



Comité de Transparencia
Unidad de Transparencia



HACIA UNA JUSTICIA HUMANA,
EFICIENTE Y TRANSPARENTE

DOCUMENTO DE SEGURIDAD

PODER JUDICIAL DEL ESTADO DE OAXACA

Unidad de Transparencia

Diciembre 2021

Correo electrónico:
utransparenciapjeo@hotmail.com y
unidaddetransparencia@tribunaloaxaca.gob.mx

Conmutador (951)5016680
Extensión 31270, 31271 y 31262
FAX 31275

Av. Gerardo Pandal Graf No. 1, Edificio J", segundo nivel, Ciudad Judicial,
Agencia de Policía Reyes Mantecón, San Bartolo Coyotepec, Oax.



Tabla de contenido

1. Introducción	3
2. Glosario	5
3. El deber de seguridad	9
4. El inventario de datos personales y	10
de los sistemas de tratamiento	10
5. Análisis de riesgo, de brecha	12
y plan de trabajo	12
5.1. Plan de trabajo	13
6. Revisión y Vigilancia	15

Anexos

Anexo 1. Catálogo de sistemas de datos personales e inventario

Anexo 2. Análisis de riesgo, de brecha y planta trabajo

Anexo 3. Revisión y Vigilancia



1. Introducción

El Poder Judicial del Estado de Oaxaca en el marco constitucional que protege el **derecho de acceso a la información**¹ tiene la calidad de sujeto obligado y como obligación transparentar toda la información que genera conforme a sus facultades, atribuciones y competencias; sin embargo, la misma normativa que garantiza este derecho lo sujeta a límites explícitos, es decir, no tiene un alcance absoluto pues se convertiría en una prerrogativa con rasgos ilícitos o abusivos, siendo el límite de esta garantía la **protección a la vida privada y los datos personales**.

Página | 3

Esta limitante, considerada también un derecho humano está garantizada en el derecho internacional como obligación y deber del Estado Mexicano de respetarlo y protegerlo en los artículos 12 de la Declaración Universal de los Derechos del Hombre; 17 del Pacto Internacional de los Derechos Civiles y Políticos, y 11 de la Convención Americana de Derechos Humanos.

Por su parte, la legislación mexicana a través de las reformas Constitucionales de 2009 y 2014, establece la protección a la vida y a los datos personales, como un derecho fundamental en los numerales 6, Apartado A, fracción II y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos. Derivado de lo anterior, en 26 de enero de 2017 nace la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO) y para el estado de Oaxaca el 19 de diciembre de 2020 se publica la reforma a la ley en materia de datos personales homologada a la general.

La Ley General en el capítulo II, "De los Deberes" establece la obligación de implementar y mantener medidas de seguridad de carácter administrativo, físico y técnico que permitan proteger contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, la información referente

¹ Artículo 6, Apartado A de la Constitución Política de los Estados Unidos Mexicanos



a la vida privada y los datos personales garantizando así su confidencialidad, integridad y disponibilidad, de la misma manera se establece lo propio en la Ley local.

Po lo anterior, el **Poder Judicial del Estado de Oaxaca** con fundamento en los artículos 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 27 de Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Oaxaca, elabora el documento de seguridad que tiene por objeto garantizar las correctas medidas de seguridad mínimas indispensables que deben considerarse conforme a la legislación aplicable, evitando vulneraciones a los sistemas administrativos, físicos y técnicos que afecten la esfera de otros derechos y libertades fundamentales de las personas cuya información a la vida privada y datos personales custodia este ente público.



2. Glosario²

I. Bases de Datos: Conjunto ordenado de datos personales referentes a una persona física, identificada o identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

II. Comité de Transparencia: Comité de Transparencia del Poder Judicial del Estado de Oaxaca a que se refieren los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública, el Título Cuarto de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno para el Estado de Oaxaca y demás aplicables de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca;

III. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

IV. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

V. Documento: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus Servidores Públicos e integrantes, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;

² Las definiciones aquí contenidas provienen de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca, Ley General de Transparencia y Acceso a la Información Pública y Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno para el Estado de Oaxaca.



VI. Documento Electrónico: Información que puede constituir un documento, archivada o almacenada en un soporte electrónico, en un formato determinado y susceptible de identificación y tratamiento;

VII. Documento de archivo: Información contenida en cualquier soporte y tipo documental, producida, recibida y conservada por cualquier organización o persona en ejercicio de sus competencias o en el desarrollo de su actividad;

VIII. Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

IX. Expediente: Unidad documental constituida por uno o varios documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados;

X. Expediente electrónico: Es el conjunto de documentos electrónicos cuyo contenido y estructura permiten identificarlos como documentos de archivo que aseguran la validez, autenticidad, confidencialidad, integridad y disponibilidad de la información que contienen;

XI. Información: La contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título, o bien aquella que por una obligación legal deban generar;

XII. Información Confidencial: La información en posesión de los sujetos obligados, que refiera a la vida privada y/o los datos personales, por lo que no puede ser difundida, publicada o dada a conocer, excepto en aquellos casos en que así lo contemple la presente Ley y la Ley de la materia;

XIII. Ley de Datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca;

XIV. Ley de Transparencia: Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno para el Estado de Oaxaca;

XV. Ley General de Datos: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;



XVI. Ley General de Transparencia: Ley General de Transparencia y Acceso a la Información Pública;

XVII. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

XVIII. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

XIX. Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

XX. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;



- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
- d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

XXI. Medio Electrónico: Sistema electrónico de comunicación abierta, que permite almacenar, difundir o transmitir documentos, datos o información;

XXII. Servidores Públicos: Los mencionados en el párrafo primero del artículo 108 de la Constitución Política de los Estados Unidos Mexicanos; 115 de la Constitución Política del Estado Libre y Soberano de Oaxaca y en la Ley de Responsabilidades de los Servidores Públicos del Estado y Municipios de Oaxaca;

Página | 8

XXIII. Responsable: Los sujetos obligados a que se refieren los artículos 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 1, párrafo quinto de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca, es decir, Poder Judicial del Estado de Oaxaca para efectos del presente documento;

XXIV Unidad de Transparencia: Instancia a la que hace referencia los preceptos 45 de la Ley General de Transparencia y Acceso a la Información Pública y 68 Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno para el Estado de Oaxaca;

XXV. Titular: La persona física a quien corresponden los datos personales.



3. El deber de seguridad

El deber de seguridad encuentra su fundamento en los artículos 31 de la Ley General de Datos y 24 de la Ley de Datos, como una obligación del responsable de implementar medidas de seguridad físicas, técnicas y administrativas para proteger los datos personales, datos personales sensibles o información confidencial contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no autorizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad se traducen en un conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales, datos personales sensibles e información confidencial (artículos 3, fracción XIV de la Ley General de Datos; 3, fracción XXIII de la Ley de Datos e inciso XVIII del glosario del presente documento de seguridad).

