



CONSEJO DE LA JUDICATURA

PODER JUDICIAL DEL ESTADO DE JALISCO

DOCUMENTO DE SEGURIDAD
2020



Contenido

Glosario.....	2
Medidas de Seguridad Implementadas.....	3
Procedimientos de respaldo y recuperación de datos personales.....	4
Controles de Identificación y Autenticación de Usuarios.....	8
Controles y mecanismos de seguridad para las transferencias.....	14
Bitácoras de Acceso, Operación Cotidiana y Vulneraciones a la Seguridad de los Datos Personales.....	14
Técnicas de Supresión y Borrado seguro de Datos Personales.....	16
Análisis de Riesgos.....	16
Análisis de Brecha.....	21
Gestión de Vulneraciones.....	22
Mecanismos de monitoreo y revisión de las medidas de seguridad.....	23
Plan de trabajo.....	23
Programa General de Capacitación.....	27
El plan de contingencia.....	27
Catálogo de Sistemas de Tratamiento de Datos Personales (Anexo 1).....	30
Formato notificación de vulneración de seguridad de los datos personales (Anexo 2).....	31
Formato para determinar que las vulneraciones fueron mitigadas (Anexo 3).....	32



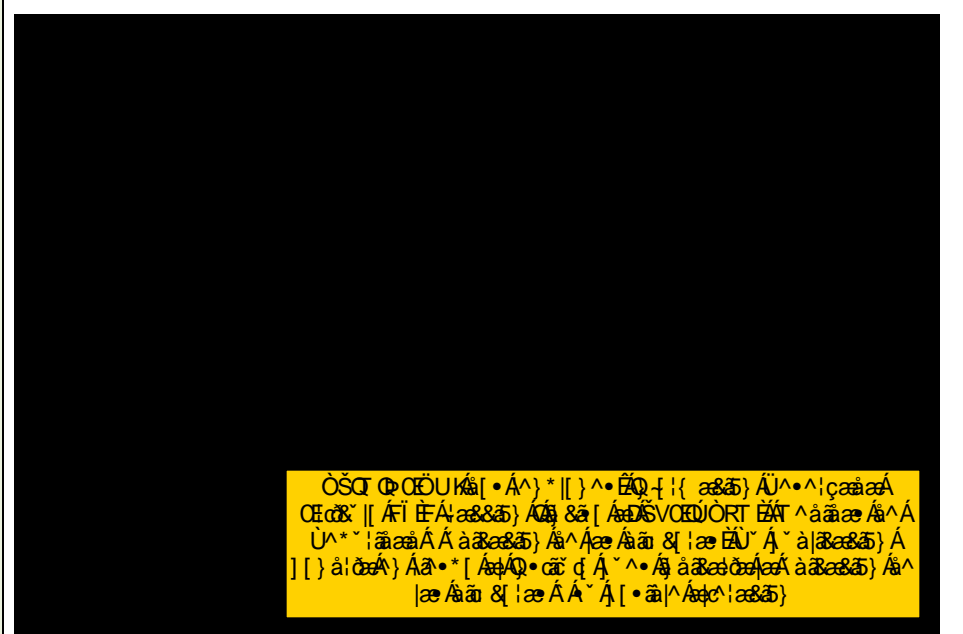
Glosario

DNS	Un Servidor DNS en informática responde a las siglas Domain Name System. Gracias a los servidores DNS conocemos los nombres en las redes, como las de Internet o las de una red privada.
DMZ	En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una zona insegura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida
LAN	Una red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
BASE DE DATOS	Concentrado de información que contenga información pública protegida.
ACTIVO DE APOYO	Documentos, archiveros, hardware, software, redes o cualquier otro recurso que se involucre para el tratamiento de información pública protegida.
INFORMACIÓN PÚBLICA PROTEGIDA	Comprende la información confidencial y reservada que recaba, resguarda y utiliza el Consejo de la Judicatura del Estado de Jalisco.
LEY GENERAL	Ley General de Protección de Datos Personales para Sujetos Obligados.
LEY DE TRANSPARENCIA	Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
LEY	Ley de Protección de Datos Personales para los Sujetos Obligados del Estado de Jalisco y sus municipios.
LINEAMIENTOS GENERALES	Lineamientos Generales de Protección de Datos Personales para el Sector Público.
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.
MEDIDAS DE SEGURIDAD	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar los protección, confidencialidad, disponibilidad e integridad de los datos personales.
N/A	No Aplica



MEDIDAS DE SEGURIDAD IMPLEMENTADAS

Este sujeto obligado establece y mantiene las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, para garantizar la confidencialidad, integridad y disponibilidad de cada sistema de datos personales que posean, con la finalidad de preservar el pleno ejercicio de los derechos tutelados en la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus municipios, frente daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.

<p>ENTORNO INSTITUCIONAL</p>	
<p>ENTORNO DE LOS DATOS</p>	<ul style="list-style-type: none"> • No se sitúan junto a las ventanas para evitar daños por agua u objetos que les caigan • Colocar los equipos en lugares seguros para evitar caídas y/o daños • Este Consejo cuenta con equipo de extinción de incendios los cuales son proveídos por un externo certificado en la materia • Se cuenta con reguladores de corriente en cada equipo de computo • Borrado Seguro: Cuando se elimine un activo como equipo de procesamiento, soporte físico o electrónico, deben aplicarse mecanismos de borrado seguro, o bien, de destrucción adecuado. Cualquier eliminación de activos debe registrarse con fines de auditoría. • Escritorio limpio Cualquier documento o activo de información se resguarda, fuera de la vista, cuando éste no sea atendido.



LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos los datos personales e información sensible y confidencial, ante este hecho una de las principales riesgos que pueden derivar en pérdidas de la información en formato digital; son errores humanos, borrado accidental, uso negligente, virus, falla en dispositivos de almacenamiento masivo.

Asumiendo lo anterior como uno de los principales riesgos para la información digital es necesaria la implementación de un mecanismo que nos permita contar con un respaldo de la información.

El respaldo de información consiste en realizar un duplicado de ésta, llamado también copia de seguridad o backup.

Existen tres tipos de respaldos de la información estos son:

- Respallos completos. Un respaldo completo es un respaldo donde cada archivo es escrito a la media de respaldo.
- Respallos incrementales. A diferencia de los respaldos completos, los respaldos incrementales primero revisan para ver si la fecha de modificación de un archivo es más reciente que la fecha de su último respaldo. Si no lo es, significa que el archivo no ha sido modificado desde su último respaldo y por tanto no se realiza una nueva copia
- Respallos diferenciales. Los respaldos diferenciales son similares a los respaldos incrementales en que ambos solamente copian archivos que han sido modificados. Sin embargo, los respaldos diferenciales son acumulativos, con un respaldo diferencial, una vez que un archivo ha sido modificado continua siendo incluido en todos los respaldos diferenciales subsecuentes

Alcance.

La presente política abarca todos los activos información pública protegida, en equipos de cómputo, sistemas de información y servicios tecnológicos donde se almacene Información pública reservada, Información pública fundamental, Información pública confidencial.



ROLES Y RESPONSABILIDADES

Roles

Administrador de sistema / Administrador del portal institucional/ Personal Técnico.

Es la persona con responsabilidad funcional de realizar los respaldos de información.

Comité de Transparencia.

Responsables de verificar que se cumplan los lineamientos para el respaldo de la información.

Responsabilidades

ROL	Actividades
Administrador de sistema / Administrador del portal institucional/ Personal Técnico.	<ul style="list-style-type: none">• Cumplir con el cronograma de respaldos.• Realizar respaldos.• Realizar pruebas de restauración de acuerdo al cronograma evaluación.• Cumplir con los términos para el resguardo, control y destrucción de los respaldos.• Llevar los registros en bitácora de las actividades.
Comité del Clasificación.	<ul style="list-style-type: none">• Verificar que la presente guía sea utilizada adecuadamente y brinde la información necesaria para la clasificación de la información.• Realizar auditorías periódicas para asegurar el cumplimiento.



TÉRMINOS PARA EL RESPALDO DE LA INFORMACIÓN			
Tipo de información	Esquema de respaldo	Periodicidad	Caducidad
Información pública fundamental. Sitio Web Institucional.	Incremental	Semanal	4 semanas
	Diferencial	Mensual	5 meses
	Completo	Semestral	6 Meses
	Completo	Anual	2 años
	Completo	Tres años (o cambio administración)	Nunca
Información pública confidencial.	Completo	Mensual	3 Meses
	Completo	Semestral	12 meses

Pruebas de restauración.

Se deberán realizar evaluaciones de respaldos de forma periódica para asegurarse que los datos se pueden leer, los resultados deben registrarse en el “formato de bitácora de respaldos”, los detalles acerca de la periodicidad y el número de archivos se especifican en al siguiente tabla.

Tipo de Información	Periodicidad	Número de Archivos
Información pública fundamental. Sitio Web Institucional.	Se deberá realizar una prueba posterior a cada respaldo	Se elegirán de manera aleatoria 20 archivos, verificando su integridad.
Información pública reservada	Se realizara una prueba cada mes.	Se elegirán de manera aleatoria 10 archivos, verificando su integridad.



Información pública confidencial.	Se realizara una prueba cada mes.	Se elegirán de manera aleatoria 10 archivos, verificando su integridad.
--	-----------------------------------	---

Términos para el resguardo, control y destrucción de los respaldos de la información.

Tipo de información	Resguardo.	Destrucción
Información pública fundamental. Sitio Web Institucional.	Por tratarse de información pública fundamental, el resguardo de los respaldos deberá ser habilitado una sede alterna al edificio de la administración municipal con la finalidad de recuperación en caso de desastre o siniestro, se deberá llevar un registro de inventario simple.	La destrucción del respaldo se realizara por borrado simple, se deberá registrar en el inventario la fecha, hora y operador de la eliminación
Información pública reservada	Debido a la naturaleza de la información, se deberán resguardar los respaldos protegidos por contraseña segura, se deberá registrar en el inventario de resguardo de información.	Unidades de almacenamiento masivo (Discos Duros, Cintas, Memorias, SAN) se deberá realizar un borrado basado en el algoritmo de eliminación de datos Wiping, se deberá registrar en el inventario la fecha, hora y operador de la eliminación
Información pública confidencial.	El acceso al medio de respaldo debe ser restringido a personal autorizado.	DVD's y/o CD's Se deberá destruir mediante procedimientos físicos (Cortar, Romper, Rayar por ambos lados), se deberá registrar en el inventario la fecha, hora y operador de la eliminación



CONTROLES DE IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos la información pública protegida, en la actualidad los equipos de cómputo, aplicaciones y servicios informáticos, son herramientas fundamentales para los procesos y actividades de la administración pública, debido a esto es indispensable un documento que defina las políticas y estándares de seguridad para la protección de información pública protegida activos de información que deberán observar de manera obligatoria todos los usuarios(funcionarios públicos, contratistas) para el buen uso del equipo de cómputo, cuentas de usuarios, red, sistemas de información y aplicaciones informáticas.

Partiendo de la premisa que la correcta gestión de cuentas de usuario y las contraseñas son un aspecto fundamental de la seguridad de los recursos informáticos ya que una contraseña mal elegida o protegida puede resultar en un agujero de seguridad para toda la administración municipal. Por ello, todos los servidores públicos, administradores de sistemas, personal técnico, contratistas, proveedores y terceros, son responsables de velar por la seguridad de las contraseñas.

Objetivo.

El objetivo es asegurar que toda cuenta de usuario y contraseña sea gestionado de forma segura, por lo que se deben respetar una serie de medidas y buenas prácticas encaminadas a mejorar la seguridad. En este sentido, la concientización de los administradores de sistemas y usuarios va enfocada a la gestión eficiente de las cuentas y contraseñas que son utilizadas en los procesos y operaciones que requiere autenticación dentro de la administración municipal.

Alcance.

La presente política atañe todos los activos de información pública protegida almacenados en equipos de cómputo, sistemas de información y servicios tecnológicos que requieran la creación de cuentas de usuario para la protección del acceso.

El alcance de esta política es definir los roles y responsabilidades para la gestión de cuentas de usuarios y la creación de contraseñas fuertes, la protección de dichas contraseñas, y el cambio frecuente de las mismas.

Incluye además a todos aquellos usuarios externos que deban acceder a algún recurso o servicio de la administración.



ROLES Y RESPONSABILIDADES

ROLES

Administrador de sistema.

Es la persona con responsabilidad funcional de gestionar cuentas de usuario, almacenar y resguardar los activos de información de manera electrónica.

Responsables o usuarios.

Son aquellos funcionarios que por sus actividades y responsabilidades dentro de la administración pública hacen uso de cuentas o servicios informáticos donde se almacenan activos de información pública protegida.

Comité de clasificación.

Responsables de verificar que se cumplan se cumplan las políticas de gestión de cuentas y contraseñas.

RESPONSABILIDADES

ROL	ACTIVIDADES
Administrador de sistema	<ul style="list-style-type: none">• Cumplir los términos para Administradores de Sistemas para la gestión de cuentas y contraseñas.• Cumplir con los criterios para la construcción de Contraseñas Seguras
Responsables o Usuarios	<ul style="list-style-type: none">• Cumplir los términos de usuario para el uso de credenciales.• Cumplir con los criterios para la construcción de Contraseñas Seguras
Comité de clasificación	<ul style="list-style-type: none">• Verificar se cumplan los lineamientos para la gestión de usuarios y contraseñas.• Realizar auditorías periódicas para asegurar el cumplimiento.



