San Isidro, 26 de Noviembre del 2025

RESOLUCION N° 000156-2025-DG/JNJ

VISTOS:

El Informe Nº 000258-2025-OTIGD-JNJ y el Memorando N° 000664-2025-OTIGD-JNJ de la Oficina de Tecnologías de la Información y Gobierno Digital, los Informes Nos 000262 y 000271-2025-OPM-JNJ de la Oficina de Oficina de Planeamiento y Modernización, y el Informe N° 000581-2025-OAJ-JNJ de la Oficina de Asesoría Jurídica.

CONSIDERANDO:

La Ley de Gobierno Digital, aprobada por el Decreto Legislativo N° 1412, establece un marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

El Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N° 029-2021-PCM establece que el Sistema de Gestión de Seguridad de la Información (SGSI), comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación;

Mediante Resolución Directoral N° 022-2022-INACAL/DN, se aprobó el uso Obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición”; y la Norma Técnica Peruana “NTP-ISO/IEC 27005:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición”;

En se sentido señala que las unidades de organización de tecnologías de la información o las que hagan sus veces en las entidades públicas son responsables de la planificación, implementación, ejecución y supervisión del uso y adopción de las tecnologías digitales como habilitantes de la implementación de la cadena de valor, soluciones de negocio, modelos de negocio o similares priorizadas en el marco de los instrumentos de gestión de la entidad, con el propósito de permitir alcanzar sus objetivos estratégicos, crear valor público y cumplir con lo establecido por el Comité de Gobierno Digital Institucional;

Mediante Resolución N° 092-2019-DG-JNJ se aprobó la Directiva N° 025-2019-DG-JNJ “Normas y procedimientos para la administración de cuentas y claves de acceso a los usuarios y el uso de los servicios de correo electrónico e internet en la Junta Nacional de Justicia”, sin embargo, la aludida directiva fue aprobada antes de la entrada en vigencia del Reglamento de la Ley de Gobierno Digital por lo que corresponde actualizarla;

La Oficina de Tecnologías de la Información y Gobierno Digital ha elaborado la Guía Técnica para la Administración de cuentas y claves de Acceso a los Usuarios y el uso de servicio de correo electrónico e internet en la Junta Nacional de Justicia, la misma que reemplaza a la Directiva aludida en el considerando precedente;

A través de la Resolución N° 086-2025-DG-JNJ se aprobó la relación de documentos normativos de la JNJ, la misma que señala que una Guía Técnica es un documento normativo que muestra orientaciones técnicas y prácticas, proporciona instrucciones, paso a paso, consejos e información básica para la ejecución de los procesos asimismo contiene modelos para realizar determinadas tareas;

Por su parte, la Resolución N° 097-2025-DG-JNJ que aprobó la Directiva para la formulación, revisión, aprobación, publicación, difusión y derogación de documentos normativos en la Junta Nacional de Justicia dispone, las guías técnicas son aprobadas con resolución de Dirección General;

En ese sentido, corresponde emitir el acto de administración que apruebe la Guía Técnica para la Administración de cuentas y claves de Acceso a los Usuarios y el uso de servicio de correo electrónico e internet en la Junta Nacional de Justicia y que deje sin efecto la Directiva N° 025-2019-DG-JNJ “Normas y procedimientos para la administración de cuentas y claves de acceso a los usuarios y el uso de los servicios de correo electrónico e internet en la Junta Nacional de Justicia”;

De conformidad con lo dispuesto en el Reglamento de Organización y Funciones de la Junta Nacional de Justicia; las Resoluciones N° 86 y 097-2025-DG-JNJ y, con el visado de los jefes de las Oficinas de Tecnología de la Información y Gobierno Digital, de Planeamiento y Modernización y de Asesoría Jurídica;

SE RESUELVE:

Artículo 1. Aprobar la Guía Técnica para la Administración de cuentas y claves de Acceso a los Usuarios y el uso de servicio de correo electrónico e internet en la Junta Nacional de Justicia, que forma parte integrante de la presente resolución.

Artículo 2. Dejar sin efecto la Resolución N° 092-2019-DG-JNJ que aprueba la Directiva N° 025-2019-DG-JNJ “Normas y procedimientos para la administración de cuentas y claves de acceso a los usuarios y el uso de los servicios de correo electrónico e internet en la Junta Nacional de Justicia”.

Artículo 3. Disponer la publicación de la presente resolución, en el portal de transparencia y en el portal institucional de la Junta Nacional de Justicia (www.gob.pe/jnj).

Regístrese, comuníquese y publíquese.