En este aspecto el Poder Judicial del Estado de Oaxaca como sujeto obligado responsable de proteger los datos personales, datos personales sensibles e información confidencial que trata a través de las unidades administrativas, Dirección de Administración del Consejo de la Judicatura y Dirección de Escuela Judicial del Consejo de la Judicatura, contenidos en su orden, en los sistemas "SysRH" y "Carrera Judicial", ha implementado las medidas de seguridad **administrativas, físicas y técnicas** para prevenir el acceso, pérdida, destrucción, uso, tratamiento, daño, alteración y modificación no autorizados de esta información, las cuales están obligadas a observar durante todo el ciclo de vida de los datos personales, desde su obtención hasta su eliminación.

Estas medidas de seguridad se materializan a través de acciones documentadas y contenidas en los sistemas de gestión, interrelacionados que permiten establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales conforme lo exigen las normas de la materia para dar cabal cumplimiento al derecho humano a la protección a la vida privada y datos personales que tutelan los artículos 6, Apartado A, fracción II y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos.

En tal virtud la Unidad de Transparencia del Poder Judicial del Estado de Oaxaca, en franca colaboración con las unidades administrativas, Dirección de Administración del Consejo de la Judicatura y Dirección de Escuela Judicial del Consejo de la Judicatura, estructuraron el presente documento de seguridad aprobado por el Comité de Transparencia, y que da cabal cumplimiento a los artículos 35 de la Ley General de Datos y 27 de Ley de Datos.



4. El inventario de datos personales y de los sistemas de tratamiento

Como una primera exigencia de la Ley General de Datos y Ley de Datos, establece que el responsable en el documento de seguridad que elabore debe contener el inventario de los datos personales y de los sistemas de tratamientos que tratan información relativa a los datos personales, datos personales sensibles e información confidencial custodiada por el responsable a través de las unidades administrativas, Dirección de Administración del Consejo de la Judicatura y Dirección de Escuela Judicial del Consejo de la Judicatura.

Página | 10

Este primer momento de suma relevancia pues permite conocer a exactitud el nombre, cargo, funciones y obligaciones de los usuarios servidores públicos que tratan datos personales, mismos que son los encargados de implementar y aplicar el conjunto de acciones, actividades, controles y mecanismos administrativos, técnicos y físicos que protegen la información relativa a la vida privada y a los datos personales a través de las medidas de seguridad existentes.

Así también dentro de las funciones y obligaciones de los usuarios servidores públicos que tratan datos personales se encuentra la obligación de informar sin dilación alguna al responsable las vulneraciones a los sistemas de gestión que contienen la información sobre la que trata el presente documento consistentes en usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida dicha información que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

Así también el inventario que realizó el responsable ha permitido identificar el tipo de soporte del sistema con los que cuentan los sistemas de gestión "SysRH" y "Carrera Judicial" conformados por bases de datos, documentos, documentos electrónicos, documentos de archivo, expedientes, expedientes electrónicos y medios electrónicos.

En el presente documento en el **Anexo 1, Catálogo de sistemas de datos personales e inventario** ha quedado definido además las finalidades del tratamiento de la información a la vida privada y datos personales que recaban las unidades administrativas, Dirección de Administración del Consejo de la Judicatura y Dirección de Escuela Judicial del Consejo de la Judicatura, el ciclo de vida de la información, así como los medios de identificación y autenticación para el acceso autorizado a la información, así como el catálogo respectivo.



En tal virtud, para dar cumplimiento al artículo 33 fracciones II y III de la Ley General de Datos y al similar 26, fracciones II y III de la Ley de Datos en el anexo del presente capítulo, contiene la información a detalle del manejo y acceso a los sistemas de gestión del responsable, integrado un 50% por la unidad administrativa Dirección de Administración del Consejo de la Judicatura, respecto al sistema "SysRH" y el otro 50% de la unidad administrativa Dirección de Escuela Judicial del Consejo de la Judicatura, relativo al sistema "Carrera Judicial", en el que se definen las funciones y obligaciones de la manera siguiente:

Anexo 1, Catálogo de sistemas de datos personales e inventario

- 1.1. Denominación de la Unidad Administrativa
- 1.2. Funciones de los servidores públicos que tratan datos personales
- 1.3. Inventario

Anexo 1.1. Otros usuarios



5. Análisis de riesgo, de brecha y plan de trabajo

Considerado el derecho a la protección a la información a la vida privada y datos personales un derecho humano reconocido a nivel internacional y garantizado en la Carta Magna en los artículos 6, Apartado A, fracción II y segundo párrafo del 16, las leyes que lo regulan consideran de vital importancia que el responsable pueda de manera fehaciente identificar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.

Página | 12

Por lo que, los preceptos 33 fracciones IV, V y VI de la Ley General de Datos y el similar 26, fracciones IV, V y VI de la Ley de Datos, exigen que, para identificar una amenaza y evitar una vulneración a los sistemas que contienen datos personales se realice una análisis de riesgo y brecha, para estar en posibilidad de implementar un plan trabajo que permita de ser necesario corregir, o en su caso, reforzar las medidas de seguridad que protejan en su totalidad la información relativa a la vida privada y datos personales que trata.

Pero **¿Qué es una vulneración?** es un incidente de seguridad de la información que afecta la información a la vida privada y los datos personales en cualquier fase de tratamiento, la Ley General de Datos³ y la Ley de Datos⁴, consideran cuatro tipos de vulneraciones de seguridad:

- I. La pérdida o destrucción no autorizada;
- II. El robo, extravío o copia no autorizada;
- III. El uso, acceso o tratamiento no autorizado, o
- IV. El daño, la alteración o modificación no autorizada

Así también dicha normativa establece el proceso⁵ a seguir en caso de que surja una vulneración, adicionalmente el numeral 163, fracción III de la Ley General de Datos y el 115, fracción III de la Ley de Datos, establecen como causas de responsabilidad e infracción a la información a la vida privada y datos personales la de usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión, los cuales de

³ Artículo 38

⁴ Artículo 29

⁵ Artículo 37, 39, 41 y 40 de la Ley General de Datos y 29, párrafos segundo y tercero y 30 de la Ley de Datos.



sucedan pueden derivar en procesos administrativos o del orden civil, penal o de cualquier otro tipo que puedan resultar de la amenaza, vulneración, incidente o infracción.

El responsable, para identificar de manera adecuada cualquier tipo de amenaza, vulneración, incidente o infracción a la información en materia de datos personales que trata a través de las unidades administrativas, Dirección de Administración del Consejo de la Judicatura y Dirección de Escuela Judicial del Consejo de la Judicatura en las bases de datos que conforman los sistemas de gestión, en su orden, "SysRH" y "Carrera Judicial", aplicó el método Montecarlo⁶, técnica matemática que se emplea para realizar un análisis cuantitativo de riesgos y toma de decisiones.

