Junta Nacional de Justicia

RESOLUCIÓN Nº 019-2023-DG-JNJ

San Isidro, 30 de marzo de 2023

VISTOS:

El Informe N° 000002-2023-OCA-OTIGD/JNJ de la Oficina de Tecnologías de la Información y Gobierno Digital, así como el Informe N° 000060-2023-OPCT/JNJ de la Oficina de Planificación y Cooperación Técnica, referidos a la propuesta de Lineamientos Técnicos para la Seguridad de la Información en la Junta Nacional de Justicia; y,

CONSIDERANDO:

Mediante Resolución Ministerial Nº 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática, a fin de establecer un sistema de gestión de seguridad de la información que permita conocer y manejar los riesgos asociados a los activos de información;

Mediante Resolución Ministerial Nº 246-2007-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de realizar la gestión de la seguridad de la información;

Mediante Resolución N° 020-2020-P-JNJ, se aprueba el Reglamento de Organización y Funciones de la Junta Nacional de Justicia, el mismo que en el artículo 71° establece las funciones de la Oficina de Tecnologías de la Información y Gobierno Digital, siendo una de ellas, la de planificar y ejecutar medidas de seguridad necesarias que permitan proteger la información, software y hardware, en concordancia con las políticas institucionales;

En el marco de sus funciones, la Oficina de Tecnologías de la Información y Gobierno Digital, ha elaborado los "Lineamientos Técnicos para la Seguridad de la Información en la Junta Nacional de Justicia", el cual permite establecer y ejecutar un sistema de gestión de seguridad de la información institucional;

La Oficina de Planificación y Cooperación Técnica, en el marco de sus competencias, ha validado los aspectos metodológicos y de diseño de los "Lineamientos Técnicos para la Seguridad de la Información en la Junta Nacional de Justicia"; en tal sentido, corresponde aprobar los lineamientos técnicos propuestos;

Firma Digital

Firmado digitalmente por SIFUENTES DEL MAR Rafael Nicolas FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.03.2023 15:55:34 -05:00

Firma Digital

Firmado digitalmente por ALVAREZ QUISPE Mario Alejandro FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.03.2023 15:27:13 -05:00

De conformidad con el inciso f) del numeral 1.2 de la Resolución N° 002-2023-P-JNJ, mediante el cual se ha delegado a la Dirección General la facultad para aprobar directivas y/o manuales, así como todo documento normativo, en el marco de sus competencias, por lo que, le corresponde emitir el acto administrativo que apruebe los referidos Lineamientos; y con el visado de las Oficinas de Planificación y Cooperación Técnica y de Asesoría Jurídica;

SE RESUELVE:

Artículo 1.- Aprobar los Lineamientos Técnicos para la Seguridad de la Información en la Junta Nacional de Justicia, cuyo texto en anexo, forma parte de la presente resolución.

Firma Digital

Firmado digitalmente por SIFUENTES DEL MAR Rafael Nicolas FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.03.2023 15:55:57 -05:00

Artículo 2.- Encargar a la Oficina de Planificación y Cooperación Técnica, la difusión de los Lineamientos Técnicos para la Seguridad de la Información en la Junta Nacional de Justicia, que se aprueba con la presente resolución, a las unidades de organización de la entidad.

Artículo 3.- Dejar sin efecto la Resolución N° 111-2019-DG-JNJ, que aprobó la Directiva N° 031-2019-DG/JNJ “Normas de Seguridad de la Información en la Junta Nacional de Justicia”.

Firma Digital

Firmado digitalmente por ALVAREZ QUISPE Mario Alejandro FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.03.2023 15:27:37 -05:00

Artículo 4.- Publicar la presente resolución en el portal de transparencia de la página electrónica y en el portal institucional de la Junta Nacional de Justicia (www.jnj.gob.pe).

Regístrese, comuníquese y archívese.