(documento firmado digitalmente)
KATIA MARIA DEL CARMEN NUÑEZ MARISCAL
DIRECTORA GENERAL
JUNTA NACIONAL DE JUSTICIA

Junta Nacional de Justicia

GUÍA TÉCNICA PARA LA ADMINISTRACIÓN DE CUENTAS Y CLAVES DE ACCESO A LOS USUARIOS Y EL USO DE SERVICIO DE CORREO ELECTRÓNICO E INTERNET EN LA JUNTA NACIONAL DE JUSTICIA

Concepto	Nombre y Apellido - Puesto	Firma	Fecha
Elaborado por:	Mario Vallejos Herencia Oficial de Seguridad y Confianza Digital	Firma Digital Firmado digitalmente por VALLEJOS HERENCIA Mario Alberto FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 05.11.2025 15:17:19 -05:00	En firma digital
Elaborado por:	José Alarcón Butrón Jefe de la Oficina de Tecnologías de la Información y Gobierno Digital	Firma Digital Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 05.11.2025 15:26:32 -05:00	En firma digital
Revisado por:	Rafael Sifuentes del Mar Jefe de la Oficina de Planeamiento y Modernización	Firma Digital Firmado digitalmente por SIFUENTES DEL MAR Rafael Nicolas FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 07.11.2025 09:02:53 -05:00	En firma digital
Aprobado por:	Katia Núñez Mariscal Directora General	Firma Digital Firmado digitalmente por NUÑEZ MARISCAL Katia Maria Del Carmen FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 26.11.2025 15:18:05 -05:00	En firma digital

I. OBJETIVO:

Cautelar la seguridad de la información, la óptima administración de cuentas de usuario y uso de claves de acceso a las plataformas informáticas y sistemas de información, correo electrónico institucional e internet en la Junta Nacional de Justicia (JNJ).

II. AMBITO DE APLICACIÓN:

Esta guía es de cumplimiento obligatorio para todos los servidores civiles de la JNJ, sin importar su nivel jerárquico, régimen laboral o modalidad contractual, así como para los beneficiarios de modalidades formativas, en lo que corresponda.

III. CONTROL DE CAMBIOS:

N°	FECHA	NUMERAL	TEXTO MODIFICADO	RESPONSABLE

IV. BASE LEGAL:

4.1. Base Legal:

- Constitución Política del Perú.
- Ley N° 29733, Ley de Protección de Datos Personales y sus modificatorias.
- Ley N° 30096, Ley de Delitos Informáticos.
- Decreto Supremo N° 016-2024-JUS, que aprueba el Reglamento de la Ley 29733, Ley de Protección de Datos Personales.
- Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva Nº 005-2003-INEI/DTNP sobre “Normas para el uso del servicio de correo electrónico en las entidades de la administración pública.”
- Resolución Directoral N° 022-2022-INACAL/DN, que aprueba el uso Obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición”; y la Norma Técnica Peruana “NTP-ISO/IEC 27005:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición”; y la Norma Técnica Peruana “NTP ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición”.
- Resolución de Contraloría N° 146-2019-CG, que aprueba la Directiva N° 006-2019-CG/INTEG, la cual implementa el "Sistema de Control Interno en las entidades del Estado".

Las citadas normas incluyen sus respectivas modificatorias de ser el caso.

4.2. Definiciones:

- **Administrador de Red**: Servidor civil de la Oficina de Tecnologías de la Información y Gobierno Digital designado (OTIGD) por el jefe de la citada oficina, que se encarga de establecer los accesos y configuración de la plataforma tecnológica que permita acceder o no a los servicios informáticos de la JNJ; además, se encarga de la protección de la información cautelando la no distribución, acceso, modificación, destrucción y/o uso no autorizado.
- **Clave de acceso**: Combinación de números, letras y signos que deben teclearse para tener acceso a un sistema informático, estación de trabajo, punto de red, entre otros.
- **Controlador de Dominio**: Servidor de red donde los usuarios se autentican, guardan las políticas de acceso, seguridad, y sirve como mecanismo de control.
- **Correo electrónico**: Es un servicio de red para permitir a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos.
- **Cuenta de usuario**: Identificación proporcionada a un usuario, que le permite tener acceso a un sistema informático, estación de trabajo, punto de red, entre otros. La cuenta se encuentra relacionada a un nombre de usuario y una clave de acceso.
- **Firewall:** Normalmente conocido como barrera cortafuegos. Es un filtro de software y/o hardware que controla todas las comunicaciones entrantes y salientes de una red a otra red, cuya función principal es denegar o permitir el acceso a comunicación. Así, para denegar o autorizar una comunicación, el firewall primero analiza el perfil del usuario si tiene o no acceso a un determinado servicio: (acceso a Internet, correo, transferencia FTP, etc.) y luego denegará o permitirá el acceso a la comunicación.
- **Información confidencial**: Toda aquella información restringida que debe ser accedida por personas expresamente autorizadas, en base al concepto de "necesidad-de-conocer" *(need-to-know)*. Su divulgación requiere del consentimiento formal del responsable de la misma.
- **Información interna**: Toda aquella información de uso interno de la JNJ y cuyo acceso puede ser permitido a cualquier servidor de la institución, pero que no puede ser transmitida fuera de la JNJ sin autorización escrita de quien generó la información.
- **Información pública**: Toda aquella información cuya divulgación fuera de la JNJ no representa riesgo alguno para la institución.
- **Internet:** Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, funcionando como una red lógica única.
- **Mesa de ayuda (Help Desk):** Servicio de ayuda y soporte en línea informático que se brinda a todos los usuarios de la Institución. Cuenta con herramientas de hardware y software para resolver cualquier tipo de problema.
- **Navegación web:** También denominada navegación por la red, es la actividad que consiste en explorar en Internet en búsqueda de información útil.
- **Usuario:** Persona que realiza determinada labor o servicio para una unidad de organización de la JNJ, a quien se le ha asignado una identificación digital para acceder a ciertos recursos informáticos y de telecomunicaciones disponibles en la red.