En el **Anexo 2. Análisis de riesgo, de brecha y planta trabajo**, arroja los resultados respecto a las posible vulneraciones a las que están expuestos las bases de datos que conforman los sistemas de gestión "SysRH" y "Carrera Judicial" respecto a la pérdida (P); destrucción (DE); uso (U); acceso (AC); tratamiento (T); daño (DA); alteración (AL) y modificación (M) no autorizadas. Relacionado con la información confidencial y el personal involucrado en el tratamiento de la misma, así como las medidas como acciones (A); actividades (AD); mecanismos administrativos (MA); mecanismos técnicos (MT); mecanismos físicos (MF); relacionados con la información confidencial y el personal involucrado en el tratamiento de la misma.

5.1. Plan de trabajo

La Procuraduría Federal de la Defensa del Trabajo de manera atinada cita que *"La capacitación juega un papel primordial para el logro de tareas y proyectos, dado que es el proceso mediante el cual las y los trabajadores adquieren los conocimientos, herramientas, habilidades y actitudes para interactuar en el entorno laboral y cumplir con el trabajo que se les encomienda"*.

Por lo anterior, y atendiendo al resultado del análisis de riesgo y brecha, del que se observa un número considerable de servidores públicos que intervienen en el tratamiento de la información relativa a la vida privada y datos personales, resulta indispensable implementar un programa de capacitación constante en materia de datos personales, pero además de acceso a la información para que tengan pleno conocimiento y capacidad para que puedan determinar al momento en que se requiere acceder a la información que tratan o en su caso protegerla.

⁶ Economía Excel. Modelos y aplicaciones Excel para la economía y la gestión de empresas, 2019.



En tal virtud, como plan de trabajo se establece un programa de capacitación constante a los servidores públicos que tratan información a la vida privada y datos personales en las bases de datos que conforman los sistemas de gestión "SysRH" y "Carrera Judicial", capacitación en cualquiera de sus versiones: cursos, talleres, conferencias, congresos, diplomados.

Acciones que en su conjunto tiene como finalidad capacitar y profesionalizar a los servidores públicos que tratan datos personales, adquiriendo conocimientos teóricos y prácticos para actualizar sus conocimientos, adquieran nuevos y fortalezcan su capacidad de respuesta ante los cambios del entorno o de sus requerimientos laborales, así como la necesidad de resguardar la información que tratan, por medio de reglas claras que otorga la Ley General de Transparencia, Ley de Transparencia, Ley General de Datos y Ley de Datos, mismas que dotan de un equilibrio necesario entre transparencia y acceso a la información pública y protección a la información a la vida privada y datos personales, los cuales se programaran durante 10 meses de cada año de forma tal que lo permitan las actividades laborales de cada servidor público y unidad administrativa.

5.1. Plan de trabajo para reducir el riesgo y las brecha de vulnerabilidades

Capacitaciones, cursos, talleres, conferencias, congresos, diplomados										
Unidad Administrativa responsable	ENE	FEB	MAR	ABR	MAY	JUN	AGO	SEP	OCT	NOV
Dirección de Administración	*	*	*	*	*	*	*	*	*	*
Escuela Judicial	*	*	*	*	*	*	*	*	*	*



6. Revisión y Vigilancia

Monitorear, revisar y vigilar el cumplimiento a las medidas de seguridad administrativa, física y técnica de acuerdo con la legislación de protección de datos personales, es un deber de los servidores públicos que tratan información a la vida privada y datos personales en las bases de datos que conforman los sistemas de gestión "SysRH" y "Carrera Judicial".

Por ello, dichos servidores públicos monitorean, revisan y vigilan de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente:

- a) La nueva información que se incluyan en la gestión de riesgos;
- b) Las modificaciones a los sistemas como el cambio o migración tecnológica, entre otras;
- c) Las nuevas amenazas activas dentro y fuera del sujeto obligado
- d) La posibilidad de nuevas vulnerabilidades o incrementen las existentes
- e) Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- f) El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- g) Los incidentes y vulneraciones de seguridad ocurridas.

Es así que en el **Anexo 3. Revisión y Vigilancia** se establece la temporalidad de monitoreo, revisión y vigilancia de ambos sistemas respecto a los soportes físicos y electrónicos respecto a las amenazas y vulneraciones a las que están sujetos los sistemas que tratan datos personales, como lo son pérdida (P); destrucción (DE); uso (U); acceso (AC); tratamiento (T); daño (DA); alteración (AL) y modificación (M) no autorizadas.

De igual forma en el mismo **anexo 3**, definen la periodicidad en la que monitorea, revisa y vigila las medidas de seguridad implementadas relativa a (A); actividades (AD); mecanismos administrativos (MA); mecanismos técnicos (MT); mecanismos físicos (MF) en los soportes físicos y electrónicos de los sistemas.

Todo lo anterior con la finalidad de tratar la protección de datos contra accesos no autorizados y protegerlos de una posible amenaza, vulneración, incidente o infracción durante todo su ciclo de vida.



Anexo 1 Catálogo de sistemas de datos personales e inventario



1.1. Denominación de la Unidad Administrativa
 Dirección de Administración del Consejo de la Judicatura

Nombre del sistema
 SysRH

Responsable [A que se refiere el artículo 1, párrafo quinto y 3, fracción XXVIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados]
 Poder Judicial del Estado de Oaxaca

Nombre:
 Mag. Eduardo Pinacho Sánchez

Cargo:
 Magistrado Presidente

Usuarios
 Carrera Judicial

Dirección de Escuela Judicial del Consejo de la Judicatura

1.2. Funciones de los servidores públicos que tratan datos personales

Nombre [Usuario 1]:
Mtro. Guillermo Trejo Carbajal

Cargo:
 Director de Administración

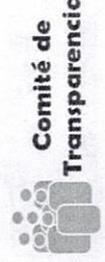
Nombre [Usuario 2]:
Mtro. Héctor Humberto Vásquez Quevedo

Cargo:
 Director de la Escuela Judicial

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Administrar el uso de los recursos humanos, materiales y servicios generales del Poder Judicial o de aquellos que estén al cuidado y custodia del mismo, en términos del artículo 82 de la Ley Orgánica del Poder Judicial del Estado de Oaxaca y 128 del Reglamento Interno del Consejo de la Judicatura del Estado de Oaxaca; 14 y 15 del Reglamento de la Escuela Judicial del Consejo de la Judicatura del Estado de Oaxaca.

Seleccionar, formar, capacitar, actualizar y perfeccionar continuamente a los magistrados, jueces y demás servidores públicos que integren el Poder Judicial, conforme a los artículos 70, fracción VII, 93, y 95 fracciones I, V, XII y XIV, de la Ley Orgánica del Poder Judicial del Estado de Oaxaca; y 142, fracciones IV y V, del Reglamento Interior del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca; 14 y 15 del Reglamento de la Escuela Judicial del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca.