Políticas de seguridad para la gestión de cuentas y contraseñas.

Todo usuario de la administración municipal deberá poseer una o cuenta de usuario personal, que actuará como una credencial que lo identifique de manera única, y que le permitirá tener acceso a los recursos tecnológicos y de la red institucional.

Para todo sistema información o recurso tecnológico donde se resguarden activos de información el usuario deberá autenticarse mediante credencial electrónica y contraseña segura "Password".

Criterios para la Gestión de cuentas de usuario.

NIVEL	DESCRIPCIÓN
Usuarios	Son todas aquellas cuentas que son utilizadas por los usuarios para acceder a los diferentes recursos tecnológicos y sistemas de información del Municipio. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de activos de información sobre la que tiene privilegios.
Administrador de sistemas / Personal Técnico	Son aquellas cuentas de usuario que permiten la administración de sistemas o recursos tecnológicos y tienen privilegios para realizar tareas específicas a nivel directivo, como ejemplo: agregar/modificar/eliminar activos de información y cuentas de usuario.

Términos de Usuario para el uso de credenciales.

- El uso de la cuenta de usuario es responsabilidad de la persona a la que está asignada. La cuenta es para uso personal e intransferible.
- La cuenta de usuario se protegerá mediante una contraseña. La contraseña asociada a la cuenta de usuario, deberá cumplir los Criterios para la Construcción de Contraseñas Seguras.
- No está permitido compartir la cuenta de usuario con otras personas.
- Si un usuario detecta que su credencial de acceso (usuario y contraseña) está siendo utilizado por otra persona, debe hacer el cambio de su contraseña y contactar al administrador del sistema para notificar la incidencia a la mayor brevedad posible.
- Ningún usuario debe acceder a los sistemas con una credencial diferente a la propia, aun con el consentimiento del propietario de la cuenta.



CONSEJO DE LA JUDICATURA

PODER JUDICIAL DEL ESTADO DE JALISCO

- En caso de que el usuario requiera alejarse de su equipo estará obligado al bloqueo de pantalla y para tiempos prolongados deberá cerrar su sesión de usuario.
- No revele su contraseña por teléfono, mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica
- No revele la contraseña a sus compañeros cuando se marche de vacaciones.
- No revele su contraseña a sus superiores, ni a sus colaboradores.

Términos para Administradores de Sistemas para la gestión de cuentas.

- Solo se deben otorgar a las cuentas de usuario el conjunto mínimo de privilegios que le permitan desarrollar sus funciones correctamente.
- Asegurarse que toda credencial de usuario respete los Criterios para la Construcción de Contraseñas Seguras.
- Toda cuenta de usuario sin excepción deberá estar protegida por una contraseña segura.
- Deberán proveer de un mecanismo para expirar las contraseñas y obligar a los usuarios al cambio de la misma en un periodo no mayor a 90 días.
- Aplicar el criterio de historial de contraseña para evitar el uso de contraseñas recurrentes.
- Instrumentar mecanismos de número máximo de intentos de inicio de sesión no válidos de manera que tras 5 intentos fallidos la cuenta se bloquee por 15 minutos y en caso de recurrencia se deshabilite de manera temporal.
- Instrumentar mecanismos para el bloqueo automático de pantalla tras un lapso de 5 minutos de inactividad.
- Se debe vigilar que los usuarios no compartan bajo ninguna circunstancia su contraseña o identificación personal.
- Para el caso de las contraseñas de cuentas de administrador además de cumplir los criterios para la construcción de contraseñas seguras, el periodo de caducidad no debe ser mayor de 30 días.
- Si un superior jerárquico demanda hacer uso de la cuenta de usuario de un subordinado deberá solicitarlo por escrito o vía electrónica dirigido al Administrador del Sistema.
- Si se detecta uso indebido de una cuenta de usuario o se sospecha que la actividad de una cuenta usuario puede comprometer la integridad y seguridad de los activos de información, el acceso a dicha cuenta será suspendido temporalmente y será reactivada sólo después de haber tomado las medidas necesarias a consideración del Administrador del Sistema.
- Todas las credenciales y contraseñas deberán ser tratadas con carácter confidencial.
- Si se requiere el respaldo de las contraseñas en medio digital o impreso, el respaldo generado deberá ser único y bajo resguardo.



Superior jerárquico: términos de encargado para el uso de credenciales.

El superior jerárquico de un funcionario que causa baja, es comisionado o cambia de puesto en la administración pública, está obligado a notificar de manera escrita o vía electrónica en un plazo no mayor a 24hrs al(los) administrador(es) del sistema para que se realicen la bajas correspondientes.

Criterios para la construcción de Contraseñas Seguras.

La seguridad provista por una contraseña depende de que la misma se mantenga siempre en secreto, todas las directrices suministradas por esta política tienen por objetivo mantener esta característica;

Una contraseña segura deberá cumplir cabalmente con las siguientes características:

1. La longitud debe ser mínimo de 10 caracteres.
2. La contraseña deberá contener mezcla entre letras mayúsculas y minúsculas.
3. La contraseña deberá contener al menos 2 dígitos y 1 caracteres especiales(/, *, \$, @, etc.).
4. La contraseña no debe ser basada en información personal, fecha de nacimiento, nombres de familia, o nombre de la cuenta de usuario.
5. Se prohíben el uso de secuencias básicas de teclado (por ejemplo: "qwerty", "asdf", "1234" ó "98765")
6. No se deben repetir los mismos caracteres de manera continua en la misma contraseña. (por ejemplo: "111222").

Para la creación de contraseñas seguras.

Hoy en día el uso de las tecnologías y herramientas de la información y comunicaciones se han convertido en una de las herramientas indispensables para nuestras actividades diarias, ante esto fue necesario la creación de un mecanismo que permitiría el acceso o restricción a estos servicios, generando la necesidad de un medio identificación que permitiera probar la autenticidad de un usuario.

Uno de los mecanismos más antiguos y populares era el uso de un nombre de usuario "¿quién es usted? Y una palabra clave o de pase (Password) a manera de pregunta ¿Demuéstrelo?

En términos más prácticos, una contraseña proporciona una forma de probar la autenticidad de la persona que dice ser el usuario con ese nombre de usuario.



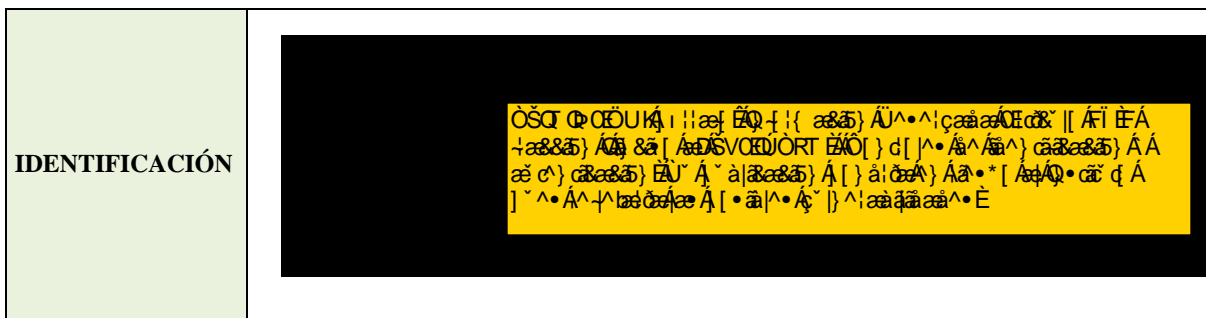
La efectividad de un esquema basado en contraseñas recae en gran parte sobre varios aspectos de la contraseña:

- La confidencialidad de la contraseña
- La resistencia de adivinar la contraseña
- La resistencia de la contraseña ante un ataque de fuerza bruta

Las contraseñas que efectivamente toman en cuenta estos problemas se conocen como contraseñas robustas, mientras que aquellas que no, se les llama débiles. Es importante para la seguridad crear contraseñas robustas, mientras más robustas sean las contraseñas, hay menos oportunidades de que estas sean descubiertas o que se adivinen.

Objetivo.

Las contraseñas son el método principal para verificar la identidad de los usuarios. Por esta razón la seguridad de las contraseñas es de suma importancia para la protección del usuario, la estación de trabajo y la red. El objetivo principal de este documento es ofrecer a los usuarios consejos efectivos para la seguridad la construcción de contraseñas robustas.





LOS CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

1. Transferencias de datos personales	<ul style="list-style-type: none">a) Deberá señalar si el envío se realiza a través de mensajero oficial, mensajero privado o correspondencia ordinaria;b) Deberá precisar si utiliza un sobre o paquete sellado de manera que sea perceptible si fue abierto antes de su entrega;c) Deberá manifestar si el sobre o paquete enviado es entregado en mano al destinatario, previa acreditación con identificación oficial;d) Deberá indicar si el remitente pide al destinatario que le informe en caso de que reciba el sobre o paquete con señas de apertura;e) Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales, yf) Deberá señalar si el remitente registra la o las transmisiones en su bitácora.
2. Transmisiones mediante el traslado físico de soportes electrónicos	<ul style="list-style-type: none">a) Deberá señalar lo previsto en el numeral 1) anterior, incisos a) al f), yb) Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos.
3. Transmisiones mediante el traslado sobre redes electrónicas	<ul style="list-style-type: none">a) Deberá señalar la información prevista en el inciso b) del numeral 2) anterior;

BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

El encargado deberá elaborar una bitácora con los siguientes requisitos:

- 1. Bitácoras para accesos y operación cotidiana**
 - a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
 - b) Para soportes físicos: Número o clave del expediente utilizado, y
 - c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
- 2. Si las bitácoras están en soporte físico o en soporte electrónico;**



CONSEJO DE LA JUDICATURA
PODER JUDICIAL DEL ESTADO DE JALISCO

- 3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
- 4. La manera en que asegura la integridad de las bitácoras, y
- 5. Respecto del análisis de las bitácoras:
 - a) Quién es el responsable de analizarlas (si es el sujeto obligado o si es un tercero) y cada cuándo las analiza, y
 - b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

Bitácoras de Acceso	<p>1. Las Bitácoras de Acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información:</p> <ul style="list-style-type: none"> • Nombre y Cargo de quien accede • Identificación del expediente • Fojas del Expediente • Propósito de acceso • Fecha de acceso • Hora de acceso • Fecha de devolución • Hora de devolución
---------------------	---

Vulneración de seguridad de los datos personales.

Las acciones para notificar la vulneración de seguridad de los datos personales son:

- a) El Encargado elabora y entrega un informe al Responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados.
- b) El incidente se registra en el formato, su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente.
- c) En caso de robo o extravío de datos personales, el Responsable del sistema, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que, en el ámbito de sus atribuciones, determine lo conducente.

El formato que se deberá manejar tiene que cumplir con los elementos descritos. **(ANEXO 2)**



LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

Métodos Físicos

1. Trituración mediante corte cruzado o en partículas: Cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados “partículas”, lo cual hace prácticamente imposible que se puedan unir.

2. Destrucción de los medios de almacenamiento electrónicos mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

Métodos Lógicos Sobre-escritura

Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

EL ANÁLISIS DE RIESGOS

El siguiente cuestionario pretende analizar si la iniciativa realizada por el área implica tratamiento de datos de carácter personal sujetos al marco jurídico que regula el derecho de protección de datos y valorar si en el tratamiento concurren circunstancias y situaciones que obliguen a realizar una Evaluación de Impacto a la Privacidad.

Tipología de Datos	
¿Se van a tratar (1) datos personales (2)? (SI/NO)	(1) Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personal eso conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción



<p>¿Se van a tratar (1) datos personales (2)? (SI/NO)</p>	<p>(2) Datos personales: toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona</p>
---	---

Finalidades del tratamiento	Detalles	Si / No
Marque SI/NO (donde aplique) en función de si el tratamiento responde a las siguientes posibles finalidades:		
¿La recolección de los datos tiene como finalidad el tratamiento a gran escala (3)? Por favor, detalle los puntos indicados a continuación para poder analizar si se trata de un tratamiento a gran escala:		
El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento)		
Las categorías de datos tratados. (Datos especialmente protegidos, Datos de carácter identificativo, Características personales, Circunstancias sociales, Datos académicos y profesionales, Detalles del empleo, Información comercial, Datos económicos, financieros y de seguro, Transacciones de bienes y servicios). Indicar cuántas de estas categorías aplicarían.		
La duración del tratamiento (instantáneo (I), días (D), semanas (S), meses (M)).		
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I)).		
¿La recolección de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables)		
¿La recogida de los datos tiene como finalidad el tratamiento de datos especialmente protegidos (4)?		