- **Virus:** Código computacional escrito intencionalmente para auto instalarse en la computadora de un usuario sin el conocimiento o el permiso de éste. Normalmente se comporta como un programa parásito, pues infecta y ataca a los archivos del sistema y del usuario. Para propagarse se replica a sí mismo ilimitadas veces, llegando a producir serios daños que pueden afectar a los sistemas y archivos en general, pudiendo estos últimos daños ocasionar que se borren o destruyan los archivos.

4.3. Responsabilidades y Roles:

i. El Jefe de la Oficina de Tecnologías de la Información y Gobierno Digital se encarga de:

- Controlar el proceso de otorgamiento de accesos, validando las solicitudes recibidas y atendiendo aquellas debidamente autorizadas.

- Administrar el servicio de correo electrónico, entrega de claves de acceso a los usuarios para los sistemas informáticos, así como velar por el cumplimiento de la presente directiva.

- Administrar adecuadamente el acceso al servicio de Internet a los usuarios autorizados de la JNJ, tomando las acciones que sean necesarias para asegurar la confiabilidad del mismo, en función a los recursos y capacidades disponibles.

- Autorizar requerimientos de manera excepcional, conforme a lo establecido en la presente directiva.

ii. El Administrador de Red es responsable de:

- Velar por la adecuada configuración de las políticas de seguridad definidas (usuarios y contraseñas) en los servicios de Internet de la JNJ.

- Apoyar al personal a cargo de los sistemas de información (propietarios de la información, gestión y de su utilización en el proceso de definición y mantenimiento de los perfiles asignados en las aplicaciones).

- Controlar que el proceso de otorgamiento de cuentas de correo a los usuarios se realice de acuerdo a lo estipulado por la Norma para la Administración de Cuentas y Claves de Acceso de Usuarios.

- Controlar el proceso de otorgamiento de cuentas de usuario con acceso a Internet, en cada uno de sus niveles.

iii. Los usuarios son responsables de:

- Hacer uso de la identificación asignada de forma personal para acceder a la red y a los sistemas informáticos de la Junta (cuenta de usuario y contraseña), conforme a las disposiciones de la presente directiva.

- Hacer buen uso del correo electrónico, de acuerdo con las disposiciones establecidas en la presente directiva.

- Hacer buen uso de los permisos de navegación a internet, conforme a las disposiciones establecidas en la presente directiva.

iv. Los servicios de correo electrónico, chat interno, internet, y otros, así como los equipos y plataformas informáticas que los hacen posible, son de propiedad de la JNJ. Las comunicaciones efectuadas por los usuarios a través de estos servicios, se encuentran protegidas por el derecho al secreto y a la inviolabilidad de las comunicaciones, consagradas en el inciso 10) del artículo 2° de la Constitución Política del Perú; por lo tanto, la JNJ se encuentra prohibida de conocer el contenido de los mensajes de correo electrónico o de las conversaciones del comando o programa de mensajería instantánea que haya proporcionado al trabajador, así como interceptarlos, intervenirlos o registrarlos. Para acreditar el uso del correo electrónico para fines diferentes a las obligaciones laborales de los trabajadores se requiere que se realice una investigación de tipo judicial, lo cual implica realizar las gestiones que correspondan, de acuerdo a ley.

4.4. Administración de perfiles, cuentas y claves de acceso de usuarios:

i. Toda cuenta de usuario debe tener un perfil asociado a cada sistema y/o equipo al que le corresponda acceder en base a sus funciones.

ii. Toda cuenta de usuario debe tener asociada obligatoriamente una contraseña. Dicha contraseña debe ser exigida en el proceso de autenticación, debe tener como mínimo 8 caracteres alfanuméricos, incluyendo mayúsculas, minúsculas y números.

iii. Se prohíbe compartir la cuenta de usuario y la contraseña con otras personas, independientemente de la jerarquía del solicitante.

iv. Las cuentas de usuarios deben ser otorgadas únicamente a personal de la JNJ. El propietario de la información es el encargado de autorizar los accesos requeridos. La cuenta del usuario debe estar conformada por el primer nombre más el primer apellido del trabajador. De existir duplicidad del nombre de la cuenta por homonimia, se deberá añadir al final de la cadena de caracteres del apellido, la inicial del segundo apellido y así sucesivamente.

v. Para el caso de locadores de servicios, las cuentas de usuario se crearán sólo a solicitud expresa y, debidamente justificada, de las áreas usuarias, con la autorización adicional del jefe de la OTIGD. Estas cuentas tendrán como nomenclatura “consultorjnj” más un número único de identificación empezando desde el 01. En estas cuentas no deberán utilizarse el nombre de la persona que presta el servicio.

vi. Se prohíbe el uso de cuentas genéricas, que permitan el acceso de varios usuarios haciendo uso de una misma identificación. En aquellos casos en que sea absolutamente necesario y justificado el uso de cuentas genéricas,

su creación deberá contar con una aprobación explícita del Jefe de la OTIGD. Se deberá asignar un responsable único por cada cuenta genérica y registrar dicha asignación y responsabilidad por escrito.