Anexo 1

Catálogo de sistemas de datos personales e inventario



Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Implementar las medidas tendientes a la adecuada administración y resguardo de los recursos humanos, materiales y servicios generales del Poder Judicial o de aquellos que estén al cuidado y custodia del mismo, en términos del artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Implementar acciones educativas de los programas de formación direccionadas a las y los servidores públicos del Poder Judicial, como lo establecen los artículos 70, fracción VII, 93, y 95 fracciones I, V, XII y XIV, de la Ley Orgánica del Poder Judicial del Estado de Oaxaca; y 142, fracciones IV y V, del Reglamento Interior del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca; 14 y 15 del Reglamento de la Escuela Judicial del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores públicos que trate datos personales]

Funciones, obligaciones y cadena de mando	Si	Funciones, obligaciones y cadena de mando	Si
Información sobre el tratamiento	Si	Información sobre el tratamiento	Si
Capacitación	Si	Capacitación	Si

Nombre [Usuario 2]:

L.A. Laurencio Fernando Velasco Dominguez

Cargo:

Jefe de la Unidad de Recursos Humanos

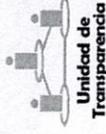
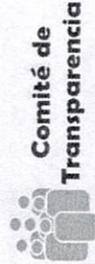
Lic. Rafael Esteva Guarota

Jefe de Departamento de la Unidad de Formación

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Supervisar la elaboración de nombramientos y documentos correspondientes a las bajas, ascensos, promociones por escalafón, licencias sin goce de sueldo y cambios de adscripción de los servidores públicos del Poder Judicial, como lo establecen el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial y el Manual de Organización de las Áreas Auxiliares de la Dirección de Administración.

Actualizar el sistema de control escolar que permita administrar los registros académicos y escolares sobre ingreso, permanencia y egreso de los/las estudiantes de la Escuela Judicial en sus diferentes programas de formación; desarrollar cursos, talleres, seminarios, simposios, conferencias y cualquier otra actividad académica que promueva la difusión de los diversos temas en materia de administración de justicia y cultura jurídica, en términos de los artículos 94 y 98 de la Ley Orgánica del Poder Judicial del Estado de Oaxaca; 143, fracción III, del Reglamento Interior del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca; 16, fracción I, 17, 18, 20 fracción I, 22 y 23, del Reglamento de la Escuela Judicial del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca.





Anexo 1

Catálogo de sistemas de datos personales e inventario



Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Vigilar la correcta integración, resguardo y custodia de los expedientes personales y su actualización utilizando los medios analógicos y digitales autorizados, vigentes y que corresponda. Así como las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Implementar en los procesos de capacitación, formatos de registro, así como recabar la información de datos personales, que permita administrar los registros académicos y escolares sobre el ingreso, permanencia y egreso de las y los estudiantes de la Escuela Judicial en sus programas de formación, como lo establecen los artículos 93, párrafo primero, 94 y 98 de la Ley Orgánica del Poder Judicial del Estado de Oaxaca; 142, 143, fracción III y 144 del Reglamento Interior del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca; 14 y 16, fracción I, 17, 18, 20 fracción I, 22 y 23 del Reglamento de la Escuela Judicial del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores públicos que trate datos personales]

Funciones, obligaciones y cadena de mando Si
Información sobre el tratamiento Si
Capacitación Si

Funciones, obligaciones y cadena de mando Si
Información sobre el tratamiento Si
Capacitación Si

Nombre [Usuario 3]:

Lic. Carlos Alejandro Ugalde Arenas

Lic. Minerva Noemí Cruz Aragón

Cargo:

Jefe del Departamento de Control de Personal

Analista

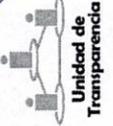
Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Coordinar la elaboración de nombramientos y documentos correspondientes a las bajas, ascensos, promociones por escalafón, licencias sin goce de sueldo y cambios de adscripción de los servidores públicos del Poder Judicial, como lo establecen el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial y el Manual de Organización de las Áreas Auxiliares de la Dirección de Administración.

Procesar la información de las y los estudiantes; actualizar la información del sistema de datos personales que permita administrar los registros académicos y escolares sobre el ingreso, permanencia y egreso de las y los estudiantes de la Escuela Judicial en sus programas de formación, así como concentrar, verificar y cotejar lo relativo a los expedientes de la comunidad estudiantil interesada en obtener un diploma de especialidad del Poder Judicial, como lo establecen los artículos 94 y 98 de la Ley Orgánica del Poder Judicial del Estado de Oaxaca; 143, último párrafo, y 144 del Reglamento Interior del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca; 16, fracción I, 17, 18, 20 fracción I, 22 y 23, del Reglamento de la Escuela Judicial del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca.



Comité de Transparencia



Catálogo de sistemas de datos personales e inventario

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Dar seguimiento la correcta integración, resguardo y custodia de los expedientes personales y su actualización utilizando los medios analógicos y digitales autorizados, vigentes y que corresponda. Así como las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Resguardar la información procesada de las y los estudiantes; así como proteger, resguardar y adoptar las medidas pertinentes respecto a los expedientes de la comunidad estudiantil, como lo establecen los artículos 93, párrafo primero, 94 y 98 de la Ley Orgánica del Poder Judicial del Estado de Oaxaca; 143, último párrafo, y 144 del Reglamento Interior del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca; 16, fracción I, 17, 18, 20 fracción I, 22 y 23, del Reglamento de la Escuela Judicial del Consejo de la Judicatura del Poder Judicial del Estado de Oaxaca.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores públicos que trate datos personales]

Funciones, obligaciones y cadena de mando Si
 Información sobre el tratamiento Si
 Capacitación Si

Funciones, obligaciones y cadena de mando Si
 Información sobre el tratamiento Si
 Capacitación Si

Nota: Se incluye anexo con usuarios diferentes a los señalados

Nota:

Observación: En caso de existir mas usuarios en nota agregar que se incluye anexo con usuarios diferentes a los señalados, entendiéndose por usuario a todas las personas que por su empleo, cargo o comisión debido a sus competencias, atribuciones y funciones tienen acceso al mismo sistema.

1.3. Inventario

Tipo de soporte de sistema:

Físico	Electrónico	Ambos	Físico	Electrónico	Ambos
Formatos	Listados	Documentos	Formatos	Listados	Documentos
Si		Si	Si		Si
	Expedientes	Expedientes		Expedientes	Expedientes



Anexo 1

Catálogo de sistemas de datos personales e inventario



Base datos	Disco duro/USB	Servidores	Paquetería de office	Base datos	Disco duro	Servidores	Paquetería de office
Si	Si	Si	Si				Si

Nota: _____

Nota: _____

Finalidades del tratamiento: [Deberá especificar la razón para la que se recaba la información]

Administrar los registros académicos y escolares sobre el ingreso, permanencia y egreso de las y los estudiantes de la Escuela Judicial en sus diferentes programas de formación, así como el registro de asistencia a las capacitaciones, talleres, conferencias, entre otros y generar estadísticas, informes y las constancias.