CONSEJO DE LA JUDICATURA

PODER JUDICIAL DEL ESTADO DE JALISCO

<p>(4) Datos identificativos de personas identificadas o identificables asociadas a: Ideología u opiniones políticas, Afiliación sindical Religión u opiniones religiosas Creencias o creencias filosóficas Origen étnico o racial Datos relativos a salud Vida sexual u orientación sexual Datos de violencia de género y malos tratos Datos biométricos.- Datos genéticos que proporcionan una información única sobre la fisiología o la salud del identificado obtenidas del análisis de una muestra biológica Datos solicitados para fines policiales sin consentimiento de las personas afectadas Datos relativos a condenas y delitos penales”</p>		
<p>¿El tratamiento involucra contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo (5) o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad (6)?</p>		
<p>(5) A modo de ejemplo, las llamadas telefónicas podrían considerarse intrusivas</p>		
<p>(6) A modo de ejemplo, la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geo localización, Big Data o la utilización de etiquetas de radiofrecuencia o RFID 10 (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro”</p>		
<p>¿La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p. e.: menores de 14 años, ancianos, personas con riesgo de exclusión social, empleados,...)?</p>		
<p>¿Se van a tratar datos personales para elaborar perfiles, categorizar / segmentar, o para la toma de decisiones (7)?</p>		
<p>(7) A modo de ejemplo, la segmentación de clientes en base a sus datos personales con el objetivo de realizar comunicaciones comerciales</p>		
<p>¿El tratamiento de los datos implica una toma de decisión es automatizadas que hay a ningún a persona que intervenga en la decisión o valor el o resultados (8)</p>		
<p>¿Se enriquece la información de los interesados mediante la recolección de nuevas categorías de datos o se usen las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados (9), o incluso pueda llegar a bloquear el disfrute de algún servicio?</p>		



¿El tratamiento implica que un elevado número de personas (más allá de las necesarias para llevar a cabo el mismo) tenga acceso a los datos personales tratados? Por ejemplo, un departamento que no participe en el tratamiento.		
¿Se van a tratar datos relativos a la observación de zonas de acceso público? (por favor, tenga en cuenta que las zonas de acceso público únicamente estarán situadas en la vía pública, excluyendo los lugares de trabajo (p .e.: oficinas comerciales)		
Para llevar acabo este tratamiento, ¿se combinan conjuntos de datos utilizados por otros responsables de tratamiento cuya finalidad diste en exceso de las expectativas del interesado (10)?		
(10) A modo de ejemplo, utilizar el resultado de un tratamiento de análisis de datos de un cliente para realizarle ofertas comerciales en base a dichos resultados		
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		

Tecnologías empleadas para el tratamiento	Detalles	Si / No
Marque SI/NO en función de si dichas tecnologías se usan para soportar las finalidades del tratamiento:		
¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado, cuyo alcance no puede ser previsto por el interesado de forma clara o razonable e implique elevado riesgo para el acceso no autorizado (11)?		
(11) A modo de ejemplo, la combinación de tecnologías ya existentes, como el uso de dispositivos inteligentes de nueva creación y reconocimiento facial para aumentar la seguridad del acceso físico a las instalaciones, se considera una tecnología inmadura		



Tecnologías empleadas para el tratamiento	Detalles	Si / No
Marque SI/NO:		
¿Es este tratamiento similar a otro para el que hayas ido necesario realizar una Evaluación de Impacto de la Protección de Datos Personales (12)?		
¿Este tratamiento puede con llevar una pérdida o alteración de la información?		
¿Se utiliza documentación en papel para tratar datos personales?, en tal caso, indicar las medidas aplicadas:		
<ul style="list-style-type: none">• Se guarda bajo llave• Se destruye de forma confidencial• Se guarda con un registro de accesos• Otro		

Riesgos en el tratamiento:

- Obtención de datos incompletos o incorrectos,
- Omitir la notificación al titular de los datos personales del aviso de confidencialidad,
- No tener evidencia de que el titular de los datos personales conoce los términos del aviso de confidencialidad.
- No difundir el aviso de confidencialidad.
- Falta de capacitación en los servidores públicos que recaban información confidencial sobre la importancia de los datos personales.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen información confidencial.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.
- Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes.
- Alteración de la información.

Inexistencia de contrato de confidencialidad, aviso o responsiva firmada por los servidores públicos que autorizados a tratar la información confidencial.



ANÁLISIS DE BRECHA

Análisis de Brecha (Medidas de seguridad existentes VS medidas de seguridad faltantes)				
Código	Pregunta o Control	¿Existente?		
		Sí	No	Observaciones
A.	Medidas de seguridad basadas en la cultura del personal			
A.1.	¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?	SI		
A.1.1.	Política de escritorio limpio	SI		
A.1.2.	Hábitos de cierre y resguardo	SI		
A.1.3.	Impresoras, escáneres, copiadoras y buzones limpios	SI		
A.1.4.	Gestión de bitácoras, usuarios y acceso	SI		Se realizara desarrollo inicial
A.2.	¿Tienes mecanismos para eliminar de manera segura la información?	SI		
A.2.1.	Dstrucción segura de documentos	SI		
A.2.2.	Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico	SI		
A.2.3.	Fijar periodos de retención y destrucción de información	SI		Se realizara desarrollo inicial
A.2.4.	Tomar precauciones con los procedimientos de reutilización	SI		
A.3.	¿Has establecido y documentado los compromisos respecto a la protección de datos?	SI		
A.3.1.	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos	SI		
A.3.2.	Fomentar la cultura de la seguridad de la información	SI		
A.3.3.	Difundir noticias en temas de seguridad	SI		Se realizara desarrollo inicial
A.3.4.	Prevenir al personal sobre la Ingeniería Social	SI		Se realizara desarrollo inicial
A.3.5.	Asegurar la protección de datos personales en subcontrataciones	SI		
A.4.	¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?	SI		
A.4.1.	Tener un procedimiento de notificación	SI		
A.4.2.	Realizar revisiones y auditorías	SI		Se realizara desarrollo inicial
A.5.	¿Realizas respaldos periódicos de los datos personales?	SI		



B.	Medidas de seguridad en el entorno de trabajo físico			
B.1.	¿Tienes medidas de seguridad para acceder al entorno de Trabajo físico?	SI		
B.1.1.	Alerta del entorno de trabajo	SI		
B.1.2.	Mantener registros del personal con acceso al entorno de trabajo	SI		
B.2.	¿Tienes medidas de seguridad para evitar el robo?	SI		
B.2.1.	Cerraduras y candados	SI		
B.2.2.	Elementos disuasorios	SI		
B.2.3.	Minimizar el riesgo oportunista	SI		

LA GESTIÓN DE VULNERACIONES

Las acciones para GESTIONAR la vulneración son:

- a) El Encargado elabora y entrega un informe al Responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados.
- b) El incidente se registra en el formato, su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente.
- c) En caso de robo o extravío de datos personales, el Responsable del sistema, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que, en el ámbito de sus atribuciones, determine lo conducente.
- d) Informar a los titulares de los datos personales lo siguiente:
 1. La naturaleza del incidente.
 2. Los datos personales afectados.
 3. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para protegerse.
 4. Las acciones correctivas realizadas de forma inmediata.
 5. Los medios donde los titulares pueden obtener más información.
 6. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente.
 7. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.



CONSEJO DE LA JUDICATURA

PODER JUDICIAL DEL ESTADO DE JALISCO

- e) Informar al INAI o al organismo garante de la Entidad Federativa correspondiente de la vulneración de seguridad ocurrida.
- f) La actualización del documento de seguridad correspondiente.
- g) Contar con una bitácora de las vulneraciones¹⁴ en la que se describa:
- h) En qué consistió la vulneración.
- i) La fecha en la que ocurrió.
- j) El motivo o causa de la vulneración.
- k) Las acciones correctivas implementadas de forma inmediata y a largo plazo.
- l) La imposición de sanciones por la autoridad correspondiente debido a la falta de implementación de medidas de seguridad.

Se deberá utilizar el formato **(ANEXO 3)** para determinar que las vulneraciones fueron mitigadas.

**LOS MECANISMOS DE MONITOREO Y REVISIÓN DE
LAS MEDIDAS DE SEGURIDAD**

Mecanismo	Medidas de Seguridad	Duración
Diagnostico	Físicas, Administrativas, Técnicas.	30 días
Análisis y revisión	Físicas, Administrativas, Técnicas.	30 días
Auditoria	Físicas, Administrativas, Técnicas.	30 días.
Recomendaciones	Físicas, Administrativas, Técnicas.	30 días.
Informe	Físicas, Administrativas, Técnicas.	30 días.

EL PLAN DE TRABAJO

La identificación del Tratamiento de Datos Personal se crea en cumplimiento de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, debido a que este Sujeto Obligado, recaba, utiliza y conserva dentro de sus registros, en cumplimiento al artículo 87 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.



El presente sistema utiliza el método conocido como Ciclo de Deming o Ciclo PHVA (Planear, Hacer, Verificar y Actuar) que contribuye a la creación e implementación efectiva de dicho sistema.

Con base al modelo del Ciclo de Deming¹ podemos conocer las 4 fases cíclicas que se deben seguir para la implementación del Sistema de Información Pública Protegida:



Ciclo de Deming: Sistema de Protección de Información Confidencial en 4 fases generales.

Con base en ello, para el cumplimiento de cada una de las 4 fases del Ciclo de Deming es necesario definir y desarrollar los pasos a seguir que permitirán darle continuidad al ciclo, en consecuencia, se establecen los pasos que deberán desarrollarse para la consecución del Sistema de Información Pública Protegida:

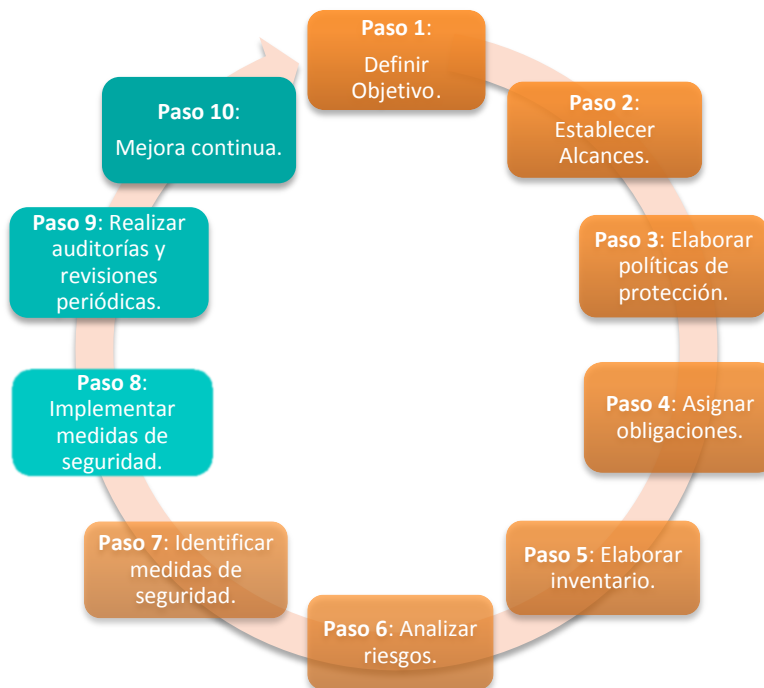
FASES	PASOS
1. Planear el Sistema	1. Objetivo del Sistema. 2. Alcances del Sistema. 3. Políticas para la protección de información confidencial y reservada. 4. Funciones y obligaciones de los servidores públicos que manejan información pública protegida. 5. Inventario de información pública protegida.

¹ Edward Deming es el creador de esta metodología cuyo objetivo es la mejora continua a partir de la implementación cíclica de 4 fases: Planear, Hacer, Verificar y Actuar.



	6. Análisis de riesgos de la información pública protegida. 7. Identificación de las medidas de seguridad.
2. Implementar medidas de seguridad	8. Implementación de las medidas de seguridad aplicables a la información pública protegida.
3. Revisar y Monitorear	9. Revisiones y auditoría
4. Mejora Continua	10. Mejora continua y capacitación

Los 10 pasos anteriores que integran las 4 fases del Ciclo de Deming, se reflejan a su vez por medio del siguiente esquema:

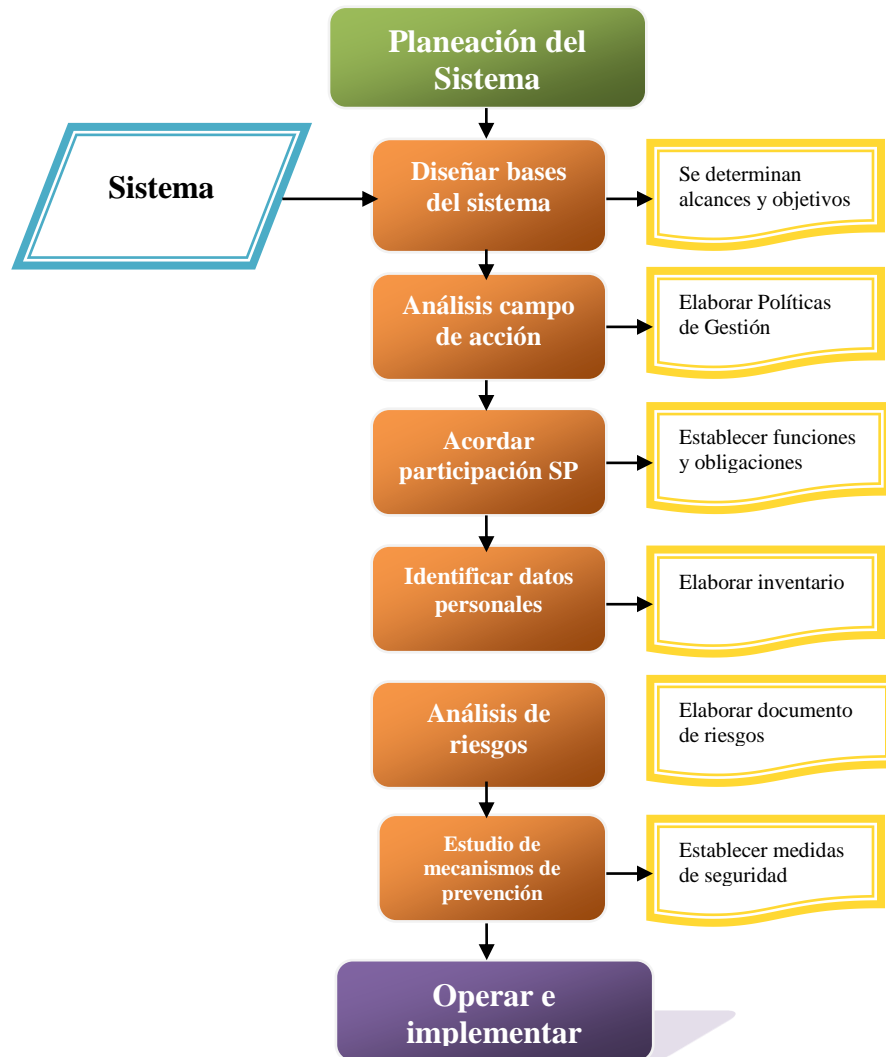




Etapas del sistema de gestión

ETAPA 1. Planear el Sistema de Gestión:

El siguiente cuadro muestra a detalle las etapas que integran la fase de planeación. En color naranja se definen los pasos correspondientes, en azul los fundamentos o documentos que alimentan o provocan el paso, y en amarillo los resultados obtenidos.