4.5. Políticas de Contraseña:

i. Los usuarios y contraseñas son de carácter reservado y de uso estrictamente personal.

ii. Los usuarios, por temas de seguridad, no deben habilitar en los sistemas de información la opción de guardar su contraseña.

iii. No se debe anotar las contraseñas de acceso en lugares de fácil acceso del público, tales como: bajo del teclado, en agendas, bajo el teléfono, detrás de una foto, etc. Cualquier contraseña encontrada en estos medios será informada al Administrador de red para que proceda al bloqueo de la cuenta y emita el informe respectivo.

iv. En casos excepcionales, cuando se requiera transmitir una contraseña, esto será de total responsabilidad del usuario dueño de la cuenta; no debe transmitirse las contraseñas verbalmente a través de líneas telefónicas, ni en texto a través de las redes. Se debe utilizar un medio confiable para la comunicación de las mismas.

v. Las contraseñas están conformadas con un mínimo de ocho (8) caracteres alfanuméricos, que incluye una letra mayúscula y un número como mínimo. Es recomendable que el usuario, al registrarlas, considere que esta debe ser fácil de recordar, pronunciable y que cumpla con las siguientes características:

   - No basarse en algún dato personal que facilite a otra persona acceder a las mismas; por ejemplo, nombres, números de teléfono, fecha de nacimiento, palabras comunes como lugares geográficos, entre otros.
   - Obligatoriamente debe contener al menos un dígito numérico, un carácter en mayúscula y otro en minúscula.
   - En el proceso de cambio de contraseñas, la nueva no debe ser igual a las últimas 3 contraseñas utilizadas.
   - La contraseña no debe estar en blanco.

   Alguna de las características antes mencionadas podrá ser validada por el sistema, de modo tal que su aplicación sea obligatoria.

vi. La OTIGD podrá, de considerar conveniente, dar un tiempo de vigencia de las contraseñas de acceso a la red y de los sistemas de información, solicitando al término del periodo estimado que el usuario efectúe el cambio de contraseña.

4.6. Sistema de Control de Acceso:

i. En las plataformas y/o sistemas de información donde se procese y/o almacene información confidencial, interna o pública, debe implementarse un

sistema de control de accesos automático o adoptar los controles pertinentes que permitan mitigar los riesgos inherentes al acceso no autorizado.

ii. Se debe implementar, en la medida que las plataformas o sistemas de información lo permitan, un sistema de control de accesos que registre los eventos relacionados con la seguridad.

iii. Se deben adoptar medidas de seguridad apropiadas para asegurar que los registros de eventos relacionados con la seguridad no sean consultados, alterados o eliminados sin previa autorización.

iv. La Oficina de Administración y Finanzas, conforme a los requerimientos formulados por la Oficina de Tecnologías de la Información y previa coordinación con ésta, adoptará las acciones necesarias para la implementación del sistema de control de accesos.

4.7. Administración de Accesos:

i. Se debe autenticar a todos los usuarios antes de que éstos accedan a los recursos asignados.

ii. Debe restringirse totalmente el acceso a información del sistema al que el usuario se está conectando, hasta que este haya sido debidamente autenticado y el proceso de conexión a los recursos haya terminado satisfactoriamente.

iii. La conexión sólo permitirá al usuario acceder a la información a la cual está autorizado, de conformidad con los requerimientos de su trabajo y según lo señalado en el Anexo N° 1 “Ficha de acceso a servicios TI”.

iv. En la medida que los sistemas lo permitan, los intentos infructuosos de conexión deberán contabilizarse, estableciéndose hasta un máximo de tres (3) para proceder al bloqueo del usuario inutilizando su conexión; estos intentos infructuosos deberán ser registrados como eventos de seguridad.

v. El usuario debe desconectarse al terminar su sesión. Siempre que la tecnología lo permita, el sistema deberá controlar los terminales inactivos de forma que proceda a su desconexión automática luego de 30 (treinta) minutos de permanecer sin actividad.

vi. El acceso a las funciones de administración de las plataformas y/o sistemas de información deberán estar restringidos a personal autorizado. En estos casos, en la medida que las herramientas disponibles lo permitan, se debe tener un control más detallado del acceso a los sistemas de información mediante dichas cuentas.

vii. Los usuarios solo podrán acceder a los equipos de cómputo asignados para sus labores; está prohibido acceder a otros equipos, salvo autorización expresa y justificada del jefe de la unidad de organización en donde se encuentre instalado el equipo, y sólo cuando sea indispensable, en atención a las necesidades del servicio, de lo que se dejará constancia.

4.8. Asignación de cuentas de usuario:

i. Las solicitudes de creación de cuentas de usuario son enviadas al Jefe de la OTIGD por parte de la unidad de organización a la cual pertenece el usuario, indicando los recursos informáticos a los que está autorizado acceder.

ii. De no mediar inconveniente, el Jefe de la OTIGD reenviará la solicitud de acceso al Administrador de Red para que otorgue los accesos solicitados.

iii. Las solicitudes de acceso a aplicaciones web, como extranet o intranet, serán remitidas al personal de informática responsable de la administración de dichas plataformas de la OTIGD, quienes crearán los usuarios respectivos, respetando las nomenclaturas de nombres de cuentas y las políticas de contraseña.

iv. Cuando un trabajador o locador deje de laborar o prestar servicios, respectivamente, sus cuentas de acceso a la red, correo electrónico y sistemas de información son cerradas. Está prohibido solicitar acceso a la información que se encuentre dentro de las cuentas de usuario o correo electrónico cerradas, debiendo el Jefe de la dependencia, bajo responsabilidad, solicitar la entrega de cargo correspondiente en la que se debe incluir los documentos, archivos y comunicaciones electrónicas necesarias para la continuidad de operaciones de la dependencia; la OTIGD bajo ninguna circunstancia accederá a cuentas ya cerradas salvo esto sea indicado por mandato judicial.