Integración del expediente personal, trámites administrativos y de consultas.

Ciclo de vida de los datos personales: [Debe contemplarse el tiempo de uso que se dé a la información]

Soporte físico
Indefinido

Soporte electrónico
Indefinido

Otro: _____

Otro: _____

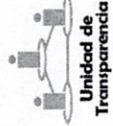
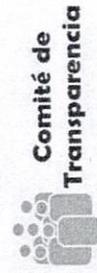
Identificación y autenticación de acceso [En caso de ser más de uno especificar en notas]:

Acceso autorizado
Si
Forma de identificación [En caso de ser más de uno especificar en notas]
Contraseña

Acceso autorizado
Si
Forma de identificación [En caso de ser más de uno especificar en notas]
Gafete

Nota: _____

Nota: _____



Anexo 1

Catálogo de sistemas de datos personales e inventario



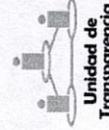
Catálogo de datos personales contenidos en el sistema [Señalar el tipo de dato personales que contiene el sistema, además de listar cada uno de los datos personales recabados]

Datos personales y sensibles de identificación			
Nombre completo	Domicilio	Estado Civil	Fecha de nacimiento
Si	Si	Si	Si
No sensible	No sensible	No sensible	No sensible
Identidad sexual	CURP	RFC	Teléfono
Si	Si	Si	Si
Sensible	No sensible	No sensible	No sensible
Correo electrónico	Características físicas	Biométricos	Médicos/Salud
Si	No	No	Si
No sensible			Sensible
Lengua/idioma	Laborales	Académicos	Curricular
Si	Si	Si	Si
No sensible	No sensible	No sensible	No sensible
Patrimoniales	Financieros	Creencias	Identificación
No	No	No	No
Número de seguridad social, nacionalidad, afiliación sindical y datos familiares			
Sensibles			
Otro (s):			

Nota:

Datos personales y sensibles de identificación			
Nombre completo	Domicilio	Estado Civil	Fecha de nacimiento
Si	No	No	Si
No sensible			No sensible
Identidad sexual	CURP	RFC	Teléfono
Si	Si	No	Si
Sensible	No sensible		No sensible
Correo electrónico	Características físicas	Biométricos	Médicos/Salud
Si	No	No	No
No sensible			
Lengua/idioma	Laborales	Académicos	Curricular
Si	Si	Si	Si
No sensible	No sensible	No sensible	No sensible
Patrimoniales	Financieros	Creencias	Identificación
No	No	No	No
Otro (s):			

Nota:





Anexo 1 Catálogo de sistemas de datos personales e inventario



Localización del sistema [Señalar la ubicación física]

Unidad de Recursos Humanos, ubicado en el sótano del edificio J2 del Centro Administrativo del Poder Ejecutivo y Judicial "General Porfirio Díaz, Soldado de la Patria" Av. Gerardo Pandal Graf No.1 Agencia de Policía Reyes Mantecón. San Bartolo Coyotepec, Oaxaca. C.P. 71257.

Unidad de Formación, de la Escuela Judicial, ubicadas en el Centro Administrativo del Poder Ejecutivo y Judicial, "General Porfirio Díaz, Soldado de la Patria", Edificio J4, segundo nivel, con domicilio en Avenida Gerardo Pandal Graf, número 1, Agencia de Policía Reyes Mantecón, en San Bartolo Coyotepec, Oaxaca, Código Postal 71257.



Anexo 1.1 Otros usuarios



1.1.1. Denominación de la Unidad Administrativa

Dirección de Administración del Consejo de la Judicatura

Nombre del sistema

SysRH

Nombre [Usuario 4]:

Joel Gerardo Pérez Jiménez

Cargo:

Jefe de Oficina 15

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]
Elaboración de nombramientos de base.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores públicos que trate datos personales]

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

No

No

Nombre [Usuario 5]:

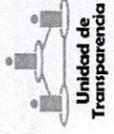
María Emilia Canseco Gómez

Cargo:

Técnico Especializado 13B

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Recepción y relación de la documentación que se integrará a expediente



Anexo 1.1 Otros usuarios

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar] Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores públicos que trate datos personales]

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si
No
No

Nombre [Usuario 6]:

Reina Judith Santiago Leyva

Cargo:

Abogado 13A

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Generar los informes y documentos en materia laboral y judicial que le sean requeridos, así como realizar los actos de notificación respecto a resoluciones o información sobre procedimientos legales o laborales a los trabajadores del Poder Judicial, atendiendo las normas procesales de tiempo, modo y lugar, a fin de que se efectúen de manera sencilla, rápida y ordenada.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores públicos que trate datos personales]

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si
No
No

Anexo 1.1 Otros usuarios



Nombre [Usuario 7]:

Felipa Josefina Juárez Soriano

Cargo:

Analista 13 (Funciones de Actuario Judicial)

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Generar los informes y documentos en materia laboral y judicial que le sean requeridos, así como realizar los actos de notificación respecto a resoluciones o información sobre procedimientos legales o laborales a los trabajadores del Poder Judicial, atendiendo las normas procesales de tiempo, modo y lugar, a fin de que se efectúen de manera sencilla, rápida y ordenada.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

Si

Si

Nombre [Usuario 8]:

Fátima Rosalba Solana Aguilar

Cargo:

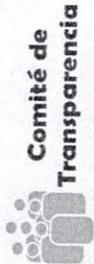
Analista 13

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Elaboración de nombramientos de confianza.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.





33
CJO

Anexo 1.1

Otros usuarios



Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si
No
No

Nombre [Usuario 9]:

Yazmín González Reyes

Cargo:

Analista 13

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Elaboración de informes solicitados por los Órganos de Control Interno y áreas externas del Poder Judicial.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si
No
No

Nombre [Usuario 10]:

Miguel Angel Bautista Luis

Cargo:

Analista 13

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Garantizar el registro, control, atención y trámite oportuno de los requerimientos de constancias de antigüedad, continuidad de servicios, nombramiento para efecto de jubilación, laborales, de percepciones y de Carrera Judicial suscritas por empleados que laboran o hayan laborado en el Poder Judicial.