Firma Digital

Firmado digitalmente por MARRUJO ASTETE Betty Liliana FAU 20194484365 soft
Motivo: Soy el autor del documento
Fecha: 30.03.2023 17:15:41 -05:00

BETTY LILIANA MARRUJO ASTETE
DIRECTORA GENERAL
JUNTA NACIONAL DE JUSTICIA

Junta Nacional de Justicia

LINEAMIENTOS TÉCNICOS PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA JUNTA NACIONAL DE JUSTICIA

Concepto	Nombre y Apellido - Puesto	Firma	Fecha
Elaborado por:	Lily Susy Villalobos Melgarejo Oficial de Seguridad y Confianza Digital	Firma Digital Firmado digitalmente por VILLALOBOS MELGAREJO Lily Susy FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 28.03.2023 11:27:31 -05:00	En firma digital
Elaborado y Revisado por:	José Alarcón Butron 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: 28.03.2023 12:11:04 -05:00	En firma digital
Revisado por:	Rafael Sifuentes del Mar Jefe de la Oficina de Planificación y Cooperación Técnica	Firma Digital Firmado digitalmente por SIFUENTES DEL MAR Rafael Nicolas FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 29.03.2023 12:57:15 -05:00	En firma digital
Aprobado por:	Betty Liliana Marrujo Astete Directora General	Firma Digital Firmado digitalmente por MARRUJO ASTETE Betty Liliana FAU 20194484365 soft Motivo: Soy el autor del documento Fecha: 30.03.2023 17:15:51 -05:00	En firma digital

CONTROL DE CAMBIOS:

N°	FECHA	NUMERAL	TEXTO MODIFICADO	RESPONSABLE

I. OBJETIVO:

Establecer los lineamientos técnicos para la seguridad de la información en la Junta Nacional de Justicia que permita establecer los mecanismos para la protección de la confidencialidad, integridad y disponibilidad de la información en los diferentes procesos que se realizan en la entidad.

II. ÁMBITO DE APLICACIÓN:

El presente documento normativo es de cumplimiento obligatorio para todos los servidores civiles de la Junta Nacional de Justicia, que hacen uso de equipos de cómputo y efectúan labores de procesamiento de datos en la Junta Nacional de Justicia.

III. BASE LEGAL:

3.1 Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital y sus modificaciones

3.2 Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y se disponen las medidas para su fortalecimiento.

3.3 Decreto Supremo Nº 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Ley de Gobierno Digital.

3.4 Decreto Supremo Nº 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

3.5 Resolución N° 190-2020-JNJ que constituye el Comité de Gobierno Digital de la Junta Nacional de Justicia.

3.6 Resolución Ministerial N° 087-2019-PCM, aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.

3.7 Resolución Ministerial N° 004-2016-PCM y sus modificatorias, aprueba el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información.

3.8 Resolución Ministerial Nº 246-2007-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información.

3.9 Resolución de la Contraloría Nº 320-2006-CG, aprueba las Normas de Control Interno.

3.10 Resolución Jefatural N° 347-2001-INEI, aprueba la Directiva Nº 018-2001-INEI/DTNP “Normas y Procedimientos Técnicos para garantizar la Seguridad de la Información publicadas por las entidades de la Administración Pública”.

3.11 Resolución Jefatural Nº 076-95-INEI, aprueba la Directiva Nº 007-95-INEI/SJI “Recomendaciones Técnicas para la Seguridad e Integridad de la Información que se procesa en la Administración Pública”.

3.12 Resolución Jefatural Nº 090-95-INEI, aprueba la Directiva Nº 008-95-INEI/SJI "Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública".

3.13 Resolución N° 042-2019-DG-JNJ, que aprueba la "Política Institucional para la Administración de Software en la Junta Nacional de Justicia".

3.14 Resolución N° 039-2019-DG-JNJ, que aprueba la Directiva N° 004-2019-DG-JNJ "Normas para la Implementación, Administración y Empleo de Software en la Junta Nacional de Justicia".