v. En el caso del personal nombrado o contratado, corresponde al jefe del Área de Recursos Humanos, solicitar al jefe de la OTIGD la cancelación de las cuentas de acceso respectivas; de igual forma para el caso de locadores de servicios, el Área de Logística, previa coordinación con el área usuaria respectiva, será responsable del envío de la solicitud de cancelación de las cuentas de acceso correspondientes. El Jefe de la OTIGD reenviará dichas solicitudes al Administrador de Red para que cancele los accesos solicitados.

vi. Cualquier acción realizada desde las cuentas de usuario que debieron ser canceladas y no fueron comunicadas a la OTIGD oportunamente, será de exclusiva responsabilidad de las dependencias indicadas en el punto anterior, según corresponda.

4.9. Auditoria y revisión de las solicitudes de acceso a usuarios

i. El Jefe de la OTIGD verifica el contenido de cada solicitud de acceso, antes de que la misma sea enviada al Administrador de red.

ii. El Administrador de Red y personal de soporte técnico de la OTIGD, ante alarmas y alertas del servidor de dominio o antivirus que indiquen posibles actividades sospechosas en los equipos de cómputo de la JNJ y previa coordinación con los usuarios de tales equipos, procederán a la revisión de los mismos a fin de descartar software malicioso o algún otro método que ponga en riesgo la estabilidad de la red institucional.

4.10. Otras consideraciones

i. El usuario efectúa el cambio de sus contraseñas cada vez que considere que están comprometidas o hayan sido divulgadas a terceros, independientemente del cambio periódico solicitado automáticamente por el sistema.

ii. Cada servidor o usuario es totalmente responsable por las acciones efectuadas empleando su identificación de usuario asignado, aunque estas se realicen cuando aquel no se encuentre frente a su computadora personal.

4.11. Uso del correo electrónico institucional:

i. *Asignación de correo y acceso*

a) El buzón de correo electrónico asignado a los servidores es propiedad de la JNJ y es suministrado únicamente con el propósito de enviar y recibir comunicaciones de la JNJ, así como con proveedores y terceros relacionados a los fines institucionales.

b) El correo electrónico es un medio de comunicación cuya confidencialidad está en función de una contraseña de acceso personal e intransferible. En el caso de que se envíe y/o reciba a través de Internet documentos altamente confidenciales, éstos deberán estar protegidos con una contraseña adicional, para lo cual podrán solicitar apoyo al personal de soporte técnico de la Institución.

c) La Oficina de Tecnologías de la Información y Gobierno Digital (OTIGD), ante la sospecha de un mal uso del correo electrónico asignado a un usuario, y cuando exista una razón de interés institucional, tales como la comisión de una falta laboral, la protección del sistema informático, el cumplimiento de obligaciones institucionales, entre otros, pone en conocimiento de estas circunstancias a la Dirección General, a fin de que, si lo considera pertinente, disponga las acciones que el caso amerite.

d) El empleo de cuentas grupales de correo por parte de la Dirección General, Secretaría General, Oficinas y a todo el personal, es exclusivamente para envío de comunicaciones con fines institucionales; queda estrictamente prohibido su uso para envío de comunicaciones personales, cadenas o mensajes que no involucren directamente a los destinatarios.

e) Se encuentra prohibida la transmisión vía correo electrónico de los siguientes elementos: usuarios, identificadores de entrada al sistema (Login, IDs), contraseñas, configuraciones de redes internas, direcciones y nombres de sistemas.

f) Cuando un usuario es desplazado a otra unidad de organización dentro de la entidad, podrá solicitar a la OTIGD el traslado de su cuenta de

correo electrónico desde su equipo de cómputo que venía usando hacia el equipo asignado en la nueva dependencia.

ii. *Buen uso del correo electrónico:*

a) El servicio de correo electrónico es provisto por la JNJ a los usuarios con el objeto de apoyar el desarrollo de sus funciones.

b) La JNJ define el estándar de una plataforma de correo institucional única; asimismo queda estrictamente prohibido la utilización de otro sistema de correo como medio oficial.

c) El uso aceptable del correo se basa fundamentalmente en la comunicación entre trabajadores internos y usuarios externos para fines institucionales.

d) Los correos electrónicos enviados desde las cuentas provistas por la JNJ tienen las mismas consideraciones tomadas en cuenta al enviar una carta formal con el membrete de la JNJ.

e) En la comunicación por correo se mantienen las mismas reglas de cortesía y formalidades de la información escrita, aplicando también todas las reglas semánticas y ortográficas.

f) Los mensajes de correo electrónico enviados después del horario de trabajo normal del usuario, se consideran enviados el día laboral siguiente.

g) Cuando se incluya el mensaje original en una respuesta, se sugiere eliminar toda información accesoria que no esté relacionada con el contenido de la respuesta. En estos casos queda estrictamente prohibido introducir modificaciones a los mensajes anteriores sin advertir por escrito esa circunstancia.

h) Cada usuario es responsable de mantener el espacio asignado en su cuenta o límites de correo para permitir la correcta recepción de mensajes, para lo cual deberá realizar labores de mantenimiento y limpieza de su correo.

