	--	--	--	--	--	--	--

Número de identificación personal: Ecuador: ..... Colombia: .....

Afiliación al Sistema General de Seguridad Social en Colombia: .....

Régimen Contributivo de Salud: .....

Sistema General de Pensiones: .....

Sistema General de Riesgos Laborales: .....

Profesión/Actividad: .....

Dirección habitual: .....

Email: .....

**2. DATOS IDENTIFICATIVOS DE LA EMPRESA (para trabajadores asalariados o dependientes) O DE LA ACTIVIDAD AUTÓNOMA (para trabajadores por cuenta propia o independientes) DEL PA ASEGURADOR.**

Nombre o razón social: .....

Nº de identificación:                    Para Ecuador: .....

Para Colombia: NIT.....

Ramo o Actividad Principal: .....

Dirección: .....

Teléfono: ..... Email: .....

Sello

Fecha: D D M M A A A A

--	--	--	--	--	--	--	--	--	--

**3. DATOS DEL DESPLAZAMIENTO**

Fecha inicial del desplazamiento: D D M M A A A A A A

--	--	--	--	--	--	--	--	--	--

Periodo que se solicita: Desde D D M M A A A A A A      Hasta: D D M M A A A A A A

--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--

**El trabajador va a ejercer la actividad profesional en el siguiente centro de trabajo:**

Nombre o razón social: .....

Nº de identificación: Para Ecuador: .....

**ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR**

Para Colombia: NIT: .....

Dirección: .....

Teléfono: ..... Email: .....

**COMPLEMENTAR POR LA INSTITUCIÓN COMPETENTE DEL PAÍS ASEGURADOR**

**4. LA INSTITUCIÓN DESIGNADA DEL PAÍS A CUYA LEGISLACIÓN ESTÁ SOMETIDO EL TRABAJADOR**

Denominación: .....

Dirección: .....

Declara que el trabajador: .....

Permanece sometido a la legislación de:  Ecuador  Colombia

Durante el periodo: desde D D M M A A A A Hasta D D M M A A A A

D	D	M	M	A	A	A	A	Hasta	D	D	M	M	A	A	A	A

Sello Fecha: D D M M A A A A

D	D	M	M	A	A	A	A

**INSTRUCCIONES**

El formulario deberá cumplimentarse por triplicado ejemplar en letra tipo imprenta, en el supuesto de trabajadores, ecuatorianos o colombianos, que se desplacen al otro país por un período inferior a dos años.

La Institución Competente del país asegurador expedirá los formularios a petición del empleador o trabajador por cuenta propia, remitiendo uno al solicitante y otro a la Institución Competente del país receptor.

**Indicaciones para el empleador o trabajador:**

Si el traslado o el desplazamiento se prolongan más allá de los dos años inicialmente previstos, el empleador o el trabajador por cuenta propia deberán formular una solicitud de prórroga no superior a un año debidamente justificada ante la Institución Competente del país asegurado, con tres meses de antelación a la finalización del periodo autorizado.

NOTA COLOMBIANA: De conformidad con el principio de territorialidad establecido en la Ley 100 de 1993 y de conformidad con el Decreto 2710 de 2010, los servicios de salud para el cotizante y su grupo familiar se presentarán únicamente en Colombia.

**AUTORIDADES COMPETENTES**

(Artículo 5 Acuerdo)

**En Ecuador:**

INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL

Dirección: .....

Teléfono: .....

Email: .....

**En Colombia:**

MINISTERIO DE TRABAJO

Carrera 14 No. 99-33

Bogotá - Colombia

PBX: 489-3900 / 489-3100

www.mintrabajo.gov.co

**ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR**

**PRORROGA DE TRASLADO TEMPORAL  
Artículo 14, apartado 1, literal b) y d) y Artículo 15, apartado 2 del Acuerdo**

**A CUMPLIMENTAR POR EL EMPLEADOR O TRABAJADOR ASALARIADO O INDEPENDIENTE**

**1. INSTITUTO COMPETENTE DEL PAÍS DE DESTINO (A)**

Nombre: .....  
Dirección: .....