EL PROGRAMA GENERAL DE CAPACITACIÓN.

El programa general de capacitación se desarrolla de la siguiente forma:

Capacitación	Duración	Programación
Diplomado en Protección de Datos Personales, Transparencia y Acceso a la Información Pública.	Semestral	Anual
Básico de Protección de Datos Personales	4 horas	Semestral
Medio de Protección de Datos Personales.	4 horas	Semestral
Alto de Protección de Datos Personales.	4 horas	Semestral
Relación de la Protección de Datos Personales en la función judicial.	4 horas	Semestral

EL PLAN DE CONTINGENCIA



Contención del Incidente.

A continuación, se enumeran someramente algunas de las medidas de contención que podrían ser de aplicación en función de cada caso:



CONSEJO DE LA JUDICATURA

PODER JUDICIAL DEL ESTADO DE JALISCO

1. Si es posible, impedir el acceso al origen de la divulgación: dominios, puertos, servidores, la fuente o los destinatarios de la divulgación. Dependiendo del vector de ataque, impedir el acceso al origen: dominios, conexiones, equipos informáticos o conexiones remotas, puertos, parches, actualización del software de detección (antivirus, IDS, etc.) bloqueo de tráfico, deshabilitar dispositivos, servidores, etc.
2. Suspender las credenciales lógicas y físicas con acceso a información privilegiada. Cambiar todas las contraseñas de usuarios privilegiados o hacer que los usuarios lo hagan de manera segura.
3. Hacer una copia del sistema (clonado), hacer una copia bit a bit del disco duro que contiene el sistema, y luego analizar la copia utilizando herramientas forenses.
4. Aislar el sistema utilizado para revelar los datos con el fin de realizar un análisis forense más tarde.
5. Si los datos han sido enviados a servidores públicos, solicitar al propietario (o webmaster) que elimine los datos divulgados. · Si no es posible eliminar los datos divulgados, proporcionar un análisis completo al departamento correspondiente (Legal, Compliance, RRHH, etc.) o a quien ejerza dichas funciones en la empresa.
6. Vigilar la difusión de los documentos/datos filtrados en los diferentes sitios web y redes sociales (FB, Twitter, etc.) así como los comentarios y reacciones de los usuarios de Internet.

Solución y erradicación

Algunos ejemplos de tareas de erradicación podrían ser las que se enumeran a continuación: ·

1. Definir el proceso de desinfección, basado en firmas, herramientas, nuevas versiones/revisiones de software, etc. y probarlo. Asegurar que el proceso de desinfección funciona adecuadamente sin dañar servicios.
2. Comprobar la integridad de todos los datos almacenados en el sistema, mediante un sistema de hashes por ejemplo, que permita garantizar que los ficheros no han sido modificados, especial atención debe ser tenida con relación a los ficheros ejecutables.
3. Revisar la correcta planificación y actualización de los motores y firmas de antivirus.
4. Análisis con antivirus de todo el sistema, los discos duros y la memoria.
5. Restaurar conexiones y privilegios paulatinamente. Especial acceso restringido paulatino de máquinas remotas o no gestionadas. Con objeto de planificar la respuesta al incidente deberá fijarse un plazo para la implementación de las tareas de erradicación.



CONSEJO DE LA JUDICATURA

PODER JUDICIAL DEL ESTADO DE JALISCO

Recuperación.

Esto puede implicar la adopción no solo de medidas activas, sino también implementando controles periódicos y eficaces que permitan el seguimiento pormenorizado de los procesos de mayor riesgo. Identificación y análisis de soluciones (corto, medio, plazo): Se identificarán las distintas soluciones dirigidas a evitar nuevos incidentes de seguridad basados en la misma causa, así como a reducir el riesgo de los mismos. Debe hacerse contraste con las medidas adoptadas para solventar el incidente en cuestión y garantizar un análisis pormenorizado de soluciones.

Selección estratégica: Teniendo en cuenta el riesgo que quiera asumir la entidad, así como la eficiencia y costes de las distintas opciones planteadas, se seleccionará la estrategia que deberá seguirse a futuro.

Implementación (suspensión medidas de contención excepcionales, implementación de medidas preventivas eviten incidente): Implementación de las medidas en base a la estrategia adoptada teniendo en cuenta tanto el proyecto de continuidad de negocio de la entidad como la criticidad y el propio riesgo intrínseco en los activos que hayan sido afectados por el incidente, sin olvidar los procesos afectados y los datos que se tratan en los mismos.

Verificación de recuperación e implementación de medidas: Se garantizará no solo el restablecimiento a la situación previa al incidente, sino que se revisará el análisis de riesgos y se recogerá la implementación en la entidad de controles adicionales y periódicos para evitar futuros incidentes similares.



CONSEJO DE LA JUDICATURA
PODER JUDICIAL DEL ESTADO DE JALISCO

Documento de Seguridad para la Protección de
Datos Personales del Consejo de la
Judicatura del Estado de Jalisco

ANEXO 1

CATÁLOGOS DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Sistema de Tratamiento de la Dirección de Transparencia e Información Pública			
Administrador	Mtro. Hugo Rodríguez Heredia		
Cargo	Coordinador General		
Área	Dirección de Transparencia e Información Pública		
Funciones y obligaciones	<p>1.- Como función principal la de garantizar el acceso de la sociedad a la información que se genera dentro del mismo organismo.</p> <p>2.- Entre sus obligaciones está la de orientar y facilitar al público la consulta y acceso a la información mediante un procedimiento de acceso que inicia con la presentación de la solicitud de información y concluye con la contestación a ésta; se requiere y recaba en las oficinas correspondientes la información pública de las solicitudes procedentes, en caso de negativa de los encargados de las oficinas para entregar información pública de libre acceso se informara al instituto y se remitirá al mismo las que no le corresponda atender, así como el trámite y resolución de las que sí sean de su competencia en sentido afirmativo, afirmativo parcialmente y negativo; en caso de impugnación conocer y resolver el recurso de revisión.</p> <p>Es su deber llevar el registro y estadística de las solicitudes para elaborar, publicar y enviar de forma electrónica, al Instituto un informe mensual de las recibidas, atendidas y resueltas en dicho periodo y proteger la información pública en su poder, contra riesgos naturales, accidentes y contingencias, los documentos y demás medios que contengan información pública; Así como asentar en acta lo discutido y acordado en reuniones y publicar dichas actas, salvo las consideradas como reuniones secretas por disposición legal expresa vigilar que sus oficinas y servidores públicos en posesión de información pública atiendan los requerimientos de su Unidad para dar contestación a las solicitudes presentadas y las demás que establezcan otras disposiciones legales o reglamentarias aplicables.</p>		
Personal autorizado para tratamiento			
Puesto	Nombre	Base de datos	Enumerar las bases de datos
Jefe de Sección	Carlos Valdez Enciso	Física y electrónica	1.- Solicitudes 2.- Correos
Funciones y obligaciones	<p>1.- Recibir Solicitudes de Información por medio de correo, sistema INFOMEX y por medio de comparecencia.</p> <p>2.- Recibir contestaciones de las áreas generadoras de la información.</p> <p>3.- Encargado del correo institucional oficial de la Dirección de Transparencia.</p> <p>4.- Dar contestación final a las solicitudes de información</p>		
Jefe de Sección	Arturo Yolitzin Espinoza Ramírez	Física y electrónica	1. Solicitudes
Funciones y obligaciones	<p>1. Revisar las solicitudes de Derechos ARCO</p> <p>2. Realizar los proyectos para los avisos de privacidad</p> <p>3. Realizar el proyecto del Documento de Seguridad</p> <p>4. Recibir las contestaciones sobre los Derechos ARCO</p> <p>5. Encargado de la realización de proyectos de contestaciones para las solicitudes de Derechos ARCO</p>		
Notificador	Emiliano Briseño Castellanos	Física	1.- Libreta 2.- Oficios en tramite
Funciones y obligaciones	Notificar		
Auxiliar Judicial	Lourdes Karina Martínez Ibarra	Física y Electrónica	1.- Libreta de Expedientes 2.- Libreta de Oficios 3.- Libreta de Asistencia

			4.- Solicitudes 5.- Correos
Funciones y obligaciones	1.- Recibir Solicitudes de Información por medio de correo, sistema INFOMEX y por medio de comparecencia. 2.- Recibir contestaciones de las áreas generadoras de la información. 3.- Revisar el Correo Institucional de la Dirección de Transparencia. 4.- Dar contestación final a las solicitudes de información. 5.- Informar al ITEI mes con mes el total de solicitudes recibidas. 6.- Atención al público, física, electrónica y telefónica.		
Auxiliar Judicial	Laura Castillo Velázquez	Física	1.- Libreta de registro de solicitudes ARCO
Funciones y obligaciones	1.- Gestión y trámite de las solicitudes. 2.- Realizar Actas de Comité de Transparencia		
Auxiliar Judicial	Jorge Armando Chávez Méndez	Física y electrónica	1.- Guardar documentos de Acuses de Oficios de gestión. 2.- Se guarda electrónicamente las solicitudes que se reciben.
Funciones y obligaciones	1.- Dar Contestación a las solicitudes, dar acceso, prevenir o incompetencia sobre la solicitud. 2.- Gestionar ante las áreas generadoras de la información sobre la petición del solicitante.		
Auxiliar Judicial	Cesar Giovanni Zavala Ávila	Física y electrónica	1.- Guardar documentos de Acuses de Oficios de gestión. 2.- Se guarda electrónicamente las solicitudes que se reciben.
Funciones y obligaciones	1.- Dar Contestación a las solicitudes, dar acceso, prevenir o incompetencia sobre la solicitud. 2.- Gestionar ante las áreas generadoras de la información sobre la petición del solicitante.		
Tipo de datos personales			
Inventario	Nombres Domicilio Teléfono Correo electrónico Copias de INE/IFE		
Base de datos			
No. De titulares			
Controles de seguridad para las bases de datos	<p>ÖSQ 000UKQ+!{ asb) Ü^·^!cææCEæ ÄI ÉÁ:æææ) ÅÄ ä 8æ [ÅDÛVÖDÖRT ÉÄÜ^*!ææ/Å^Ä! · Åææ · Å^!·[} æ^·ÉÄ Qåææææææ) åææ) Å^Ä! · Åææ · ÅÄ^Ä [ä!öæ) &] dæÄ] ^ } d · Å..äæ · É</p>		
Estructura y descripción del Sistema			
Tipo de soporte	Física y Electrónica	<p>ÖSQ 000UKQ+!{ asb) Ü^·^!cææCEæ ÄI ÉÁ +æææ) ÅÄ 8æ [ÅDÛVÖDÖRT ÉÄÜ^*!ææ/Å^Ä! · Å åææ · Å^!·[} æ^·ÉÄ Qåææææææ) åææ) Å^Ä! · Åææ · ÅÄ^Ä [ä!öæ) &] dæÄ ^ Å^Ä [ä!öæ) &] dæÄ ^ } d · Å..äæ · É</p>	
Características del lugar de resguardo			
Programas en que se utilizan los D.P.	Word Excel		