i) El administrador de red, al verificar actividad inusual en el funcionamiento del servicio de correo electrónico institucional electrónico, y si esta es atribuida a una cuenta de correo de la JNJ, bloqueará dicha cuenta de correo para salvaguardar la continuidad de las operaciones del resto de usuarios. En estos casos, el personal de Soporte Técnico de la OTIGD, en coordinación con el usuario afectado, procederá a verificar el equipo de cómputo asignado y la configuración de la cuenta de correo, y con ello brindar la solución requerida.

j) Los usuarios procuran no abrir mensajes de correo electrónico de remitentes desconocidos, ya que podrían ser virus que afectarían la estabilidad del equipo de cómputo y la red institucional; en caso el usuario

tenga sospecha de algún mensaje recibido, comunica inmediatamente al personal de Soporte Técnico de la OTIGD para la revisión del contenido.

k) La JNJ no es responsable por el efecto que pueda causar un mensaje enviado por un trabajador a otro trabajador o a un grupo de trabajadores. Los mensajes enviados desde cualquier cuenta de correo son responsabilidad únicamente de la persona a la que se le confió dicha cuenta.

l) Los usuarios deben estar informados que las comunicaciones a través de los correos electrónicos podrían, dependiendo de la tecnología, ser reenviadas, interceptadas, impresas y almacenadas por otros, por lo tanto, dicha información es susceptible de fraudes y alteraciones; en ese sentido se deben tomar las provisiones que el caso amerita.

m) La JNJ deberá agregar en el pie de cada correo enviado, una nota que indique la confidencialidad de esta información.

n) Al pie de cada mensaje los usuarios insertan una auto firma, a fin que permita al receptor de datos identificar formalmente a su autor, de manera que esté vinculada únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación posterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento.

ii. Cuentas genéricas de correo electrónico:

a) El Jefe de la Oficina de Tecnologías de la Información aprueba el uso de las cuentas genéricas de correo electrónico, las que son asignadas a una persona, que será responsable de la cuenta y aparecerá como tal.

b) Todas las cuentas genéricas tienen contraseñas robustas, y son conformadas por caracteres alfanuméricos y con un largo mínimo de 8 (ocho) caracteres alfanuméricos que incluye una letra mayúscula y un número como mínimo.

iii. Prohibiciones del servicio de correo electrónico:

a) Se prohíbe el uso del correo electrónico para fines ajenos a la institución, tales como recibir o transmitir música, videos, humor, gráficos e imágenes inapropiadas. El contenido de los mensajes no debe ser injurioso, ofensivo o irrespetuoso. Los correos electrónicos deben contener temas propios y de interés de la Institución.

b) En el caso que la información particular sea canalizada a través de una persona que se ausente de la JNJ, ésta deberá delegar esta función a otra persona de la misma dependencia durante su ausencia y anunciar a sus corresponsales el motivo del cambio.

c) Se prohíbe difundir por correo electrónico al interior de la organización, noticias que provengan de Internet o de otros medios, o tomar información de dicha red dándola por cierta.

d) Cualquier documento que se adjunte a un mensaje, deberá estar libre de virus. Será responsabilidad del usuario emisor del mensaje la revisión mediante antivirus. Las áreas receptoras de mensajes infectados con virus deberán abstenerse de abrirlos y deberán informar al Administrador de Red sobre su presencia.

e) Sólo el Administrador de Red puede utilizar el correo electrónico para advertir sobre virus o su posible existencia en las PC, habiendo verificado la autenticidad de la fuente de información.

f) Se prohíbe difundir por correo electrónico, dentro o fuera de la JNJ información clasificada como confidencial. Sin embargo, si este fuera el caso, el correo electrónico deberá tener en el campo asunto la palabra CONFIDENCIAL, y de ser posible se deberá utilizar técnicas de encriptación, para lo cual deberá coordinar con la Oficina de Tecnologías de la Información para realizar un envío seguro.

g) Los trabajadores de la JNJ no deben utilizar el correo electrónico como base de datos. Es exclusiva responsabilidad de los usuarios mantener en el disco duro de su computadora los archivos recibidos como anexos o adjuntos y los mensajes de correo que estime importantes. El resto de mensajes debe eliminarse periódicamente.

h) La OTIGD no se hace responsable por la eliminación de mensajes producido por: virus, mal funcionamiento de la PC, eliminación por parte del usuario, u otro.

iv. Bloqueo de correos electrónicos:

a) La OTIGD bloquea los mensajes provenientes de servidores de correo gratuito (Hotmail, Yahoo, Gmail, etc.), siempre que se detecte que de cuentas creadas en estos servidores se envíe información mal intencionada a los usuarios de la Junta, tales como correos SPAM (correos basura de publicidad), correos PHISHING (correos suplantando identidades).

b) La OTIGD bloquea los mensajes provenientes de servidores de correo electrónico de instituciones privadas o entidades estatales que no superen el mecanismo de control Antispam implementado en la institución; bajo ninguna circunstancia se permitirá el ingreso de dichos mensajes hasta que los servidores de origen superen sus deficiencias de seguridad.

c) La OTIGD bloquea los mensajes provenientes de servidores gratuitos que tengan adjuntos de archivos de los siguientes tipos: ejecutables (*.exe, *.msi, etc.), comprimidos (*.zip, *.rar, etc.), de música y video en

todos sus formatos (*.mp3, *.wav, etc.), entre otros; pues podrían contener virus, spyware, gusanos, etc.

d) La OTIGD evita la usurpación de identidad, impidiendo el ingreso de mensajes provenientes de Internet de supuestos remitentes que pertenecen al dominio "JNJ.gob.pe", pues los remitentes permitidos enviarán siempre mensajes desde dentro de la red de la JNJ y no de fuera de ella.