IV. GLOSARIO DE TÉRMINOS:

Para los efectos del presente documento, se entiende por:

- **Accesos autorizados**: Autorizaciones concedidas a los usuarios para la utilización de los diversos recursos.
- **Activos a proteger**: Recursos del sistema de información o relacionados con éste, como software, sistemas operativos, hardware, sistemas de red, expedientes y archivos impresos, entre otros, necesarios para que la JNJ funcione correctamente y alcance los objetivos propuestos.
- **Amenazas**: Evento interno o externo que impiden y/o perjudican la confidencialidad, integridad y disponibilidad de la información.
- **Autenticación**: Procedimiento de comprobación de la identidad de un usuario.
- **Backups:** Copias de seguridad.
- **Centro de cómputo**: Es el lugar donde se encuentran los servidores informáticos y equipos de redes y telecomunicaciones.
- **Control de acceso**: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
- **Hardware:** Componentes materiales y físicos de un dispositivo.
- **Identificación**: Procedimiento de reconocimiento de la identidad de un usuario**.**
- **Impacto**: Daño producido a la organización por un posible incidente.
- **Proceso crítico**: Proceso que impacta significativamente la gestión institucional, tiene consecuencias de tipo legal, repercute negativamente en la atención al usuario y amenaza la sobrevivencia de la institución.
- **Riesgo**: Posibilidad de que se materialice una amenaza.
- **Sistemas de información**: Conjunto de archivos de datos automatizados, base de datos, programas, soporte y equipos, empleados para el almacenamiento y tratamiento de la información.
- **Software:** Conjunto de programas o aplicaciones, instrucciones y reglas informáticas.
- **Tecnología de información**: Software y hardware, sistemas operativos, sistemas de gestión de base de datos, sistemas de red.
- **Unidad de organización a cargo del sistema**: Es la unidad de organización responsable, que genera y procesa los datos involucrados de un sistema de información específico.

V. DISPOSICIONES GENERALES:

5.1 Declaración de Política de Seguridad de la Información:

La Junta Nacional de Justicia, reconoce la importancia de la información como activo valioso para sus procesos, por lo tanto, se compromete a asegurar su confidencialidad, integridad y disponibilidad mediante la gestión de riesgos, la promoción de una cultura organizacional en seguridad de la información, la implementación de infraestructura y tecnología acorde con las necesidades de la organización, en el marco legal y los estándares internacionales que permitan la continuidad de sus operaciones.

La Junta Nacional de Justicia, asume el compromiso de gestionar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) y otros requerimientos exigidos con relación a la seguridad de la información; y, en estricto cumplimiento de la protección de los datos personales, tanto del personal de la JNJ como de las personas involucradas en los procesos parte del alcance del SGSI, adecuándose a la normatividad vigente.

La Junta Nacional de Justicia, brinda comunicación oportuna de las políticas y procedimientos de seguridad de la información definidos, asegurando que sean comprendidos y se encuentren disponibles para todos los interesados.

5.2 Seguridad de la Información:

Es el conjunto de controles que establece una organización para proteger su información de un amplio rango de amenazas; y, se caracteriza por la preservación de:

a. La confidencialidad, asegura que sólo quienes estén autorizados tendrán acceso a la información.
b. La integridad, asegura que la información y los métodos de los procesos son exactos y completos;
c. La disponibilidad, asegura que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

5.3 Actores en la Gestión o Administración de Seguridad de la Información:

Unidad de Organización / Rol	Funciones
Pleno de la JNJ	- Constituye el Comité de Gobierno y Transformación Digital de la entidad, a través de acto resolutivo.
Presidencia de la JNJ	- Aprueba las políticas y normas de seguridad de la información de la institución
Comité de Gobierno y	- Dirigir, mantener, y supervisar el Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad.