**2. DATOS DEL TRABAJADOR  ASALARIADO O DEPENDIENTE  CUENTA PROPIA O INDEPENDIENTE**

Apellido(s): ..... Nombre: .....

Fecha de nacimiento

D	D	M	M	A	A	A
A						

Nacionalidad: .....

Número de identidad personal: Ecuador: ..... Colombia: .....

Afiliación al Sistema General de Seguridad Social en Colombia:

Régimen Contributivo de Salud: .....

Sistema General de Pensiones: .....

Sistema General de Riesgos Laborales: .....

Profesión / Actividad: .....

Email: .....

**3. DATOS DEL DESPLAZAMIENTO**

El trabajador anteriormente citado está en posesión del formulario ECUA/COL-04 autorizado para el periodo:

Desde:

D	D	M	M	A	A	A
A						

Hasta:

D	D	M	M	A	A	A
A						

pedido por la

siguiente Institución:

Nombre: .....

Dirección: .....

El trabajador sigue trasladado o continua ejerciendo la actividad en el siguiente centro de trabajo:

Nombre o razón social: .....

Dirección: .....

Teléfono: ..... Email: .....

No. De identificación: Para Ecuador: .....

Para Colombia: NIT: .....

ACUERDO DE SEGURIDAD SOCIAL
ENTRE LA REPUBLICA DE COLOMBIA Y LA REPUBLICA DEL ECUADOR

Se solicita que continúe sometido a la legalización de : Ecuador Colombia

Durante el período desde: [DDMM AAAA] hasta: [DDMM AAAA]

4. DATOS IDENTIFICATIVOS DE LA EMPRESA (para trabajadores asalariados o dependientes) o DE LA ACTIVIDAD ( para trabajadores por cuenta propia o independientes) DEL PAÍS ASEGURADOR

Nombre o razón social:
Ramo o actividad principal:
No. De identificación : Para Ecuador:
Para Colombia: NIT:
Dirección:
Teléfono: Email:

Sello

Fecha: [DDMM AAAA]

Firma:

COMPLEMENTAR POR LA INSTITUCIÓN COMPETENTE DEL PAÍS DE DESTINO

5. LA INSTITUCIÓN COMPETENTE DEL PAÍS DE DESTINO

Denominación:
Dirección:

DECLARA: Estar de acuerdo no estar de acuerdo

En que el trabajador:

Siga sometido a la legislación de la Seguridad Social de: Ecuador Colombia

Durante el período desde: [DDMM AAAA] hasta: [DDMM AAAA]

Fecha: [DDMM AAAA]

Firma:



**ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR**

**INTRUCCIONES**

El formulario deberá complementarse por cuadruplicado ejemplar en letra tipo imprenta.

Una vez cumplimentado por el empleador o trabajador o por cuenta propia será enviado por la Institución Competente de país asegurador a la Institución Competente del país de empleo.

Esta última Institución, expresada su conformidad o disconformidad en el mismo, devolverá tras ejemplares a la Institución Competente del país asegurador. La misma remitirá 2 ejemplares a la empresa solicitante o al trabajador por cuenta propia.

**NOTA COLOMBIANA:**

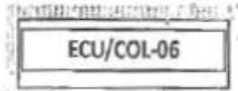
De conformidad con el principio de territorialidad establecido en la Ley 100 de 1993 y de conformidad con el Decreto 2710 de 2010, los servicios de salud para el cotizante y su grupo familiar se prestarán únicamente en Colombia.

Así mismo, bajo la legislación española, las prestaciones de salud no están cubiertas para los trabajadores desplazados a España por lo que se sugiere que dichas prestaciones mientras está en desplazamiento tenga un cubrimiento adicional.