4.12. Del acceso y uso de Internet:

i. Los usuarios al utilizar los servicios de Internet provisto por la JNJ deben tener precaución con las páginas que ofrecen servicios gratuitos a cambio de una inscripción donde se solicita un conjunto de datos. Se debe tener precaución con la información que se suministra. No debe suministrarse información de la JNJ ni de su infraestructura tecnológica ni de comunicaciones.

ii. La OTIGD implementará mecanismos de seguridad, como filtros de contenido, Proxy y Firewall que disminuyan la posibilidad de acceder a las redes de la JNJ a personas no autorizadas. Como principio general se debe utilizar "todos los servicios que se encuentran deshabilitados a excepción de los que se encuentran explícitamente aprobados".

iii. Sólo se podrá hacer uso de los servicios de Internet (navegación, correo y otros) a través del canal de comunicación provisto por la JNJ. No se podrá efectuar conexiones a Internet vía modem o medios alternativos a no ser que se cuente con la autorización formal por parte del Administrador de Red de la Información (o quien haga sus veces).

iv. Se prohíbe el uso de Internet para fines que no sean netamente laborales, así como participar en actividades políticas, religiosas o comerciales que puedan comprometer la información de la JNJ, estar involucrado en actividades fraudulentas o distribuir intencionalmente información falsa o difamatoria que podría deteriorar la imagen de la JNJ.

v. Se prohíbe el uso de Internet para acceder a música, pornografía u otros tópicos que no concuerden con las funciones o actividades asignadas por la JNJ.

vi. Cuando por propósitos justificados para el desarrollo de las responsabilidades de un servidor público de la JNJ sea necesario obtener software desde Internet, éste será canalizado a través del encargado de Soporte Técnico (Help Desk) de la OTIGD. Las faltas al respecto serán monitoreadas e informadas al Administrador de Red.

vii. Se debe controlar la introducción de virus en forma intencional o accidental a través de archivos obtenidos de Internet.

viii. En caso que algún usuario requiera tener acceso a un servicio no autorizado, por las tareas que tiene asignada, el Administrador de Red deberá evaluar la

posibilidad de incorporar mecanismos que permitan asegurar la confidencialidad e integridad de la información transferida por ese medio y activar el servicio de darse el caso, previa autorización del Jefe de la OTIGD.

ix. Está prohibido acceder o intentar acceder al Internet utilizando otras configuraciones de Proxy, DNS, Puertas de enlace y otras sin autorización del Administrador de Red.

x. El uso de las herramientas de navegación y el acceso a Internet debe orientarse a cubrir las necesidades específicas de la JNJ.

xi. La JNJ se reserva el derecho de monitorear o hacer el seguimiento de la navegación web que realicen los usuarios del servicio de Internet, pudiendo tomar medidas correctivas en caso de incumplimiento de la presente norma.

4.13. Buen uso del servicio de navegación:

i. Comunicación entre trabajadores internos y usuarios externos para cubrir las necesidades específicas de la JNJ.

ii. Soporte técnico para temas de tecnología de información.

iii. Revisión de sitios Web de proveedores y empresas allegadas al sector para obtener información de los productos, obtener referencia sobre marcos legales, información técnica y recursos.

iv. Obtener información financiera, técnica, de actualidad, etc. relevante a las necesidades específicas de la JNJ.

v. Comunicación con otras empresas, socios estratégicos, etc.

vi. El uso de Internet con fines de investigación y desarrollo personal, tales como capacitaciones, desarrollo de tesis, elaboración de monografías, entre otros, relativos a estudios de capacitación y/o especialización, estará permitido únicamente fuera de horarios de oficina y bajo conocimiento del Jefe inmediato superior; a excepción de aquellas en donde la Junta Nacional de Justicia sea el organizador, patrocinador o se cuente con la aprobación de la alta dirección.

4.14. Prohibiciones del servicio de navegación:

i. Todos los usuarios de la JNJ sin excepción estarán prohibidos de navegar a sitios no alineados con las buenas conductas como son los de contenido pornográfico, actividades ilegales (drogas, terrorismo, actividades criminales, etc.), juegos en línea, aplicaciones de escritorio remoto, compras en línea, entre otros.

ii. Los usuarios tendrán prohibido el uso de herramientas de Chat, redes sociales, videos en línea, aplicaciones de escritorio remoto, salvo exista la justificación de accesos mediante solicitud formal del Jefe inmediato superior dirigido al Jefe de la OTIGD.

iii. La habitualidad de visita a estos sitios no aceptables, constituye una infracción ética por parte de los empleados públicos de la JNJ.

iv. Navegar o acceder a servicio de Internet desde los servidores, para bajar un parche, actualización de firmware o conectarse a servicio técnico remoto, salvo que sea estrictamente necesario.