Comité de
Transparencia



Unidad de
Transparencia



Anexo 1.1 Otros usuarios



Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar] Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

No

No

Nombre [Usuario 11]:

Maria Blanca Martínez Gutiérrez

Cargo:

Analista 13

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Captura en sistema la documentación que se integrará al expediente personal

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

Si

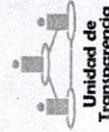
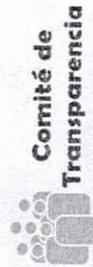
Si

Nombre [Usuario 12]:

Mitzi Magali Arellanes Blanco

Cargo:

Técnico 10





Anexo 1.1 Otros usuarios



Funciones: *[Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]*

Apoyar en el registro, control, atención y trámite oportuno de los requerimientos de constancias de antigüedad, continuidad de servicios, laborales, de percepciones y de Carrera Judicial suscritas por empleados en activo del Poder Judicial, así como aquellos que hayan causado baja o se encuentren pensionados.

Obligaciones: *[Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]*

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: *Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores*

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

No

No

Nombre [Usuario 13]:

Eber Jehovany Pérez Alonso

Cargo:

Técnico 10

Funciones: *[Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]*

Recepción, clasificación, foleo de documentación para la elaboración o actualización de expedientes de personal. Integración de la documentación generada por las diferentes áreas administrativas a expedientes de personal. Responsable de la generación de vales de préstamo de personal. Organización, resguardo y control de expedientes.





Anexo 1.1 Otros usuarios



Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

No

No

Nombre [Usuario 14]:

Julio Cesar Valencia Cruz

Cargo:

Capturista de datos 5

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Consulta y generación de reportes de personal.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

Si

Si

Nombre [Usuario 15]:

Cesar Amílcar Lázaro Santiago

Cargo:

Encargado del Departamento de Seguridad Social, Seguro de Vida y Desarrollo de Personal





Anexo 1.1 Otros usuarios



Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]
Gestionar los trámites relacionados con la seguridad social, seguros de vida y prestaciones laborales que son competencia y responsabilidad de Recursos Humanos,

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]
Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores
Funciones, obligaciones y cadena de mando
Información sobre el tratamiento
Capacitación

Nombre [Usuario 16]:

Patricia Naranjo Justo

Cargo:

Técnico 10

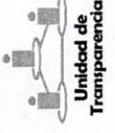
Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]
Realizar los análisis de las prestaciones que deben aplicarse a los trabajadores, conforme a la normatividad en la materia o los convenios vigentes establecidos con gremios sindicales del Poder Judicial

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]
Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores
Funciones, obligaciones y cadena de mando
Información sobre el tratamiento
Capacitación



**Comité de
Transparencia**





Anexo 1.1 Otros usuarios



Nombre [Usuario 17]:

Raymundo Cruz Robles

Cargo:

Oficial Administrativo 4

Funciones: *[Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]*

Recibir, integrar y controlar los registros y documentación para los trámites administrativos de altas y bajas de los trabajadores del Poder Judicial ante el Instituto Mexicano del Seguro Social, conforme a los procedimientos institucionales vigentes.

Obligaciones: *[Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]*

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: *Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores*

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

No

No

Nombre [Usuario 18]:

Adrián Isaias Lucas Aragón

Cargo:

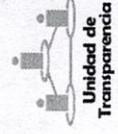
Encargado del Departamento de Supervisión de Personal

Funciones: *[Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]*

Coordinar el proceso de evaluación y control del registro de asistencia de los servidores públicos del Poder Judicial, para efectos de determinar las incidencias administrativas a que haya lugar, así como la validación de registros para garantizar la correcta aplicación los pagos, descuentos, estímulos y premios

Obligaciones: *[Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]*

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.





Anexo 1.1 Otros usuarios



Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si
No
No

Nombre [Usuario 19]:

Jesús Moisés Santiago Ortiz

Cargo:

Jefe de Oficina 15

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Organizar y dar seguimiento a la supervisión de incidencias administrativas o su justificación, correspondiente al registro de asistencias a laborar del personal del Poder Judicial

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si
No
No

Nombre [Usuario 20]:

Jaime Ignacio Ayala González

Cargo:

Jefe de Oficina 15

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Supervisar, evaluar y controlar los registros de asistencia del personal del Poder Judicial, así como informar los resultados de los operativos realizados, para garantizar la correcta aplicación los pagos y descuentos y coadyuvar en el buen funcionamiento del área.





Anexo 1.1 Otros usuarios



Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar] Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si
No
No

Nombre [Usuario 21]:

Javier Eduardo Rivalpalacios Aragón

Cargo:

Analista 13

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Supervisar, evaluar y controlar los registros de asistencia del personal del Poder Judicial, así como informar los resultados de los operativos realizados, para garantizar la correcta aplicación los pagos y descuentos y coadyuvar en el buen funcionamiento del área.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

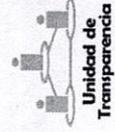
Si
No
No

Nombre [Usuario 22]:

Victor Omar Cruz Méndez

Cargo:

Técnico Administrativo 12





Anexo 1.1 Otros usuarios



Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar] Supervisar, evaluar y controlar los registros de asistencia del personal del Poder Judicial, así como informar los resultados de los operativos realizados, para garantizar la correcta aplicación los pagos y descuentos y coadyuvar en el buen funcionamiento del área.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar] Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si
No
No

Nombre [Usuario 23]:

Fernando Ramirez Martinez

Cargo:

Oficial Administrativo 8A

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Supervisar, evaluar y controlar los registros de asistencia del personal del Poder Judicial, así como informar los resultados de los operativos realizados, para garantizar la correcta aplicación los pagos y descuentos y coadyuvar en el buen funcionamiento del área.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

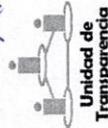
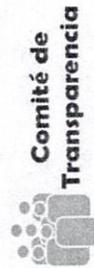
Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores públicos

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si
No
No





Anexo 1.1 Otros usuarios



Nombre [Usuario 24]:

Alma Delia Antonio Sosa

Cargo:

Técnico 10

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Realizar la captura de incidencias de la asistencia del Personal del Poder Judicial, así como las justificaciones correspondientes en el Sistema informático de Recursos Humanos (sysRH)

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando
Información sobre el tratamiento

Capacitación

Si

No

No

Nombre [Usuario 25]:

Elvia Zarate Fernández

Cargo:

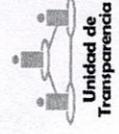
Técnico Especializado 12A

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Apoyar en la generación de información y los trabajos administrativos correspondientes a las vacaciones y las incapacidades del personal del Poder Judicial

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.