**(A) AUTORIDADES COMPETENTES  
(Artículo 5 Acuerdo)**

En Ecuador: <b>INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL</b> Dirección..... Teléfono..... Email:.....	En Colombia: <b>MINISTERIO DE TRABAJO</b> Carrera 14 No. 99 – 33 Bogotá – Colombia PBX: 489 – 3900 / 489 – 3100 www. mintrabajo.gov.co
---	---

ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR



EJERCICIO DEL DERECHO DE OPCIÓN

Artículo 14, apartado 1, literal i) y j) del Acuerdo

1. DATOS IDENTIFICATIVOS DEL TRABAJADOR

Apellido (s): ..... Nombre: .....

Fecha de nacimiento: 

D	D	M	M	A	A	A	A
---	---	---	---	---	---	---	---

 Nacionalidad: .....

Número de identificación personal: Ecuador: ..... Colombia: .....

Afiliación al Sistema General de Seguridad Social en Colombia:

Régimen contributivo de Salud: ..... Sistema General de Pensiones: .....

Sistema General de Riesgos Laborales: .....

Dirección habitual: .....

Email: .....

2. DATOS DE LA ACTIVIDAD LABORAL

Labora desde: 

D	D	N	M	A	A	A	A
---	---	---	---	---	---	---	---

 en la misión diplomática u oficina consular que se cita a continuación:

Dirección: .....

Teléfono: ..... Email: .....

Ejerce la siguiente actividad: (1)

O está al servicio privado de (2)

Dirección: .....

Teléfono: ..... Email: .....

3. DERECHO DE OPCIÓN (3)

El trabajador declara optar por la aplicación de la legislación de Seguridad Social de ..... (4)

Conforme a lo establecido en el artículo: 14.1 i) 14.1 j) del  Acuerdo.

Lugar y fecha: .....

Firma: .....

4. LA INSTITUCIÓN DESIGNADA DEL PAÍS A CUYA LEGISLACIÓN ESTA SOMETIDO EL TRABAJADOR

Denominación: .....

ACUERDO DE SEGURIDAD SOCIAL  
ENTRE LA REPÚBLICA DE COLOMBIA Y LA REPÚBLICA DEL ECUADOR

ECU/COL-06

Dirección:

Declaro que el trabajador está sometido a la legislación de: Ecuador Colombia  
A partir de y

D	D	M	M	A	A	A	A
---	---	---	---	---	---	---	---

mientras permanezca en esta situación.

Sello

Fecha:

D	D	M	M	A	A	A	A
---	---	---	---	---	---	---	---

Firma:

**INSTRUCCIONES**

El formulario deberá cumplimentarse por triplicado en caracteres de imprenta.

La Institución competente del país asegurador expedirá los formularios a petición del trabajador, remitiendo uno al solicitante y otro a la Institución Competente del país de empleo.

El trabajador conservará el formulario con objeto de acreditar su situación frente a la Seguridad Social en el país de empleo.

**NOTAS**

- (1) Indicar la actividad del interesado; administrativo, traductor, chofer etc.
- (2) Indicar nombres y apellidos del empleador.
- (3) El derecho de opción sólo puede ser ejercido por los nacionales del país acreditante que no tengan la condición de funcionarios públicos. La opción deberá ser ejercida dentro de los tres primeros meses siguientes a la fecha de iniciación del trabajo.
- (4) Indicar Ecuador o Colombia según proceda.
- (5) **NOTA COLOMBIANA:**

De conformidad con el principio de territorialidad establecido en la Ley 100 de 1993 y de conformidad con el Decreto 2710 de 2010, los servicios de salud para el cotizante y su grupo familiar se prestarán únicamente en Colombia.

Autoridades Competentes

(Artículo 5 Acuerdo)

En Ecuador:

INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL

Dirección: .....

Teléfono: .....

Email: .....

En Colombia:

MINISTERIO DE TRABAJO.

Dirección: .....

Teléfono: .....

Email: .....

Instituto Ecuatoriano de Seguridad Social.- Es fiel Copia del original.- Lo certifico.

f.) Abg. David García S., Prosecretario, Consejo Directivo. Certifico que es fiel copia del original.- f.) Ing. Patricio Prócel I.,

Dirección Nacional de Gestión Documental del IESS.