4.15. Asignación de accesos a los servicios de Internet:

i. El acceso a los servicios de Internet es solicitado por el Jefe inmediato superior de la dependencia a la que pertenece el usuario, mediante un Memorando o correo electrónico dirigido al Jefe de la OTIGD, adjuntando el Anexo N° 1 "Ficha de acceso a servicios TI" que cuente con el V°B° de dicho jefe, donde se indica el nivel de acceso que requiere para el usuario, así como la justificación de dicha necesidad.

ii. Los niveles de acceso para la navegación a Internet son:

a) *Nivel I:* que puede ser a su vez:

- Nivel I con redes sociales: Acceso sin restricciones, en este nivel el usuario podrá hacer uso sin ningún tipo de limitaciones a la navegación hacia Internet, con excepción de lo señalado en el punto 1 del título "Prohibiciones del Servicio de Navegación".

  El jefe de cada unidad de organización que solicite este nivel para alguno de sus servidores, deberá justificar mediante Memorando dirigido al Jefe de la OTIGD, con copia a la Dirección General, las labores que realiza el personal a su cargo que requieren del acceso a redes sociales, como Facebook, twitter, Instagram entre otros.

- Nivel I sin Redes Sociales, en este nivel el usuario podrá hacer uso sin limitaciones a la navegación hacia internet, sin embargo no tendrá acceso a redes sociales como Facebook, Instagram, twitter, spotify, entre otros.

b) *Nivel II:* Acceso con restricciones, en este nivel se restringirá el acceso a páginas de video en línea (youtube), chat en línea, redes sociales, juegos, transmisiones de radio o tv por internet y lo señalado en el punto 1 del título "Prohibiciones del Servicio de Navegación".

c) *Nivel III:* Acceso Limitado, en este nivel solo se podrá acceder a las páginas de gobierno (.gob), paginas educativas (.edu), paginas militares (.mil), páginas de organismos no gubernamentales (.org), páginas de diarios e información. Todas las demás páginas quedaran restringidas, considerando lo señalado en el punto 1 del título "Prohibiciones del Servicio de Navegación".

En lo referente a páginas de diarios e información, si dicha página contiene un archivo multimedia o un enlace a un canal de videos como YouTube, no

se podrá visualizar los videos ya que ello está permitido únicamente en el Nivel I.

d) *Nivel IV:* Sin acceso, en este nivel solo se podrá acceder a las páginas internas institucionales como: Portal de la JNJ, Intranet, Extranet y otros que no requieran permisos de navegación hacia servidores externos.

iii. Cuando un usuario con acceso al servicio de Internet es dado de baja, la Unidad de Organización responsable deberá solicitar la desactivación del servicio a la OTIGD a través de un Memorando o correo electrónico, en lo posible el mismo día del cese de funciones del usuario.

iv. Los servicios de Internet deberán ser provistos a los usuarios de acuerdo a las necesidades específicas de la JNJ.

4.16. Auditoria y revisión del uso correcto de los servicios de Internet

i. El administrador de red, al verificar el funcionamiento y monitoreo del equipo firewall, detecta actividad inusual que ocasiona el incumplimiento de las políticas de navegación y/o la degradación del ancho de banda del Internet Institucional, procederá a identificar el equipo de cómputo que se encuentre efectuando dicha actividad. En estos casos el personal de Soporte Técnico de la OTIGD, en coordinación con el usuario que utiliza el equipo de cómputo en mención, realizaran las acciones necesarias para solucionar el problema detectado, informando de las mismas al Jefe de la OTIGD.

ii. En ocasiones que exista la necesidad de preservar el ancho de banda de Internet para el cumplimiento de las funciones oficiales de la JNJ como pueden ser: transmisiones de video streaming, envío de información como parte de los procesos de convocatorias u otros, el administrador de red estará facultado para bloquear el acceso a los servicios multimedia y redes sociales a la totalidad de usuarios de la institución sin previo aviso y hasta que la actividad oficial concluya.

iii. El Administrador de Red deberá incorporar en sus actividades la revisión selectiva de los reportes de incidentes de acceso o uso inadecuado de Internet.

V. ANEXOS:

- Anexo N° 01 – *Ficha de Acceso a Servicios de TI*

Anexo N° 01
Ficha de Acceso a Servicios de TI

Fecha	
Solicitante	
Unidad de Organización	

I. Solicitud					
Usuario Nuevo		Actualización Usuario		Desactivación de Usuario	
Nombre Usuario					
DNI					
Tipo de Contrato					

II. Accesos:					
Acceso a la Red		Correo Electrónico		Navegación a Internet	
Sistemas					
Sistema de Gestión Documental		Bandeja Personal		Bandeja Depedencia	
Intranet		Especificar Módulos:			
Extranet		Especificar Módulos:			
SIM		Especificar Módulos:			
SIGA					
SIAF					
STESO					
OTROS		Especificar Módulos:			

III. Unidades Compartidas: (Especificar las carpetas almacenadas en el storage que el usuario podrá tener acceso, señalar el tipo de acción por cada carpeta)					
Nombre Carpeta:					
Tipo de Acceso		Lectura		Escritura	
Nombre Carpeta:					
Tipo de Acceso		Lectura		Escritura	
Nombre Carpeta:					
Tipo de Acceso		Lectura		Escritura	
Nombre Carpeta:					
Tipo de Acceso		Lectura		Escritura	