Anexo 1.1 Otros usuarios



Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores
 Funciones, obligaciones y cadena de mando
 Información sobre el tratamiento
 Capacitación

Nombre [Usuario 26]:

Jesús Iovany Flores Ramos

Cargo:

Técnico Administrativo 12

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Apoyar en la generación de información y los trabajos administrativos correspondientes a las vacaciones y las incapacidades del personal del Poder Judicial

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando
 Información sobre el tratamiento

Capacitación

Nombre [Usuario 27]:

Jenny Iveth Zarate López

Cargo:

Oficial Administrativo 8C

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Apoyar en la generación de información y los trabajos administrativos correspondientes, respecto a las incidencias del personal del Poder Judicial

Si
No
No

Si
No
No





Anexo 1.1 Otros usuarios



Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar] Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

No

No

Nombre [Usuario 28]:

Gustavo Morales Salinas

Cargo:

Jefe del Departamento de Nómina

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Determinar las percepciones y deducciones derivadas de la relación laboral, que correspondan a cada empleado adscrito al Poder Judicial, generando la información precisa y apropiada para la remuneración de los mismos, así como proporcionar la información para el cumplimiento de obligaciones legales y pago a terceros

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

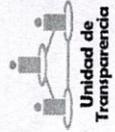
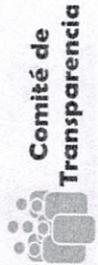
Si

No

No

Nombre [Usuario 29]:

Rosa Ivette Cruz Ramirez





Anexo 1.1 Otros usuarios



Cargo:

Jefe de Oficina

Funciones: *[Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]*

Asistir en la integración de los montos de percepciones y deducciones de la nómina de sueldos y prestaciones ordinarias, así como prevenir los pagos y descuentos indebidos y optimizar el aprovechamiento de los recursos ministrados para la remuneración del personal.

Obligaciones: *[Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]*

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: *Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores*

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

No

No

Nombre [Usuario 30]:

Erycka Joselyn García León

Cargo:

Técnico 10

Funciones: *[Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]*

Asistir al Jefe de la Unidad en las tareas diarias de gestión de la oficina, así como brindar soporte en el registro y procesamiento simple de información, y en la relación con los usuarios internos y externos para favorecer un eficiente funcionamiento del área.

Obligaciones: *[Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]*

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.



Anexo 1.1 Otros usuarios



Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

No

No

Nombre [Usuario 31]:

Beatriz Rayón Ávila

Cargo:

Oficial Administrativo 4

Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema, motivar y fundar]

Efectuar la recepción, registro y entrega de las comunicaciones oficiales documentadas que se realicen a la Unidad de Recursos Humanos implementando mecanismos de organización y control en el trámite correspondiente.

Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema, motivar y fundar]

Las establecidas en el artículo 130 del Reglamento Interior del Consejo de la Judicatura y en el Acuerdo General 08/2014 del Consejo de la Judicatura del Poder Judicial.

Medios para acreditar el cumplimiento: Documentos que establezcan las funciones y atribuciones, que tengan conocimiento y capacitación de servidores

Funciones, obligaciones y cadena de mando

Información sobre el tratamiento

Capacitación

Si

No

No

Análisis de riesgo, de brecha y plan de trabajo

2.1. Análisis de riesgo

- a) Debe valorarse cada riesgo de impacto en una escala del 1 al 4, siendo 1 el más bajo y 4 el más alto.
- b) Las probabilidades se refieren a pérdida (P); destrucción (DE); uso (U); acceso (AC); tratamiento (T); daño (DA); alteración (AL) y modificación (M) no autorizadas. Relacionado con la información confidencial y el personal involucrado en el tratamiento de la misma.
- c) El riesgo conforme a la calificación será **Bajo (1-8); Medio (9-16); Alto (17-24) y Muy alto (25-32)**

Dirección de Administración del Consejo de la Judicatura

Dirección de Escuela Judicial del Consejo de la Judicatura

Nombre del sistema

SysRH

Carrera Judicial

Soporte físico

Vulneraciones	Probabilidades									Calf	Riesgo
	P	DE	U	AC	T	DA	AL	M			
Exposición de los usuarios en el tratamiento	1	1	1	1	1	1	1	1	1	8	Bajo
Requerimientos regulatorios para el tratamiento	1	1	1	1	1	1	1	1	1	8	Bajo
Riesgo inherente a los datos	1	1	1	1	1	1	1	1	1	8	Bajo
Riesgo inherente a los soportes físicos	1	1	1	1	1	1	1	1	1	8	Bajo
Sanciones a los usuarios por vulneraciones	1	1	1	1	1	1	1	1	1	8	Bajo
Sensibilidad de los datos	1	1	1	1	1	1	1	1	1	8	Bajo
Valor potencial cuantitativo de terceros	1	1	1	1	1	1	1	1	1	8	Bajo
Valor potencial cualitativo de terceros	1	1	1	1	1	1	1	1	1	8	Bajo
Vulneraciones previas al sistema	1	1	1	1	1	1	1	1	1	8	Bajo
Desarrollo tecnológico	1	1	1	1	1	1	1	1	1	8	Bajo
Número de usuarios que accesan										31	Muy alto

Nota:

Soporte electrónico



Anexo 2

Análisis de riesgo, de brecha y plan de trabajo

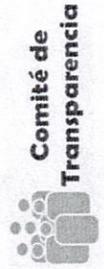


Revisión de la seguridad	3	3	3	2	2	13	Medio existente	1	1	1	1	5	Faltante
Identificación de la información	3	4	4	4	3	18	Existente	3	3	3	3	15	Medio existente
Clasificación de la información	4	4	3	3	3	17	Existente	3	3	3	3	15	Medio existente
Supresión de datos de forma segura	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante
Sensibilización y capacitación del personal en materia de protección de datos	3	3	2	3	2	13	Medio existente	2	2	2	2	10	Medio faltante

Nuevas medidas de seguridad

Medidas de seguridad físicas

Tipo de medida	Medidas de seguridad						Brecha	Medidas de seguridad						Brecha
	A	AD	MA	MT	MF	Calf		A	AD	MA	MT	MF	Calf	
Prevención de acceso no autorizado a las instalaciones	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante	
Prevención de acceso no autorizado a las áreas críticas	3	3	3	4	4	17	Existente	1	1	1	1	5	Faltante	
Prevención de acceso no autorizado a los recursos	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante	
Prevención de acceso no autorizado a la información	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante	
Prevención de daño a las instalaciones físicas	3	3	3	3	3	15	Medio existente	2	2	2	2	10	Medio faltante	
Prevención de daño a las áreas críticas	3	3	3	3	3	15	Medio existente	2	2	2	2	10	Medio faltante	
Prevención de daño a los recursos	3	3	3	3	3	15	Medio existente	2	2	2	2	10	Medio faltante	
Prevención de daño a la información	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante	
Prevención de interferencia a las instalaciones físicas	3	3	2	3	2	13	Medio existente	3	3	3	3	15	Medio existente	
Prevención de interferencia a las áreas críticas	3	3	3	3	3	15	Medio existente	3	3	3	3	15	Medio existente	
Prevención de interferencia a los recursos	3	3	2	3	3	14	Medio existente	3	3	3	3	15	Medio existente	
Prevención de interferencia a la información	4	4	3	3	3	17	Existente	3	3	3	3	15	Medio existente	
Protección de los recursos móviles o portátiles	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante	



