ACUERDO GENERAL NÚMERO VEINTIDÓS

--- En la ciudad de San Juan, Provincia del mismo nombre, República Argentina, a tres días del mes de marzo de dos mil veintitrés, reunida la Corte de Justicia, presidida por el Dr. GUILLERMO HORACIO DE SANCTIS, con los Señores Ministros, Dr. MARCELO JORGE LIMA, la Señora Ministra, Dra. ADRIANA VERÓNICA GARCÍA NIETO, y los Señores Ministros, Dr. DANIEL GUSTAVO OLIVARES YAPUR y Dr. JUAN JOSÉ VICTORIA, contando con la asistencia del Fiscal Gral. de la Corte, Dr. EDUARDO QUATTROPANI, **DIJERON**: ----------

--- Que, mediante Expediente N° 137040 caratulado "DIRECCION DE INFORMÁTICA S/ Peticiona (ref. Revisión y Aprobación Política de Seguridad de la Información) el Director y Sub - Director de Informática solicitan la aprobación e implementación del Protocolo de Seguridad de la información.----------

--- Que, las amenazas de ciberseguridad continúan evolucionando y representan un riesgo significativo para las operaciones, los datos y la reputación de todas las organizaciones.----------

--- Que, es necesario asegurar que el programa de ciberseguridad del Poder Judicial sea sólido, seguro, consistente y efectivo para identificar y gestionar activamente los riesgos y proteger los activos de información contra posibles amenazas.----------

--- Que, la propuesta elevada por la Dirección de Informática ha sido desarrollada de acuerdo con los estándares y las mejores prácticas internacionales más recientes, incluyendo ISO / IEC 27001 Y 27002, que proporciona pautas claras y procedimientos para ayudar a proteger nuestra organización contra las amenazas de ciberseguridad.----------

--- Que, el Protocolo de Seguridad de la Información propuesto cubre todos los aspectos de la seguridad de la información, incluyendo políticas de seguridad, organización de la seguridad de la información, gestión de activos, seguridad de recursos humanos, seguridad física y ambiental, gestión de comunicaciones y operaciones, control de acceso, adquisición, desarrollo, mantenimiento y revisión de sistemas de información, prevención y gestión de incidentes de seguridad de la información, procedimiento anti catástrofe, gestión de continuidad de operaciones y cumplimiento de tareas.----------

--- Que, como un componente esencial del Programa de Ciberseguridad del Poder Judicial, el Protocolo de Seguridad de la Información proporciona un marco para la gestión segura de la información y los datos de este Poder del Estado, definiendo los roles y responsabilidades de los interesados, proporcionando orientación para la implementación de medidas de seguridad, como controles de acceso, prevención, gestión de incidentes y recuperación de desastres.----------

--- Que, por todo ello en uso de las facultades que le confiere en artículo 207 de la Constitución de la Provincia y la Ley Orgánica de Tribunales (LP N° 2352-O), **ACORDARON**:----------

1.- Aprobar el Protocolo de Seguridad Informática, que en Anexo integra la presente.----------

2.- Disponer la obligatoriedad del cumplimiento del Protocolo de Seguridad Informática por parte de la totalidad del personal del Poder Judicial, considerando cualquier conducta contraria u omisiva de las reglas de seguridad allí establecidas como falta disciplinaria, pasible de sanción.----------

3.- Crease el Comité de Seguridad en los términos explicitados en el Protocolo aprobado.----------

4.- Disponer se dé amplia difusión del mismo en todo el ámbito del Poder Judicial y publíquese por un día en el Boletín Oficial de la provincia.---------

--- Dispuestas las comunicaciones del caso, termina el acuerdo, que se firma por ante mí.-

Dr. EDUARDO QUATTROPANI
Fiscal General de la Corte de Justicia

Dr. Guillermo Horacio De Sanctis
PRESIDENTE

Dr. Juan José E. Victoria
MINISTRO

Dr. Daniel Gustavo Olivares Yapur
MINISTRO

Dra. Adriana Verónica García Nieto
Ministra

Dr. MARCELO JORGE LIMA
MINISTRO

Dr. Javier Vera Frassinelli
SECRETARIO ADMINISTRATIVO
CORTE DE JUSTICIA

ANEXO ACUERDO GENERAL N° 22/2023

Protocolo de Seguridad Informática del Poder Judicial de San Juan

Delitos Informáticos

Revisiones de Cumplimiento de Seguridad

Revisión independiente de la Seguridad de la Información

Cumplimiento del Protocolo y Procedimientos de Seguridad

Verificación de Cumplimiento en los Sistemas de Información

Prefacio

La *Corte de Justicia de San Juan*, entidad rectora del "*Poder Judicial de la Provincia de San Juan*", en cumplimiento de su estrategia de informatización, su política de mejora en los servicios y acceso a la Justicia y su rol constitucional, establece la necesidad de contar con un *Protocolo de Seguridad Informática* que se aplicará a la totalidad de sus unidades jurisdiccionales y oficinas de apoyo a dicha labor.