Transformación Digital	
Oficial de Seguridad y Confianza Digital	- Coordinar la implementación y mantenimiento del SGSI en la entidad, atendiendo las normas en materia de seguridad digital, confianza digital y gobierno digita
Oficina de Tecnologías de la Información y Gobierno Digital (OTIGD)	- Brindar soporte operativo e implementar los mecanismos de seguridad de la información a los sistemas de información que se utilizan en la JNJ. - Identificar a la unidad de organización responsable de los sistemas de información y brindar soporte a los que se usen en la actualidad y a los nuevos que se incorporen a la JNJ. - Elaborar propuestas de manuales y/o instrumentos que coadyuven a la seguridad de la información en la JNJ, para protegerla de riesgos, amenazas y afrontar contingencias y desastres de todo tipo. - Supervisar el funcionamiento de los elementos de protección ambiental y eléctrica del Centro de Datos de la JNJ. - Realizar diariamente copias de seguridad (Backups) del ambiente de producción en forma automática y manual, y almacenarlas en un lugar o ambiente externo a la Entidad, ante cualquier caso de desastre.
Área de Comunicación e Imagen Institucional	- Registrar a los visitantes que ingresen a la Entidad (nombre y apellidos del visitante, documento de identificación, hora de ingreso, razón de la visita, persona o área visitada y hora de salida), a través de las personas encargadas de recepción.
Director(a) /Jefe(a) /Ejecutivo(a) de unidad de organización	- Custodiar la documentación que sustenta o fundamenta los registros en los sistemas como: expedientes, informes, reportes y otros documentos físicos. - Administrar los activos de información, que están bajo su responsabilidad funcional. Asimismo, asumir la responsabilidad de los sistemas de información de la JNJ, bajo el detalle indicado en el Anexo N° 1 del presente documento. Clasificar y reclasificar la información que administra de acuerdo a la tipología establecida y sus funciones y atribuciones. - almacenar en áreas separadas y seguras, la información clasificada como altamente sensible (secreta o reservada). - responsable de la eliminación de información clasificada como confidencial, la cual debe ser en forma segura y definitiva.
Servidores Civiles (en general)	- Ser responsable de la información registrada en los sistemas de información de la JNJ, al que tiene usuario de acceso. - Adoptar la política de escritorios limpios, la cual considera que al culminar la jornada de trabajo, deben guardar los documentos e información de la JNJ en

	estantes, cajones o lugares adecuados, evitando dejarlos encima del escritorio. - Usar la cuenta de correo institucional asignado a cada servidor civil será usada para comunicar o recibir mensajes relacionados a la actividad laboral de la Entidad y no para fines particulares. - Evitar poner en riesgo la información de la JNJ, por acción u omisión, considerando que será calificada como falta. **Nota:** Al incurrir en dicho suceso, se procederá como lo establece el artículo 103° del Reglamento Interno de Servidores Civiles de la JNJ.

VI. DISPOSICIONES ESPECÍFICAS:

6.1 Clasificación de Activos de Información:

a. La JNJ es propietaria de la información que genera y administra, a través de los servidores civiles mediante la utilización de equipos de cómputo, telefonía u otros, considerándola como un activo intangible vital, por lo que debe ser protegido y custodiado. La información es clasificada por su nivel de confidencialidad o importancia, bajo las siguientes denominaciones:

- "Público": Información que por su contenido es de carácter público y de libre acceso tanto para usuarios internos como externos.
- "Uso Interno": Información que solo es de valor para los usuarios internos de la entidad y que son utilizados para el desarrollo de sus procesos.
- "Confidencial, Secreta o Reservada": Esta información, plasmada en documentos que se encuentran en poder de la Entidad, no puede ser divulgada, publicada, sustraída, utilizada o reproducida por cualquier medio, sin la debida autorización suscrita o por medio electrónico. Esta prohibido violar el secreto de la documentación considerada bajo esta clasificación.

b. Para conocer la clasificación de la información, la unidad de organización que genera o administra debe etiquetarla o signarla, para su identificación y control; se puede utilizar etiquetas físicas o codificación electrónica, según sea la naturaleza de la información.