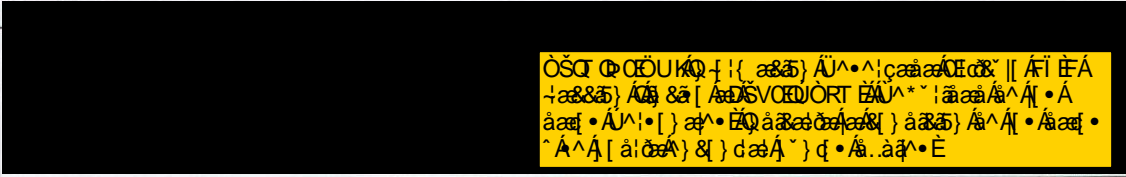

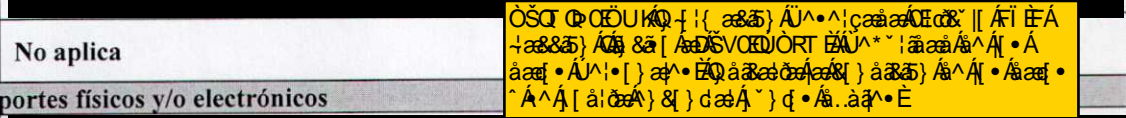
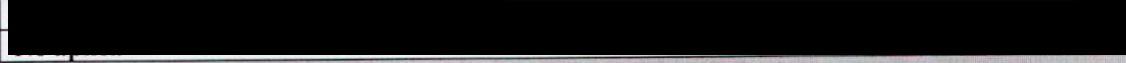
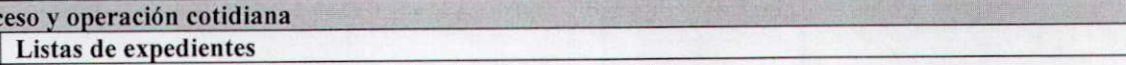
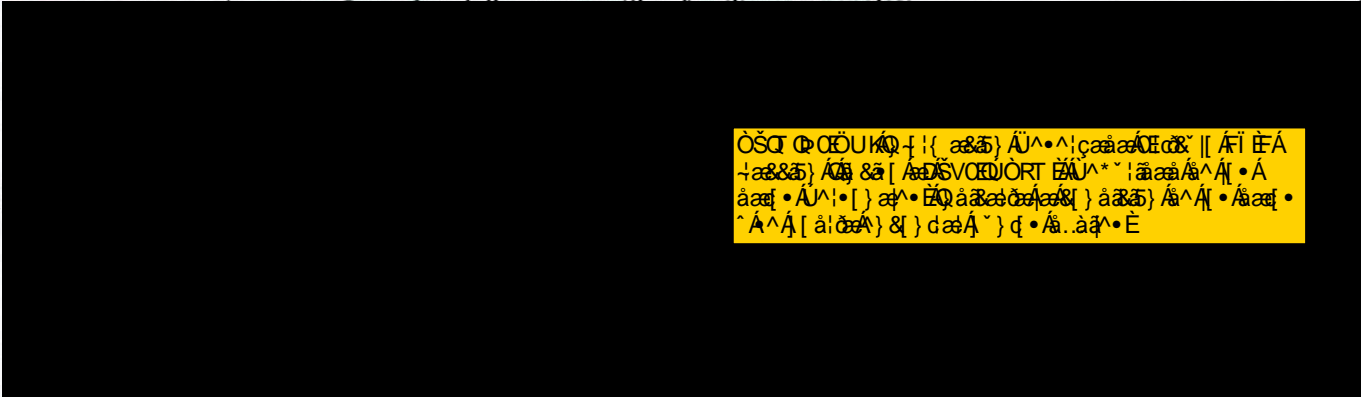
	Nitro Dropbox	
Resguardo de los soportes físicos y/o electrónicos		
Físicos		
Electrónicos		
Las bitácoras de acceso y operación cotidiana		
Bitácoras físicas		
Clave de la bitácora		
Bitácoras electrónicas		
Clave de la bitácora		
Las bitácoras de Vulneraciones de seguridad		
ID	SOPORTE	RESPONSABLE

Programas en que se utilizan los D.P.	CAPACITACIÓN.	
Resguardo de los soportes físicos y/o electrónicos		
Físicos	[REDACTED]	
Electrónicos	[REDACTED]	
Las bitácoras de acceso y operación cotidiana		
Bitácoras físicas	[REDACTED]	
Clave de la bitácora	[REDACTED]	
Bitácoras electrónicas	[REDACTED]	
Clave de la bitácora	[REDACTED]	
Las bitácoras de Vulneraciones de seguridad		
ID	SOPORTE	RESPONSABLE
[REDACTED]		

DEPARTAMENTO DE AUXILIARES DE LA ADMINISTRACIÓN DE JUSTICIA			
Administrador	LIC. JEANETT LETICIA CARRILLO MAGDALENO	DIRECCIÓN DE FORMACIÓN Y ACTUALIZACIÓN JUDICIAL	UNA BASE DE DATOS
Cargo	JEFA DE DEPARTAMENTO		
Área	DEPARTAMENTO DE AUXILIARES DE LA ADMINISTRACIÓN DE JUSTICIA		
Funciones y obligaciones	<ul style="list-style-type: none"> <input type="checkbox"/> Elaborar plan de trabajo anual tanto administrativo como de difusión, operativo y académico. <input type="checkbox"/> Acordar con el personal a su cargo los programas de trabajo. <input type="checkbox"/> Proponer la convocatoria anual para ingreso de peritos <input type="checkbox"/> Proponer los formatos de ingreso de documentos para el proceso de recepción de documentos durante la convocatoria <input type="checkbox"/> Integrar, resguardar y mantener actualizados los expedientes de los auxiliares de la administración de justicia. <input type="checkbox"/> Emitir opiniones sobre el ingreso y permanencia de los Auxiliares de Administración de Justicia después de analizar la documentación ingresada durante la convocatoria. <input type="checkbox"/> Publicar la nueva lista de auxiliares de la administración de la justicia. <input type="checkbox"/> Llevar a cabo los registros pertinentes de su área. <input type="checkbox"/> Recibir y analizar los informes cuatrimestrales de las actividades de los auxiliares. <input type="checkbox"/> Acordar los informes cuatrimestrales <input type="checkbox"/> Registrar en base de datos los acuerdos de peritos <input type="checkbox"/> Vigilar a través de la revisión periódica y sistemática, la conducta de los auxiliares de la administración de justicia en el ejercicio de sus funciones, mediante el boletín judicial, informes y tomando muestras aleatorias de expedientes que reportan la intervención pericial. <input type="checkbox"/> Vigilar a través de visitas a los 32 partidos judiciales, los expedientes en los que haya intervención de peritos para detectar posibles irregularidades <input type="checkbox"/> Entrevistarse con jueces y demás personal de juzgados a efectos de conocer la función pericial, su cumplimiento o incumplimiento en cada juzgado. <input type="checkbox"/> Atender, integrar, remitir las quejas presentadas en contra de los auxiliares de la administración de justicia a la Comisión de Carrera Judicial. <input type="checkbox"/> Promueve la actualización de conocimientos y habilidades de los auxiliares de la Administración de Justicia, según el área de especialización. <input type="checkbox"/> Difunde las actividades del Departamento, como: Listas de Peritos de c/año, eventos Académicos mediante Internet, vía telefónica o por oficio. Celebrar reuniones con: <ul style="list-style-type: none"> <input type="checkbox"/> Peritos. <input type="checkbox"/> Jueces. <input type="checkbox"/> Instituciones Para unificar criterios y la elaboración de proyectos, propuestas de cursos, conferencias, etc. <input type="checkbox"/> Programar y operatividad la Semana de la Salud de cada año. 		
Personal autorizado para tratamiento			
Nombre del puesto	Victor Manuel Santos Inchaurregui	LISTA PERITOS	UNA BASE DE DATOS

DEPARTAMENTO DE PSICOLOGÍA Y EVALUACIÓN			
Administrador	L.P.O. ANGÉLICA CASTILLEJA PÉREZ	PSICOLOGÍA Y EVALUACIÓN Ver 1.0	UNA BASE DE DATOS
Cargo	JEFA DE DEPARTAMENTO		
Área	DEPARTAMENTO DE PSICOLOGÍA Y EVALUACIÓN		
Funciones y obligaciones	<ul style="list-style-type: none"> <input type="checkbox"/> Definir y diseñar los perfiles intelectuales, psicológicos y neuropsicológicos de los aspirantes a ocupar los diferentes puestos en base al conocimiento científico de las ciencias del comportamiento y neurociencias y aquellos criterios que determine el Consejo de la Judicatura y la Ley Orgánica del Poder Judicial del Estado. <input type="checkbox"/> Diseñar protocolos y seleccionar las baterías psicométricas que ostenten mayor grado de confiabilidad, validez y actualidad para la evaluación de los aspirantes. <input type="checkbox"/> Valorar e interpretar los resultados de las pruebas psicométricas aplicadas a los aspirantes. <input type="checkbox"/> Emitir el dictamen correspondiente a cada aspirante especificando el estatus de "Recomendable" o "No Recomendable" según se advierta en base a los perfiles aprobados para cada puesto. <input type="checkbox"/> Realizar entrevista psicológica a todos los evaluados para complementar la valoración de los resultados de las pruebas psicométricas. <input type="checkbox"/> Entrevistar y valorar a los aspirantes que integran la bolsa de trabajo. <input type="checkbox"/> Actualizar permanentemente las baterías psicométricas, perfiles y descripciones de puestos que así se requiera. <input type="checkbox"/> Solicitar calificaciones de conocimientos a la Dirección de Formación y Actualización Judicial. <input type="checkbox"/> Proporcionar retroalimentación sobre los resultados obtenidos en las pruebas psicométricas a los titulares que así lo soliciten. <input type="checkbox"/> Proporcionar a Movimientos de Personal, los resultados de las evaluaciones para propuestas de Pleno. <input type="checkbox"/> Salvaguardar la confidencialidad de los resultados y la información obtenida en las entrevistas y pruebas psicométricas. <input type="checkbox"/> Supervisar la elaboración de reportes semanales y firmarlos de Vo. Bo. <input type="checkbox"/> Mantener contacto continuo con la Dirección de Formación y Actualización Judicial sobre los procedimientos, actividades y proyectos que se lleven a cabo en el Departamento. <input type="checkbox"/> Dar retroalimentación y seguimiento continuo al trabajo del personal que integra el Departamento. <input type="checkbox"/> Revisar y optimizar los sistemas y procedimientos de trabajo dentro del Departamento, así como diseñar nuevas formas de actuación encaminados al mejoramiento continuo y la eficiencia. <input type="checkbox"/> Apoyo en la exposición de un curso referente a las relaciones humanas, cuando se solicite por parte de la Dirección de Formación y Actualización Judicial. <input type="checkbox"/> Proponer temas que puedan ser impartidas tanto para fortalecer el lado humano del personal del Consejo, como temas de actualidad que nutran la función cotidiana que desempeñan. <input type="checkbox"/> Apoyo en guardias y eventos tanto dentro del horario de trabajo como fuera de él. <input type="checkbox"/> Apoyo a la Dirección y demás departamentos que la conforman en lo que soliciten. 		
Personal autorizado para tratamiento			
Nombre del puesto	ALMA KARINA ROMERO MACÍAS ANALISTA ESPECIALIZADO	PSICOLOGÍA Y EVALUACIÓN Ver 1.0	UNA BASE DE DATOS

Estructura y descripción del Sistema		
Tipo de soporte	[REDACTED]	
Características del lugar de resguardo	[REDACTED]	
Programas en que se utilizan los D.P.	PSICOLOGÍA Y EVALUACIÓN Ver 1.0	
Resguardo de los soportes físicos y/o electrónicos		
Físicos	[REDACTED]	
Electrónicos	[REDACTED]	
Las bitácoras de acceso y operación cotidiana		
Bitácoras físicas	[REDACTED]	
Clave de la bitácora	[REDACTED]	
Bitácoras electrónicas	[REDACTED]	
Clave de la bitácora	[REDACTED]	
Las bitácoras de Vulneraciones de seguridad		
ID	SOPORTE	RESPONSABLE
[REDACTED]	[REDACTED]	[REDACTED]

Sistema de tratamiento de la Unidad Departamental de Archivo	
Administrador	LIC. JOSÉ GUSTAVO CHÁVEZ LOZA
Cargo	Jefe de la Unidad Departamental de Archivo del Consejo de la Judicatura del Estado de Jalisco.
Área	Dirección de Oficialía de Partes, Archivo y Estadística del Consejo de la Judicatura del Estado de Jalisco.
Funciones y obligaciones	Se puede consultar en la siguiente liga: https://docs.google.com/viewer?url=http://cjj.gob.mx/files/transparencia/fraccion4/ART8_FRACIV_I NCISOC.PDF
Personal autorizado para tratamiento	
Nombre del puesto	Jefe de Sección de la Unidad Departamental de Archivo
Funciones y obligaciones	Se puede consultar en la siguiente liga: https://docs.google.com/viewer?url=http://cjj.gob.mx/files/transparencia/fraccion4/ART8_FRACIV_I NCISOC.PDF
Nombre del puesto	Auxiliares Judiciales
Funciones y obligaciones	Se puede consultar en la siguiente liga: https://docs.google.com/viewer?url=http://cjj.gob.mx/files/transparencia/fraccion4/ART8_FRACIV_I NCISOC.PDF
Tipo de datos personales	
Inventario	expedientes
Base de datos	Listas físicas y cuadernos
No. De titulares	
Controles de seguridad para las bases de datos	
Estructura y descripción del Sistema	
Tipo de soporte	Físico
Características del lugar de resguardo	
Programas en que se utilizan los D.P.	No aplica
Resguardo de los soportes físicos y/o electrónicos	
Físicos	
Electrónicos	
Las bitácoras de acceso y operación cotidiana	
Bitácoras físicas	Listas de expedientes
	