Anexo 2 Análisis de riesgo, de brecha y plan de trabajo

Mantenimiento a las instalaciones	3	3	3	3	3	3	15	Medio existente	1	1	1	1	1	5	Faltante
Mantenimiento a los equipos de cómputo	3	3	2	3	3	3	14	Medio existente	1	1	1	1	1	5	Faltante

Nuevas medidas de seguridad

Medidas de seguridad técnicas

Tipo de medida	Medidas de seguridad							Brecha	Medidas de seguridad							Brecha
	A	AD	MA	MT	MF	Calf	A		AD	MA	MT	MF	Calf			
Prevención de acceso no autorizado a las bases de datos	4	4	4	4	4	20	Existente	3	3	3	3	15	Medio existente			
Prevención de acceso a los recursos que contienen las bases	4	4	4	4	4	20	Existente	3	3	3	3	15	Medio existente			
Prevención de acceso no autorizado a las información digital	4	4	4	4	4	20	Existente	1	1	1	1	5	Faltante			
Prevención de acceso a los recursos que contienen la información	4	4	4	4	4	20	Existente	1	1	1	1	5	Faltante			
Asignación de usuarios con permisos definidos	4	4	4	4	4	20	Existente	1	1	1	1	5	Faltante			
Contraseñas de acceso establecidas	4	4	4	4	4	20	Existente	1	1	1	1	5	Faltante			
Gestión de mantenimiento de software	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante			
Gestión de mantenimiento de hardware	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante			
Gestión de medios de almacenamiento	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante			
Gestión de medios de operación	3	3	3	3	3	15	Medio existente	1	1	1	1	5	Faltante			

Nuevas medidas de seguridad

2.3. Plan trabajo

El Plan de trabajo se encuentra integrado en el documento de seguridad del responsable en el capítulo 5. Análisis de riesgo, de brecha y plan de trabajo, en el acápite 5.1. Plan de trabajo.



Anexo 3 Revisión y vigilancia



3.1. Monitoreo de vulneraciones a los sistemas

Monitorear, revisar y vigilar de manera periódica las amenazas y vulneraciones a las que están sujetos los datos personales [Entiéndase por tipo de vulneración pérdida (P); destrucción (DE); uso (U); acceso (AC); tratamiento (T); daño (DA); alteración (AL) y modificación (M) no autorizadas]. Deberá seleccionarse la frecuencia con la que se monitorea o revisa la misma]

Dirección de Administración del Consejo de la Judicatura

Judicatura

Nombre del sistema

SysRH

Carrera Judicial

Soporte físico

Vulneraciones	Tipo de vulneración							Tipo de vulneración							
	P	DE	U	AC	T	DA	M	P	DE	U	AC	T	DA	AL	M
Exposición de los usuarios en el tratamiento	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Requerimientos regulatorios para el tratamiento	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Riesgo inherente a los datos	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Riesgo inherente a los soportes físicos	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Sanciones a los usuarios por vulneraciones	Otro	Otro	Otro	Otro	Otro	Otro	Otro	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Sensibilidad de los datos	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Valor potencial cuantitativo de terceros	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Valor potencial cualitativo de terceros	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Vulneraciones previas al sistema	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Desarrollo tecnológico	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Número de usuarios que accesan	31							3							

Otro [especificar]:

60 días



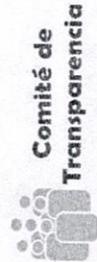


Anexo 3 Revisión y vigilancia



SopORTE electrónico

Vulneraciones	Tipo de vulneración						Tipo de vulneración					
	P	DE	U	AC	T	M	P	DE	U	AC	T	M
Exposición de los usuarios en el tratamiento	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Requerimientos regulatorios para el tratamiento	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Riesgo inherente a los datos	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Riesgo inherente a los soportes físicos	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Sanciones a los usuarios por vulneraciones	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Sensibilidad de los datos	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Valor potencial cuantitativo de terceros	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Valor potencial cualitativo de terceros	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Vulneraciones previas al sistema	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Desarrollo tecnológico	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días	30 días
Número de usuarios que accesan	31											
Otro [especificar]:	3											





Anexo 3

Revisión y vigilancia



3.2. Monitoreo de medidas de seguridad

Monitorear, revisar y vigilar de manera periódica las medidas de seguridad implementadas [Entiéndase por medidas de seguridad como acciones (A); actividades (AD); mecanismos administrativos (MA); mecanismos técnicos (MT); mecanismos físicos (MF)]. Deberá seleccionarse la frecuencia con la que se monitorea o revisa la misma]

Nota: Si en el análisis de brecha alguna medida de seguridad fue faltante dejar en blanco la periodicidad de monitoreo, revisión o vigilancia.

Medidas de seguridad administrativas

Tipo de medida	Medidas de seguridad				
	A	AD	MA	MT	MF
Políticas y procedimientos para la gestión	30 días	30 días	30 días	30 días	30 días
Soporte de la seguridad	30 días	30 días	30 días	30 días	30 días
Revisión de la seguridad	30 días	30 días	30 días	30 días	30 días
Identificación de la información	30 días	30 días	30 días	30 días	30 días
Clasificación de la información	30 días	30 días	30 días	30 días	30 días
Supresión de datos de forma segura	30 días	30 días	30 días	30 días	30 días
Sensibilización y capacitación del personal en materia de protección de datos	30 días	30 días	30 días	30 días	30 días

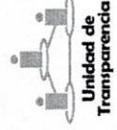
Medidas de seguridad				
A	AD	MA	MT	MF
30 días	30 días	30 días	30 días	30 días
30 días	30 días	30 días	30 días	30 días
30 días	30 días	30 días	30 días	30 días

Otro [especificar]:

Medidas de seguridad físicas

Tipo de medida	Medidas de seguridad				
	A	AD	MA	MT	MF
Prevención de acceso no autorizado a las instalaciones	30 días	30 días	30 días	30 días	30 días

Medidas de seguridad				
A	AD	MA	MT	MF





Anexo 3

Revisión y vigilancia



Contraseñas de acceso establecidas	30 días																		
Gestión de mantenimiento de software	30 días																		
Gestión de mantenimiento de hardware	30 días																		
Gestión de medios de almacenamiento	30 días																		
Gestión de medios de operación	30 días																		

Otro [especificar]:

3.3. Otros tipos de monitoreo de vulneraciones y de sistemas de seguridad

Existencia de nuevos tipos de soporte físico a los reportados	Ninguno																		
Existencia de nuevos tipos de soporte electrónico a los reportados	Ninguno																		
Modificaciones a los soportes físicos existentes	Ninguno																		
Modificaciones a los soportes electrónicos existentes	Ninguno																		
Vulneraciones ocurridas a los soportes físicos reportados	Ninguno																		
Vulneraciones ocurridas a los soportes electrónicos reportados	Ninguno																		
Vulneraciones a soportes físicos diferentes a los reportados	Ninguno																		
Vulneraciones a soportes electrónicos diferentes a los reportados	Ninguno																		