6.2 Seguridad Física y Ambiental:

a. El Jefe (a) del Área de Comunicación e Imagen Institucional, a través de las personas encargadas de recepción, es responsable del registro de todos los visitantes que ingresen a la institución (nombre y apellidos del visitante, documento de identificación, hora de ingreso, razón de la visita, persona o área visitada y hora de salida).

b. El acceso físico al Centro de Datos de la JNJ, requiere de la autorización de la OTIGD; quienes ingresen al ambiente de servidores lo harán, bajo un control adecuado y acompañado de un servidor civil que designe el Jefe de la OTIGD.

c. La gestión del Centro de Datos seguirá los estándares técnicos determinados para su protección ambiental y eléctrica considerando los siguientes equipos: aire acondicionado con funcionamiento constante, extintores de mano, UPS (Uninterruptable Power Supply, en español Sistema de Alimentación Ininterrumpida - SAI), detector de fuego y humo, entre otros. Además, los equipos de cómputo deben estar protegidos ante fallas de suministros de energía u otras anomalías eléctricas (estabilizadores de voltaje, pozo de línea a tierra); el cableado de telecomunicaciones y energía deben estar separados y protegidos mediante canaletas o ductos que impidan interceptaciones o daños. Se debe respetar las medidas de seguridad.

6.3 Mantenimiento de Equipos y Redes de Computo:

a. Los equipos y redes de cómputo de la JNJ contarán con un mantenimiento preventivo anual como mínimo para asegurar su disponibilidad e integridad; La OTIGD debe de verificar que no exista riesgos de fuga de información al momento de realizarse los mantenimientos preventivos.

6.4 Gestión de Operaciones de los Sistemas de Información:

Cada uno de los equipos informáticos son asignados a un funcionario o servidor responsable, quien deberá hacer buen uso de los mismos.

a. Para la administración de los sistemas de información, la OTIGD utilizará tres (03) servidores o ambientes de almacenamiento, cada uno en exclusividad según su uso:

   - Ambiente de desarrollo (sistemas y base de datos en fase de diseño)
   - Ambiente de pruebas (sistemas y base de datos en fase de pruebas por el usuario)
   - Ambiente de producción (sistemas y base de datos de uso oficial).

b. Los sistemas de información que se desarrollaron para las diferentes unidades de organización de la JNJ son propiedad de la Entidad; cada sistema de información se registrará como propiedad intelectual de la JNJ, ante las entidades públicas o privadas que correspondan.
c. Cuando la JNJ realice la compra de licencia de uso de programas de software, la Oficina de Administración y Finanzas (OAF), a requerimiento de la OTIGD, celebrará contratos de mantenimiento de licencias de software

por periodos de tiempo renovables, según la disponibilidad del servicio y la normatividad vigente, que corresponda.

d. Los cambios efectuados y/o traslados de los equipos de cómputo (hardware y software) por una unidad de organización, será informado y autorizado por el Director(a), Jefe(a) o Ejecutivo(a), según corresponda, a la OTIGD, quién comunica a la Unidad de Abastecimiento para su actualización en la asignación de bienes patrimoniales.
e. El acceso a páginas web que no guarden relación con la labor que realiza el servidor civil como de mensajería electrónica (MSN, etc.), música y video, está prohibido, salvo que se presente ante la OTIGD la autorización emitida por el Director(a), Jefe(a) o Ejecutivo(a) de la unidad de organización donde labore el servidor civil.

6.4.1 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital debe realizar las pruebas correspondientes para mantener la integridad de la seguridad interna de la red de datos.

6.4.2 Los servidores de la JNJ y/o las personas ajenas a la institución que requieran ingresar a la sede equipos de almacenamiento de información (laptop, computadoras y otros), que no sean de propiedad de la JNJ, deben solicitar su ingreso por escrito a la Oficina de Administración y Finanzas quien lo remite a la Unidad de Control Patrimonial para conocimiento y registro.