Sistema de tratamiento Unidad Departamental de Oficialía de Partes Común			
Administrador	ITZCOATL CASTAÑEDA FLETES	ADMINISTRADOR DE JUZGADOS VERSION 6.0 CONSULTA P. LISTAS DE DOCUMENTOS RECIBIDOS EN JUZGADO.	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE.
Cargo	JEFE DE UNIDAD DEPARTAMENTAL		
Área	DIRECCIÓN DE OFICIALIA DE PARTES, ARCHIVO Y ESTADISTICA.		
Funciones y obligaciones	<ul style="list-style-type: none"> - ADMINISTRACION DE RECURSOS MATERIALES DISPONIBLES. - ADMINISTRACION DEL PERSONAL ADSCRITO A LA UNIDAD. - SUPERVISAR EL DESEMPEÑO LABORAL DEL PERSONAL ASIGNADO A LA UNIDAD. - VERIFICACION Y AUTORIZACION DE TURNOS MANUALES. - ENVIO DE LISTADO DE DEMANDAS NUEVAS PARA SU PUBLICACION AL BOLETIN JUDICIAL. - GESTION DE RECURSOS MATERIALES Y HUMANOS. 		
Personal autorizado para tratamiento			
Nombre del Puesto JEFE DE SECCIÓN	JUAN PABLO DELGADILLO ENCARNACIÓN.	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE.
Funciones y obligaciones	<ul style="list-style-type: none"> -SUPERVISIÓN DE PERSONAL. - REVISION DE RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO - CAPTURA DE DATOS EN SISTEMA. 		
Nombre del puesto AUXILIAR ADMINISTRATIVO	ANGELA MATILDE ESTRADA PANTOJA	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE.
Funciones y obligaciones	<ul style="list-style-type: none"> -RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO - CAPTURA DE DATOS EN SISTEMA 		
Nombre del puesto AUXILIAR ADMINISTRATIVO	OLGA ELIZABETH ORTIZ GONZALEZ	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE.
Funciones y obligaciones	<ul style="list-style-type: none"> -RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO - CAPTURA DE DATOS EN SISTEMA 		
Nombre del puesto AUXILIAR ADMINISTRATIVO	BRENDA BERENICE FLORES PULIDO	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE.
Funciones y obligaciones	<ul style="list-style-type: none"> -RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO - CAPTURA DE DATOS EN SISTEMA 		

Nombre del puesto AUXILIAR ADMINISTRATIVO	CAROLINA GUADALUPE ORTIZ GONZALEZ	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE.
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO - CAPTURA DE DATOS EN SISTEMA		
Nombre del puesto AUXILIAR ADMINISTRATIVO	ENRIQUE PADILLA CORDOVA	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	BERTHA ALICIA OCAMPO PADILLA	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	MARIA MARGARITA BARRIOS LOPEZ	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	ROSA MARIA CAMPOS TORRES	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	LILIA MARGARITA GUERRERO DEL TORO	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	GUSTAVO CESAR DELGADO PEREZ	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	JOSE ARTURO LOPEZ ARAUJO	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE

Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	ESTELA RAMOS GUZMAN	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	IGNACIO ALEJANDRO RAMOS MEJIA	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	RAFAEL RUVALCABA VEGA	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	MARIA ISELA DIAZ NUÑEZ	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	EDGAR OMAR ALVARADO GARCIA	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	ROBERTO RODRIGUEZ GONZALEZ	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Nombre del puesto AUXILIAR ADMINISTRATIVO	GUILLERMO GALICIA ARELLANO	ADMINISTRADOR DE JUZGADOS VERSION 6.0	NOMBRE DE PARTES EN UN JUICIO, JUZGADO Y NUMERO DE EXPEDIENTE
Funciones y obligaciones	-RECEPCION DE DOCUMENTOS - TURNO ELECTRONICO		
Tipo de datos personales			
Inventario	-NOMBRES DE PARTES EN JUICIOS. -TIPO DE JUCIO. JUZGADO QUE CONOCE DEL ASUNTO		

Base de datos	ADMINISTRADOR DE JUZGADOS VERSION 6.0	
No. De titulares	[REDACTED]	
Controles de seguridad para las bases de datos	[REDACTED]	
Estructura y descripción del Sistema		
Tipo de soporte	ELECTRONICO.	
Características del lugar de resguardo	[REDACTED]	
Programas en que se utilizan los D.P.	ADMINISTRADOR DE JUZGADOS VERSION 6.0 CONSULTA P.	
Resguardo de los soportes físicos y/o electrónicos		
Físicos	[REDACTED]	
Electrónicos	[REDACTED]	
Las bitácoras de acceso y operación cotidiana		
Bitácoras físicas	[REDACTED]	
Clave de la bitácora	[REDACTED]	
Bitácoras electrónicas	[REDACTED]	
Clave de la bitácora	[REDACTED]	
Las bitácoras de Vulneraciones de seguridad		
ID	SOPORTE	RESPONSABLE
[REDACTED]	[REDACTED]	[REDACTED]

SISTEMA DE TRATAMIENTO – Unidad Departamental de Talento Humano			
Administrador	Miguel Abundis Sánchez	Base de datos	-Sistema kardex -Archivos de office
Cargo	Jefe de Unidad Departamental		
Área	Dirección de Planeación, Administración y Finanzas		
Funciones y obligaciones	Administrar y ejecutar eficientemente los movimientos del personal en base a las plazas ya erogadas y normatividad vigente.		
Personal autorizado para tratamiento			
Nombre del puesto	Gómez Vejar Emma	Base de datos	-Sistema Kardex -Archivos De Office
Funciones y obligaciones	-Puesto auxiliar judicial de consejero -Dar seguimiento a las licencias económicas, guardar documentos en el archivo del área, contestar los oficios del área de dirección de Visitaduría, disciplina y responsabilidades y secretaria técnica del órgano interno de control.		
Nombre del puesto	DE LA TORRE MARTINEZ EMILIA ADRIANA	Base de datos	-SISTEMA KARDEX -ARCHIVOS DE OFFICE
Funciones y obligaciones	-PUESTO AUXILIAR ADMINISTRATIVO -VENTANILLA DE TALENTO HUMANO - RECIBIR Y ENTREGAR TODOS LOS OFICIOS QUE LLEGAN Y SE ENTREGAN CON INFORMACION POR PARTE DE LA UNIDAD DEPARTAMENTAL DE TALENTO HUMANO.		
Nombre del puesto	ESTRADA JIMENEZ MARISELA	Base de datos	-SISTEMA KARDEX -ARCHIVOS DE OFFICE
Funciones y obligaciones	-PUESTO SECRETARIA "B" -DAR SEGUIMIENTO Y CONTESTACION A LOS OFICIOS PLENARIOS, CONTESTAR LOS OFICIOS DE FISCALIA Y LAS DIFERENTES COMISIONES DE ESTE H. CONSEJO DE LA JUDICATURA, ELABORAR HOJA DE SERVICIO, ELABORAR CARTAS DE NO ADEUDO IPEJAL Y SEDAR Y CIRCULAR LA INFORMACION INTERNA DE TALENTO HUMANO.		
Nombre del puesto	LOPEZ GONZALEZ MARTHA LETICIA	Base de datos	-SISTEMA KARDEX -ARCHIVOS DE OFFICE
Funciones y obligaciones	-PUESTO AUXILIAR DE COMPUTO -ENTREGAR LA NOMINA QUINCENAL Y COMPLEMENTARIAS A LAS DIFERENTES AREAS DE ESTE H. CONSEJO DE LA JUDICATURA, LLEVAR EL CONTROL DE LAS NOMINAS ENTREGADAS Y RECIBIDAS EN ORIGINAL, REALIZAR OFICIOS PARA SOLICITAR LAS NOMINAS PENDIENTES DE REGRESAR EN ORIGINAL Y FIRMADAS, ARCHIVAR Y ESCANEAR DICHAS NOMINAS.		
Nombre del puesto	MORENO SANCHEZ PATRICIA	Base de datos	-SISTEMA KARDEX -ARCHIVOS DE OFFICE
Funciones y obligaciones	-PUESTO AUXILIAR ADMINISTRATIVO -TENER AL DIA EL ARCHIVO DE EXPEDIENTES PERSONALES DE LOS SERVIDORES PUBLICOS DE ESTE H. CONSEJO DE LA JUDICATURA (ARCHIVAR, REGISTRAR, ALTAS, BAJAS, ETC.).		
Nombre del puesto	VALLE CHAVEZ OSCAR ARMANDO	Base de datos	-SISTEMA KARDEX -ARCHIVOS DE OFFICE
Funciones y obligaciones	-PUESTO AUXILIAR JUDICIAL DE CONSEJERO -TENER AL DIA EL ARCHIVO DE EXPEDIENTES PERSONALES DE LOS SERVIDORES PUBLICOS DE ESTE H. CONSEJO DE LA JUDICATURA (ARCHIVAR, REGISTRAR, ALTAS, BAJAS, ETC.).		
Nombre del puesto	SANCHEZ FLORES IRMA LETICIA	Base de datos	-SISTEMA KARDEX -ARCHIVOS DE OFFICE
Funciones y	-PUESTO ANALISTA ESPECIALIZADO		

Controles de seguridad para las bases de datos		
Estructura y descripción del Sistema		
Tipo de soporte	SOPORTE FISICO Y ELECTRONICO	
Características del lugar de resguardo		
Programas en que se utilizan los D.P.	EXCEL, WORD, NITRO-PDF Y KARDEX	
Resguardo de los soportes físicos y/o electrónicos		
Físicos		
Electrónicos		
Las bitácoras de acceso y operación cotidiana		
Bitácoras físicas		
Clave de la bitácora		
Bitácoras electrónicas		
Clave de la bitácora		
Las bitácoras de Vulneraciones de seguridad		
ID	SOPORTE	RESPONSABLE

Administrador	Nora Yadira Tapia Hernández		
Cargo	Jefe de Sección		
Área	Dirección de Contraloría		
Funciones y obligaciones	<p>Reglamento Interno del Consejo de la Judicatura del Estado de Jalisco Artículo 63.- Son atribuciones de la Jefatura de Control Patrimonial.</p> <p>IV. Informar al Director respecto de las irregularidades que lleguen a detectar en el uso de los bienes que los servidores públicos del Consejo tengan a su resguardo.</p> <p>V. Resguardar y registrar las Declaraciones Patrimoniales presentadas por los Servidores Públicos obligados.</p> <p>VI. Informar al Director irregularidades que surjan con motivo del ejercicio de las facultades señaladas en el inciso anterior.</p> <p>VII. Presentar los informes y los resultados de las encomiendas que le sean requeridos por el Pleno, sus Comisiones o su Director.</p> <p>VIII. Las demás contenidas en la Ley, el Reglamento y las que le asigne el Pleno mediante acuerdos generales.</p> <p>Otros:</p> <ul style="list-style-type: none"> • Revisar los expedientes de los funcionarios públicos, verificando las declaraciones patrimoniales para detectar si existe alguna irregularidad. • Revisar las observaciones con el apoyo del Jefe Inmediato, notificándole al Servidor Público que tiene que presentarse para la aclaración de dudas respecto de su declaración patrimonial. • Elaborar y enviar oficios al Pleno de los Servidores Públicos que no presentaron su declaración patrimonial en tiempo y forma para que cumplan con la obligación de presentar la misma. • Controlar y llevar un registro de los Servidores Públicos que cumplieron en entregar su declaración patrimonial, en tiempo y forma. • Asignar folio a cada declaración patrimonial y capturar en sistema, para imprimir posteriormente la información sobre folios capturados. • Realizar auditorías a los Juzgados y Órganos Administrativos levantando las actas con los Servidores Públicos, respectivos, para detectar necesidades e incumplimientos en la Ley Orgánica y Reglamento Interno del Consejo. • Elaborar el borrador de los dictámenes y pliegos para dar a conocer las observaciones a los Titulares de los Juzgados y Órganos Administrativos auditados. • Apoyar a la titular en la elaboración de encomiendas especiales a la Dirección. • Apoyar a los Auditores, Jefe de Sección y Director para lograr mejores resultados en las auditorías. • Realizar revisiones físicas del mobiliario patrimonio del Consejo para su seguimiento y correcto control. • Realizar revisiones de declaraciones patrimoniales para la vigilancia de las normas de los funcionarios públicos. • Elaborar actas circunstanciadas haciendo la reseña de los hechos sucedidos en las distintas actuaciones de la contraloría para dar cumplimiento a lo dispuesto en el Reglamento Interno del Consejo como la Ley de los Servidores Públicos. • Informar mediante dictámenes las observaciones encontradas en las revisiones a los Juzgados y Órganos Administrativos del Consejo y dar seguimiento a las mismas. 		