6.4.3 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital es el responsable de la administración técnica y operativa de la base de datos en el ambiente de producción. No puede realizar el pase al ambiente de producción de sistemas y realizar modificaciones sin la autorización de la unidad de organización a cargo del sistema.

6.4.4 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital es el responsable de la administración técnica y operativa de la base de datos institucional y la unidad de organización a cargo del sistema es el responsable de la administración funcional del mismo. El trabajador encargado por la Oficina de Tecnologías de la Información y Gobierno Digital no puede modificar la base de datos de un sistema sin autorización previa de la unidad de organización a cargo del mismo.

6.4.5 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital debe instalar y administrar el programa de software antivirus a todos los equipos de cómputo, a fin de prevenir y eliminar la infección de virus informáticos. Dicho antivirus es actualizado constantemente.

6.4.6 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital debe mantener todos los programas de software en todos los equipos de cómputo de la Institución con las últimas actualizaciones de seguridad disponibles.

6.4.7 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital es el responsable de autorizar el uso de programas de software a todos los usuarios de la JNJ. Está prohibido el uso de programas de software no autorizado por la Oficina de Tecnologías de la Información y Gobierno Digital.

6.5 Control de accesos a los sistemas informáticos

6.5.1 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital es el responsable de proporcionar el servicio de acceso a los sistemas de información solo con la autorización de la unidad de organización a cargo del sistema. El acceso al sistema será basado en un perfil de acceso (solo consulta, solo modificación, acceso parcial o total del sistema).

6.5.2 Los usuarios son los responsables de mantener la custodia y confidencialidad de las cuentas de usuario y contraseñas que son puestos a su disposición por la JNJ para identificarlos o reconocer las atribuciones de acceso o manipulación de información que se les haya asignado.

6.5.3 Todos los sistemas informáticos que se implementen en la Institución tienen un sistema de autenticación (usuario y contraseña).

6.5.4 El usuario, con apoyo del servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital, debe activar contraseña de encendido y contraseña de protector de pantalla, a fin de prevenir el acceso no autorizado.

6.5.5 El servidor trabajador encargado por la Oficina de Tecnologías de la Información y Gobierno Digital es responsable de que el acceso a las librerías de los programas fuente de los sistemas de información sean adecuadamente restringidos y controlados, a fin de minimizar el daño o alteración no autorizada de los programas.

6.5.6 Toda modificación de datos en los sistemas de información debe permitir que se almacene los datos del usuario que lo realiza.

6.5.7 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital, establece un conjunto de controles de seguridad en

las redes de computadoras, para garantizar la seguridad de los datos en las redes y la protección de los servicios conectados de los accesos no autorizados.

6.5.8 Todos los contratos, convenios y otros instrumentos que impliquen acceso a la información de la JNJ, deben ser autorizados por el Comité de Gobierno Digital, para lo cual deben establecer los controles que se norman en el presente documento, y otros que se consideren necesario.

6.6 Desarrollo y mantenimiento de sistemas informáticos

6.6.1 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital debe asegurar la aplicación de estándares de procedimientos y controles de seguridad en el ciclo de vida de desarrollo de sistemas.

6.6.2 El ingreso de datos a los sistemas de información debe ser validado por la unidad de organización a cargo del procedimiento, a efectos de garantizar que éstos sean correctos y apropiados.

6.6.3 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital es responsable de que los datos procesados por los sistemas de información cuenten con procedimientos de validación.

6.6.4 Los procedimientos para el desarrollo de sistemas, mantenimiento y pruebas deben ser documentados.

6.7 Administración de la Continuidad de los sistemas de información

El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital elabora y actualiza en forma permanente un plan de contingencia que permita que la información esté disponible (aún en situaciones de desastre), que posibilite la continuidad de los procesos críticos de la institución.

6.8 Programas preparatorios y de control

6.8.1 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital debe capacitar al personal, según sus responsabilidades y necesidades específicas, en los aspectos que posibiliten o contribuyan a una mejor aplicación y observación del presente documento.