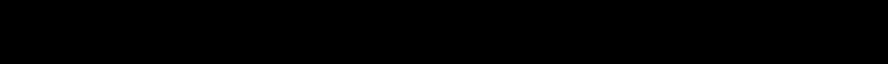
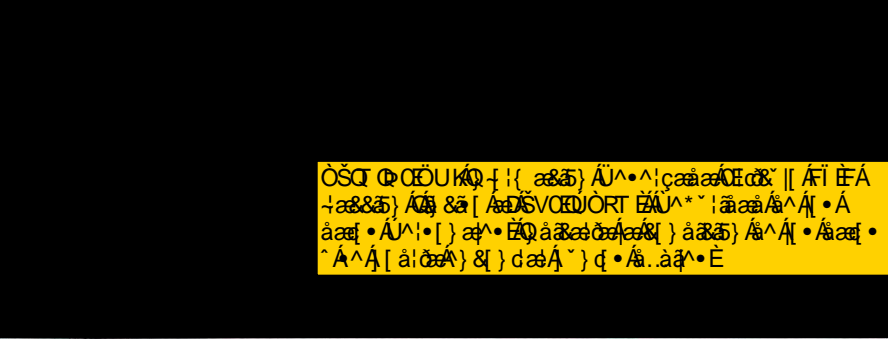
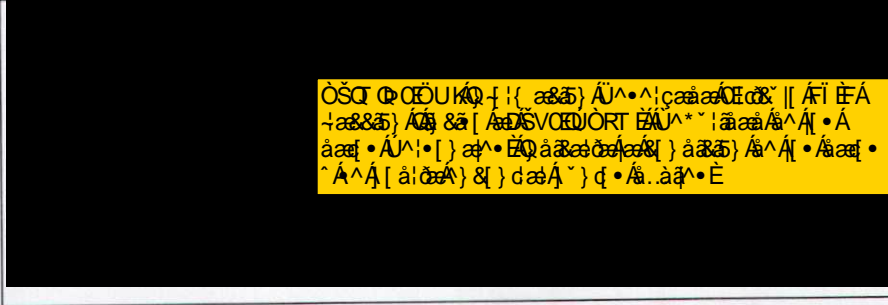
Personal autorizado para tratamiento			
Nombre del puesto	Rosa Lorena Robles Moran Auxiliar de Computo		
Funciones y obligaciones	<ul style="list-style-type: none"> • Abrir expediente de inventario de bienes muebles de cada Dependencia adscrita al Consejo en caso de ser necesario. • Preparar los expedientes de la dependencia que se va a auditar, de acuerdo al calendario de auditorías, para que el Auditor realice la auditoría correspondiente. • Archivar en el expediente una vez concluida la auditoría, el inventario final, las bajas (sí existen) y carta de resguardo, así como las observaciones hechas por los Auditores. • Cuidar que el archivo del Departamento de Control Patrimonial se encuentre actualizado. • Apoyar en la renovación del archivo de declaraciones patrimoniales, ordenando por año y checando las declaraciones hechas por los funcionarios. • Preparar las carpetas necesarias para llevar a cabo las auditorias proporcionando papelería, datos generales de la dependencia a auditar necesarias para que la auditoría, se realice eficientemente. • Elaborar oficios para los Titulares de las dependencias en donde se auditará, para informar la fecha en que se realizará y en caso de ser necesario entregando dicho oficio directamente en el Juzgado o Dirección correspondiente. • Apoyar en cualquier actividad que se requiera en la Dirección. 		
Nombre del puesto	Alma Estela Flores Ibarra Auxiliar Judicial de Consejero		
Funciones y obligaciones	<ul style="list-style-type: none"> • Elaborar los oficios relacionados con la Dirección. • Recibir correspondencia, recepcionarla. • Atender el teléfono • Archivar documentación en general. • Tramitar viáticos. • Comprobación de viáticos. • Realizar revisiones de declaraciones patrimoniales para la vigilancia de las normas de los funcionarios públicos. • Entregar comprobantes de gastos del fondo revolvente a la Unidad Departamental de Tesorería para que se expida el cheque correspondiente. • Apoyar en cualquier actividad que se requiera en la Dirección. 		
Tipo de datos personales			
Inventario	<ol style="list-style-type: none"> 1. Nombre 2. RFC 3. Fecha de Nacimiento 4. Edad 5. Lugar de Nacimiento 6. Nacionalidad 7. Estado Civil 8. Domicilio particular 9. Ciudad y Estado 10. Colonia 11. Código Postal 		

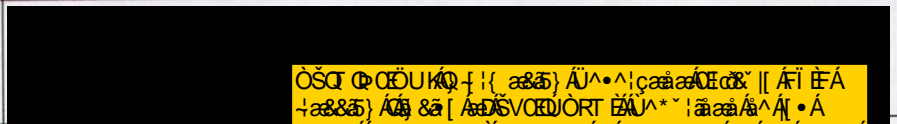

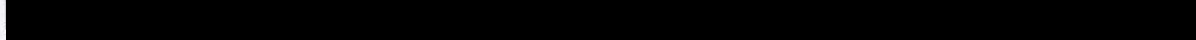
Administrador	Raquel Pérez Haro	N/A	
Cargo	Jefa de Sección de Auditoría Interna		
Área	Dirección de Contraloría		
Funciones y obligaciones	<p>Artículo 62 del Reglamento Interno del Consejo de la Judicatura del Estado de Jalisco.</p> <ul style="list-style-type: none"> • Efectuar la revisión periódica y sistemática de las actividades administrativas del Consejo, la cual deberá regirse bajo los principios de integridad, objetividad, independencia, responsabilidad, profesionalismo, honradez, normatividad, competencia, actualización profesional, difusión, colaboración, respeto y conducta ética, con el objeto de procurar la eficiencia y el fortalecimiento de las Direcciones y áreas que las conforman; • Informar al Director mediante un reporte emitido sobre las diferencias o irregularidades que detecte en las auditorías que practique; realizando las observaciones y proponga las sugerencias que le permitan ejecutar las acciones correctivas; • Apoyar a cualquier área del Consejo para mejorar la administración y consultarle acerca del aprovechamiento de sus recursos; • Intervenir en los diferentes órganos dependientes del Consejo, cuando surja algún problema de la competencia de esta Dirección; • Presentar los informes y los resultados de las encomiendas que le sean requeridos por el Pleno, sus Comisiones o su Director; y • Las demás contenidas en la Ley, el Reglamento y las que le asigne el Pleno mediante acuerdos generales. <p>Artículo 62 del Reglamento Interno del Consejo de la Judicatura del Estado de Jalisco.</p> <p>Otros</p> <ul style="list-style-type: none"> • Definir los esquemas sobre la revisión a los procesos administrativos y sus controles de los órganos del Consejo, a partir de la normatividad que rija a estos, considerando los resultados de las auditorías practicadas con anterioridad y las normas regulatorias de la función de auditoría; <u>del Consejo de</u> • Supervisar a los Auditores en la correcta ejecución de las auditorías programadas; • Llevar a cabo auditorías a los órganos administrativos del Consejo verificando que se cumpla con los controles y normas legales de funcionamiento administrativo. • Requerir la información, documentación y controles que considere necesarios para el desarrollo de la auditoría; • Formular las observaciones y recomendaciones que incidan en la mejora de los procesos técnico-administrativos de los órganos dependientes del Consejo; • Requerir y dar seguimiento al cumplimiento de las recomendaciones a los órganos auditados para su solventación • Supervisar la entrega de papel factura a los órganos Jurisdiccionales que así proceda, así como el registro que permita el control total de los números de folio que se entreguen, así mismo de aquellos utilizados y de los que hubieren sido inutilizados. • Supervisar el control de las copias del papel factura sin utilizar, el utilizado, así como de las facturas canceladas que remitan los juzgados en orden consecutivo; • Supervisar el control de las actas entrega recepción de los servidores 		

	públicos del Consejo de la Judicatura, en las que interviene personal de la Dirección de Contraloría.	
Personal autorizado para tratamiento		
Nombre del puesto	María Cristina de la Peña Gómez.- Auxiliar Judicial de Consejero	N/A
Funciones y obligaciones	<p>I. Preparar las carpetas necesarias para llevar a cabo las auditorías proporcionando papelería, datos generales de la dependencia a auditar necesarias para que la auditoría, se realice eficientemente.</p> <p>II. Capturar conteniendo la plantilla del personal y los datos que se necesitan para llevar a cabo la mencionada auditoría.</p> <p>III. Elaborar oficios para los Titulares de las dependencias en donde se auditará.</p> <p>IV. Elaborar oficios para la entrega de pliegos de observaciones y recomendaciones y de informes finales.</p> <p>V. Archivar los expedientes de las auditorías realizadas a órganos jurisdiccionales y administrativos.</p> <p>VI. Registrar y archivar los reportes que envían los juzgados sobre la utilización o no utilización de papel seguridad factura.</p> <p>VII. Realizar los oficios de dotación del papel seguridad factura cuando sea requerido por los titulares de juzgados.</p> <p>VIII. Registrar y archivar las actas entrega recepción que se reciban en la Dirección de Contraloría.</p>	
Tipo de datos personales		
Inventario	<p>En actas de auditoría: Nombre de servidores públicos, puestos, número y tipo de identificación; Títulos de propiedad; Documentos mercantiles.</p> <p>En actas de entrega-recepción: Nombre de servidores públicos, puestos, número y tipo de identificación, domicilio.</p> <p>En facturas utilizadas: Nombres de parte actora y demandada y bienes muebles adjudicados.</p>	
Base de datos	<p>Listado de actas entrega recepción.</p> <p>Registro de papel factura entregado.</p> <p>Registro de reportes del papel factura utilizado.</p> <p>Facturas escaneadas.</p>	
No. de titulares	[REDACTED]	
Controles de seguridad para las bases de datos	[REDACTED]	
Estructura y descripción del Sistema		
Tipo de soporte	<p>En actas de auditoría: Soporte físico.</p> <p>En actas de entrega-recepción: Soporte físico.</p> <p>En facturas utilizadas: Soporte físico y electrónico (facturas escaneadas).</p>	
Características del lugar de resguardo	[REDACTED]	
Programas en que se utilizan los D.P.	N/A	
Resguardo de los soportes físicos y/o electrónicos		
Físicos	[REDACTED]	

Sistema De Tratamiento			
Dirección de Visitaduría, Disciplina y Responsabilidades			
Administrador	Rosalinda Hernández Arias		
Cargo	Directora		
Área	Dirección de Visitaduría, Disciplina y Responsabilidades		
Funciones y obligaciones	Las Señaladas por la Ley General de Responsabilidades Administrativas, ley Orgánica del Poder Judicial del Estado de Jalisco y la Ley de Responsabilidades Políticas y Administrativas del Estado de Jalisco		
Personal autorizado para tratamiento			
Secretario Relator	<ul style="list-style-type: none"> Gerardo Sandoval Tovar 	1.- Sistema de control interno de procedimientos de quejas 2.- Expedientes de procedimientos administrativos 3.- Libretas de registro.	1.- Físicos y Electrónicos
Funciones y obligaciones	I.- Sustanciará el procedimiento, desde su instauración, etapa de admisión, instrucción, desahogo de pruebas, alegatos II.- Asegurar el adecuado desarrollo de los procedimientos administrativos de responsabilidad. IV.- Realizará los proyectos de resolución de los procedimientos de responsabilidad administrativa, bajo la supervisión del Director. V.- Orientar al público en general cuando así lo requiera. VI.- Revisar y firmar asistiendo al Director los autos y proyectos de resolución, correspondientes a los procedimientos de responsabilidad administrativa y proponer modificaciones necesarias. Las demás encomendadas por su superior jerárquico y las que aplique la normatividad vigente.		
Notificadores	<ul style="list-style-type: none"> Sergio Alejandro Fregoso Reyes José Humberto Ortiz Cerpa 	1.- Sistema de control interno de procedimientos de quejas 2.- Expedientes de procedimientos administrativos 3.- Libretas de registro.	1.- Físicos y Electrónicos
Funciones y obligaciones	I.- Practicar las notificaciones de los autos y actuaciones que se dicten al sustanciar el procedimiento, desde de su admisión, con la debida oportunidad y con las formalidades de ley. II. Llevar a cabo las diversas diligencias que le sean encargadas por el Director y Secretario Relator. III. Integrar los expedientes de los procedimientos de responsabilidad administrativa con las constancias de notificación, así como su foliado y entre sellado IV.- Realizar los registros de turno y baja de los expedientes que le sean turnados. V.- Llevar a cabo las listas de acuerdo internas y para el Boletín Judicial. VI.- Realizar las gestiones relativas para la obtención y justificación de viáticos necesarios para las notificaciones y diligencias correspondientes. Las demás encomendadas por su superior jerárquico y las que aplique la normatividad vigente.		
Taquimecanógrafa Judicial	<ul style="list-style-type: none"> María Dolores Sánchez Hernández 	1.- Sistema de control interno de procedimientos de quejas 2.- Expedientes de procedimientos administrativos 3.- Libretas de registro.	1.- Físicos y Electrónicos

Funciones y obligaciones	<p>I.- Asistir de manera general al Director, para el mejor cumplimiento de las tareas propias de la Dirección.</p> <p>II.- Atender a compañeros y público en general en orientación y/o derivación necesaria.</p> <p>III.- Atender llamadas telefónicas tanto oficiales como de particulares para su información o derivación.</p> <p>IV.- Control de lista de asistencia del personal.</p> <p>V.- Control de minuta de archivo.</p> <p>VI.- Registro físico y electrónico de turno de expedientes de procedimientos de responsabilidad administrativa, que son turnados para firma del Director y para publicación del acuerdo.</p> <p>VII.- Turnar física y electrónicamente los dictámenes aprobados.</p> <p>VIII.- Elaboración de oficios y memorándum dirigidos interna y externamente.</p> <p>IX.- Ser enlace entre el personal de la Dirección y de otras áreas con el titular, para una mejor coordinación laboral.</p> <p>Las demás encomendadas por su superior jerárquico y las que aplique la normatividad vigente.</p>		
Auxiliar de cómputo	<ul style="list-style-type: none"> • Sujey Guadalupe Reteguín Rivera • Paulina Judith Navarro Rentería 	<p>1.- Sistema de control interno de procedimientos de quejas</p> <p>2.- Expedientes de procedimientos administrativos</p> <p>3.- Libretas de registro.</p>	<p>1.- Físicos y Electrónicos</p>
Funciones y obligaciones	<p>Las actividades del Auxiliar de Cómputo, son establecidas en función de las necesidades del área como lo siguiente:</p> <p>I.- Asistir al Secretario Relator en el desahogo de audiencias, dictado de autos, apoyando en la substanciación de los procedimientos de responsabilidad administrativa.</p> <p>II.- Registro de turno y bajas tanto en libretas y sistema electrónico, los expedientes de procedimientos de responsabilidad administrativa.</p> <p>III.- Actualización de la información estadística que le corresponda.</p> <p>IV.- Realización de oficios y demás comunicaciones encomendadas.</p> <p>Las demás encomendadas por su superior jerárquico y las que aplique la normatividad vigente.</p>		
Secretaria B	<ul style="list-style-type: none"> • Martha Karina Martínez Bañuelos 	<p>1.- Sistema de control interno de procedimientos de quejas</p> <p>2.- Expedientes de procedimientos administrativos</p> <p>3.- Libretas de registro.</p>	<p>1.- Físicos y Electrónicos</p>
Funciones y obligaciones	<p>Se encargará de la oficialía de partes de la Dirección:</p> <p>I.- Recepción y entrega promociones</p> <p>II.- Asignar número de procedimiento de Responsabilidad Administrativa</p> <p>III.- Realizar oficios de contestación y/o retorno.</p> <p>IV.- Capturar y registrar en el sistema y libretas, las promociones y expedientes de procedimientos de responsabilidad administrativa.</p> <p>V.- Registro de las resoluciones del Pleno.</p> <p>V.- Alimentación y actualización del libro de gobierno físico y electrónico de la Dirección.</p> <p>Las demás encomendadas por su superior jerárquico y las que aplique la normatividad vigente.</p>		

Secretaria C	<ul style="list-style-type: none"> Xóchitl Sandoval Solórzano 	1.- Sistema de control interno de procedimientos de quejas 2.- Expedientes de procedimientos administrativos 3.- Libretas de registro.	1.- Físicos y Electrónicos
Funciones y obligaciones	Las actividades de la Secretaria C, son establecidas en función de las necesidades del área como lo siguiente: I.- Asistir al Secretario Relator en el desahogo de audiencias, dictado de autos, apoyando en la substanciación de los procedimientos de responsabilidad administrativa. II.- Registro de turno y bajas tanto en libretas y sistema electrónico, los expedientes de procedimientos de responsabilidad administrativa. III.- Actualización de la información estadística que le corresponda. IV.- Actualización de la base de datos de la información correspondiente en la página oficial. Las demás encomendadas por su superior jerárquico y las que aplique la normatividad vigente.		
Tipo de datos personales			
Inventario	1.- Nombre 2.- Teléfono 3.- Credencial del INE 4.- Cédula profesional 5.- Pasaporte		
Base de datos	1.- Sistema de control interno 2.- Expedientes de procedimientos administrativos 3.- Libretas de registro		
No. De titulares			
Controles de seguridad para las bases de datos			
Estructura y descripción del Sistema			
Tipo de soporte	1.- Físicos 2.- Electrónicos		
Características del lugar de resguardo			

Programas en que se utilizan los D.P.	1.- Programa de control interno de los procedimientos administrativos. 2.- De Microsoft, Word, Excel, PDF.			
Resguardo de los soportes físicos y/o electrónicos				
Físicos				
Electrónicos				
Las bitácoras de acceso y operación cotidiana				
Bitácoras físicas				
Clave de la bitácora				
Bitácoras electrónicas				
Clave de la bitácora				
Las bitácoras de Vulneraciones de seguridad				
ID	SOPORTE	RESPONSABLE		
				

SISTEMA DE TRATAMIENTO – DIRECCIÓN DE VISITADURÍA, DISCIPLINA Y RESPONSABILIDADES			
Administrador	Rosalinda Hernández Arias		
Cargo	Directora		
Área	Dirección de Visitaduría, Disciplina y Responsabilidades Departamento de Visitaduría		
Funciones y obligaciones	Las Señaladas por la Ley General de Responsabilidades Administrativas, ley Orgánica del Poder Judicial del Estado de Jalisco y la Ley de Responsabilidades Políticas y Administrativas del Estado de Jalisco		
Personal autorizado para tratamiento			
Visitador	<ul style="list-style-type: none"> • Imelda Calvillo Tello • Martín De la Cruz Ruvalcaba • Raúl González Vargas • Alejandro Guzmán Camberos • Miguel Ortega Carvajal • Raúl Pérez Zamora 	1.- Actas de Visitas en las que se allegó queja. 2.- Libretas de Registro.	Físicos y electrónicos.
Funciones y obligaciones	Las señaladas en la Ley Orgánica del Poder Judicial del Estado, Ley General de Responsabilidades Administrativas, Ley de Responsabilidades Políticas y Administrativas del Estado de Jalisco y el Reglamento Interno del Consejo de la Judicatura del Estado. Las demás encomendadas por su superior jerárquico y las que aplique la normatividad vigente.		
Jefe Especializado	<ul style="list-style-type: none"> • Albertina Ramírez Lepe 	1.- Actas de Visitas en las que se allegó queja. 2.- Libretas de Registro.	Físicos y electrónicos.

Funciones y obligaciones	<p>I.- Verificar el correcto trámite de viáticos y gastos que se requieren para las Visitas de inspección. II.- Solicitar a la Unidad departamental de Informática los ajustes y modificaciones necesarios. III.- Contestar las peticiones del área de transparencia e información. IV.- Coordinar los trabajos de los auxiliares y secretarias V.- Elaborar oficios de contestación sobre solicitudes o peticiones de otras direcciones o dependencias y memorándums. VI- Hacer del conocimiento a Servicios Generales de los desperfectos que pueda sufrir el mobiliario, equipo de oficina y a su vez de los automóviles y en su caso tramitar y dar seguimiento a las bajas del mismo ante la Dirección de Contraloría.</p> <p>Las demás encomendadas por su superior jerárquico y las que aplique la normatividad vigente.</p>		
Jefe de Sección	<ul style="list-style-type: none"> • Luis Alberto Rodríguez Varillas 	1.- Actas de Visitas en las que se allegó queja. 2.- Libretas de Registro.	Físicos y electrónicos.
Funciones y obligaciones	<p>I. Asistir a los visitadores judiciales, en la práctica de las visitas ordinarias, extraordinarias de inspección y demás diligencias en que éstos intervengan; II. Capturar las plantillas elaboradas por los visitadores en el proceso de la visita, cuando se trate de Juzgados de Primera Instancia, Menores y de Paz; III. Auxiliar a los visitadores en los programas de inspección y supervisión que efectúe la Visitaduría, así como en el despacho de la correspondencia que se reciba en el órgano auxiliar; IV. Tratar con respeto tanto al personal de la Visitaduría, como al de los órganos jurisdiccionales; y V. Las demás que les encomienden los visitadores, a fin de cumplir con los objetivos de la Visitaduría</p>		
Secretario Técnico	<ul style="list-style-type: none"> • Javier Emiliano Galvan Valencia 	1.- Actas de Visitas en las que se allegó queja. 2.- Libretas de Registro.	Físicos y electrónicos.
Funciones y obligaciones	<p>I. Asistir a los visitadores, en la práctica de las visitas ordinarias, extraordinarias de inspección y demás diligencias en que éstos intervengan; II. Capturar las plantillas elaboradas por los visitadores en el proceso de la visita, cuando se trate de Juzgados de Primera Instancia, Menores y de Paz; III. Auxiliar a los visitadores en los programas de inspección y supervisión que efectúe la Visitaduría, así como en el despacho de la</p>		

	<p>correspondencia que se reciba en el órgano auxiliar; IV. Tratar con respeto tanto al personal de la Visitaduría, como al de los órganos jurisdiccionales; y V. Las demás que les encomienden los visitadores, a fin de cumplir con los objetivos de la Visitaduría</p>		
Auxiliar de Visitador	<ul style="list-style-type: none"> • Víctor Manuel Arévalo Mascareño • José Jaime Enríquez Lamas • Jaime Alfonso García Islas • Juan Manuel Flores Valle 	<p>1.- Actas de Visitas en las que se allegó queja. 2.- Libretas de Registro.</p>	Físicos y electrónicos.
Funciones y obligaciones	<p>I. Asistir a los visitadores, en la práctica de las visitas ordinarias, extraordinarias de inspección y demás diligencias en que éstos intervengan; II. Capturar las plantillas elaboradas por los visitadores en el proceso de la visita, cuando se trate de Juzgados de Primera Instancia, Menores y de Paz; III. Auxiliar a los visitadores en los programas de inspección y supervisión que efectúe la Visitaduría, así como en el despacho de la correspondencia que se reciba en el órgano auxiliar; IV. Tratar con respeto tanto al personal de la Visitaduría, como al de los órganos jurisdiccionales; y V. Las demás que les encomienden los visitadores, a fin de cumplir con los objetivos de la Visitaduría.</p>		
Secretaria B	<ul style="list-style-type: none"> • María Teresa Arana Gómez 	<p>1.- Actas de Visitas en las que se allegó queja. 2.- Libretas de Registro.</p>	Físicos y electrónicos.
Funciones y obligaciones	<p>Las actividades de la Secretaria "B", son establecidas en función de las necesidades que el área de Visitaduría tiene, como las siguientes:</p> <ul style="list-style-type: none"> • Oficina y la correspondencia.- En lo que respecta a los trabajos de oficina, como dar contestación a la correspondencia interna, recibida en esta área, elaborar los oficios para cumplir con los requerimientos del Pleno del Consejo, de sus Comisiones o del Director. • Apoyo a los Visitadores.- Auxiliándolos a elaborar oficios; como enlace cuando los Visitadores y el demás personal se encuentran realizando inspecciones en juzgados. • Transparencia.- Apoya con los requerimientos de la Dirección de Transparencia. 		

Estructura y descripción del Sistema		
Tipo de soporte	1.- Físicos 2.- Electrónicos	
Características del lugar de resguardo	ÖSQ © ÖU KQ - ! { a85) Ü^•^! çaaæ ÖE öx Äi ÈA +æ85) Ä8 8a [AdSVCKDORT ÈU^*~ ! äæä Å^Äi • Ä äæä • Ü^! • [] æ^ • ÈQ äææ öæäæ() äæä) Å^Äi • Åæä ^ Ä^Ä [äi öæ) &] dæÄ ~ } ç • Å. äæ^ • È	
Programas en que se utilizan los D.P.	De Microsoft, Word, Excel, PDF.	
Resguardo de los soportes físicos y/o electrónicos		
Físicos		
Electrónicos	ÖSQ © ÖU KQ - ! { a85) Ü^•^! çaaæ ÖE öx Äi ÈA +æ85) Ä8 8a [AdSVCKDORT ÈU^*~ ! äæä Å^Äi • Ä äæä • Ü^! • [] æ^ • ÈQ äææ öæäæ() äæä) Å^Äi • Åæä ^ Ä^Ä [äi öæ) &] dæÄ ~ } ç • Å. äæ^ • È	
Las bitácoras de acceso y operación cotidiana		
Bitácoras físicas		
Clave de la bitácora	ÖSQ © ÖU KQ - ! { a85) Ü^•^! çaaæ ÖE öx Äi ÈA +æ85) Ä8 8a [AdSVCKDORT ÈU^*~ ! äæä Å^Äi • Ä äæä • Ü^! • [] æ^ • ÈQ äææ öæäæ() äæä) Å^Äi • Åæä ^ Ä^Ä [äi öæ) &] dæÄ ~ } ç • Å. äæ^ • È	
Bitácoras electrónicas		
Clave de la bitácora		
Las bitácoras de Vulneraciones de seguridad		
ID	SOPORTE	RESPONSABLE



ANEXO 2
FORMATO NOTIFICACIÓN DE VULNERACIÓN DE
SEGURIDAD DE LOS DATOS PERSONALES.

Anexo 2

Información del personal que detecta el incidente			
Nombre:			
Dirección:			
Teléfono:	Teléfono alternativo:		Celular:
Fax:	Correo electrónico:		
Información sobre el incidente			
Fecha:		Hora:	
Localización donde se detectó el incidente:			
Tipo de sistema de tratamiento:		Físico	Electrónico
Nombre del responsable del sistema de tratamiento:		___	___
Se encuentran involucrados datos personales en el incidente:		___	___
Tipo de datos personales involucrados:			
Descripción de lo sucedido:			
Evaluación (para ser llenado por el equipo de gestión de incidentes)			
Una vez analizada la información, se determina que se trata de un incidente de seguridad:		___	___
Justificación:			
Mencionar si existe algún posible impacto legal o contractual por el incidente:			



ANEXO 3
FORMATO PARA DETERMINAR QUE LAS
VULNERACIONES FUERON MITIGADAS

Anexo 3

DESCRIPCIÓN DE LAS ACCIONES DE MITIGACIÓN

1. Personal Involucrado

Nombre de las personas que realizaron el análisis del sistema de tratamiento afectado:

Iniciales	Nombre completo	Puesto

2. Descripción de las vulnerabilidades detectadas:

¿Fueron identificadas vulnerabilidades? Sí No

Tipo de activo ³¹	Vulnerabilidad	Descripción	Impacto
			Alto
			Medio
			Bajo
Acciones realizadas para erradicar las vulnerabilidades detectadas			

3. Validación:

¿Cuál fue el procedimiento de validación usado para asegurar que el problema fue erradicado?

--

4. Cierre:

Fecha y hora del cierre del incidente:

Nombre y firma de quién realiza la erradicación	Nombre y firma de quién validó la erradicación