6.8.2 El Jefe de la Oficina de Tecnologías de la Información y Gobierno Digital es responsable, en lo que corresponda a su competencia, de establecer y hacer cumplir procedimientos formales que aseguren que las normas

legales, contractuales o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

6.8.3 Los recursos de tecnología de información de la JNJ deben ser usados únicamente para los propósitos autorizados de la institución, de lo contrario se considera como uso inapropiado de los recursos, debiendo aplicarse las medidas disciplinarias correspondientes.

6.8.4 El servidor encargado por la Oficina de Tecnologías de la Información y Gobierno Digital debe revisar periódicamente todos los sistemas de información a fin de garantizar el cumplimiento de las políticas y estándares de seguridad de la JNJ.

VII. ANEXOS:

Anexo N° 1
Unidades de organización responsables de la aplicación de los principales sistemas de información de la JNJ

SISTEMAS DE INFORMACIÓN	UNIDAD DE ORGANIZACIÓN RESPONSABLE DEL SISTEMA DE INFORMACIÓN	RESPONSABLE DEL ARCHIVO INFORMÁTICO
Sistema de Selección y Nombramiento	Dirección de Selección y Nombramiento	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema Ficha Única	Dirección de Selección y Nombramiento, Dirección de Evaluación y Ratificación	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Procesos Disciplinarios	Dirección de Procedimientos Disciplinarios	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Registro de Jueces y Fiscales	Área de Registro de Jueces y Fiscales	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Administración de Solicitudes de Acceso a la Información Pública	Área de Acceso a la Información Pública	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Casilla de Notificaciones	Dirección de Selección y Nombramiento, Dirección de Evaluación y Ratificación, Dirección de Procedimientos Disciplinarios	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Recursos Humanos	Área de Recursos Humanos	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Tesorería	Área de Tesorería	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Boletín Oficial de la Magistratura	Secretaría General	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Compendio Normativo	Oficina de Asesoría Jurídica	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema Integrado de Administración Financiera (SIAF)	Oficina de Administración y Finanzas	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema Integrado de Gestión Administrativa (SIGA), que usa Logística y Recursos Humanos	Oficina de Administración y Finanzas	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Mesa de Partes Virtual	Área de Atención al Usuario y Trámite Documentario	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Trámite Documentario	Área de Atención al Usuario y Trámite Documentario	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Registro de envío de documentos externos	Área de Atención al Usuario y Trámite Documentario	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Secretaría General	Secretaría General	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Información Plan Operativo Institucional	Oficina de Planificación y Cooperación Técnica	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Información Estadístico	Oficina de Planificación y Cooperación Técnica	Oficina de Tecnologías de la Información y Gobierno Digital
Aplicativo CEPLAN	Oficina de Planificación y Cooperación Técnica	Dirección Nacional de Coordinación y Planeamiento CEPLAN
Aplicativo del Sistema Presupuestario	Oficina Presupuesto	DNPP del MEF – Oficina de Tecnologías de la Información

SISTEMAS DE INFORMACIÓN	UNIDAD DE ORGANIZACIÓN RESPONSABLE DEL SISTEMA DE INFORMACIÓN	RESPONSABLE DEL ARCHIVO INFORMÁTICO
Sistema de Información Gerencial	Oficina de Tecnologías de la Información y Gobierno Digital	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Imagen	Área de Comunicaciones e Imagen	Oficina de Tecnologías de la Información y Gobierno Digital
Portal Web Institucional	Área de Comunicación e Imagen	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Información Jurídica (SPIJ)	Oficina de Tecnologías de la Información y Gobierno Digital	Oficina de Tecnologías de la Información y Gobierno Digital
Sistema de Asignación Aleatoria de Expedientes para Revisión por Miembros de la JNJ	Pleno de la Junta Nacional de Justicia	Oficina de Tecnologías de la Información y Gobierno Digital