El mismo define directivas orientadas a resguardar la disponibilidad, confidencialidad e integridad de la información que se encuentra en procesamiento, transmisión o guarda, incluyendo tanto medios digitales, como computadoras y redes, como aquella información que se haya puesto a disposición de empleados o terceros a través de otros medios.

De igual manera apunta a asegurar la protección de los recursos utilizados y garantizar la continuidad de las operaciones del Poder Judicial de San Juan, en conformidad con las leyes y normativas jurídicas vigentes.

Introducción

Definición

Las tecnologías de la información permiten gestionar grandes cantidades de información. Estas tecnologías están expuestas a múltiples vulnerabilidades y amenazas, más aún cuando no se cuenta con una correcta gestión de la seguridad de la información.

El *Protocolo de Seguridad Informática* nos brinda un marco para proteger la información y garantizar la continuidad de las operaciones de los sistemas de información, asegurando de este modo el cumplimiento eficiente de los objetivos del Poder Judicial de San Juan.

Para esto es necesario imponer el presente protocolo como norma obligatoria a cumplir por las máximas autoridades del Poder Judicial de San Juan y de los titulares de todas las unidades organizativas promoviendo la difusión, consolidación y cumplimiento de las medidas adoptadas con el fin de que estos principios formen parte de la cultura organizacional.

Objetivo

El objetivo del presente protocolo, es el de proteger los activos de información y los recursos tecnológicos del Poder Judicial de San Juan utilizados en la transmisión, procesamiento y almacenamiento de la información, frente a amenazas internas o externas, deliberadas o accidentales, físicas o cibernéticas, mediante la implementación de un adecuado conjunto de controles que incluyen, políticas, procesos, procedimientos, estructura organizacional, funciones de hardware y software, identificación de recursos y partidas presupuestarias necesarias para

alcanzar dichos objetivos.

Alcance

El presente Protocolo de Seguridad Informática deberá ser conocido y cumplido por todo el personal del Poder Judicial de San Juan, incluyendo magistrados, miembros del Ministerio Público, funcionarios y agentes, sea cual fuere su nivel escalafonario y su situación de revista.

Las disposiciones que en éste se encuentran se aplican a todo el ámbito del Poder Judicial de San Juan, a todos sus recursos y a la totalidad de los procesos, ya sean estos internos, externos o vinculados a través de acuerdos o contratos con terceros.

Lineamientos

Principios

El presente protocolo se basa en los principios de Confidencialidad, Integridad y Disponibilidad de la información como también el principio de la Continuidad Operacional, postulados básicos que rigen la Seguridad de la Información.

Obligatoriedad

La Corte de Justicia de San Juan hará cumplir este Protocolo de Seguridad Informática como parte de sus herramientas de gobierno y gestión.

Aplicación y Observación

El presente Protocolo de Seguridad Informática expresa declaraciones respecto a temáticas inherentes a la seguridad y son de aplicación y observación obligatoria por todo el personal del Poder Judicial de San Juan.

Comité de Seguridad

El Comité de Seguridad, cuya existencia y composición es definida y aprobada por la Corte de Justicia de San Juan, es responsable de garantizar que los activos de la organización estén protegidos y que el Sistema de Gestión de la Seguridad, basado en este protocolo, sea eficaz, eficiente y alineado con los objetivos del Poder Judicial de San Juan.

Excepciones

Toda excepción al Protocolo de Seguridad Informática deberá ser formalmente autorizada, registrada y documentada.

La excepción al cumplimiento de la presente deberá ser solicitada de manera previa y formal por el responsable de la dependencia interesada y posteriormente evaluada por el Comité de Seguridad antes de su implementación.

Marco Normativo

Todas las definiciones del presente Protocolo de Seguridad Informática están de acuerdo con la Legislación de la República Argentina, incluyendo:

- Protección de Datos Personales, Ley N° 25.326
- Delitos Informáticos, Ley N° 26.388
- Firma Digital, Ley N° 25.506

- Ética en el Ejercicio de la Función Pública, Ley N° 25.188
- Propiedad Intelectual, Ley N° 11.723
- Normativas Particulares (Leyes provinciales, Normas del Poder Judicial de San Juan, etc.)

Glosario de Términos y Definiciones

- Amenaza: causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.
- Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Autenticador: tipo de dispositivo portátil que es usado para verificar la identidad de un individuo que desea utilizar un servicio en particular, también conocido como token de autenticación.
- Código malicioso: programa malicioso, también llamado malware o virus informático, hace referencia a cualquier tipo de software que trata de infiltrarse sin el consentimiento del usuario para robar información, dañar el sistema afectado o hacer uso de los recursos informáticos para afectar a otros sistemas.
- Confidencialidad: condición que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- Confiabilidad de la Información : refiere a que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- Control / Contramedida / Salvaguarda: medio para mitigar el riesgo; incluye políticas, procedimientos, directrices, prácticas o estructuras organizacionales y pueden ser de naturaleza administrativa, técnica, de gestión, o legal.
- Comité de Seguridad: El Comité de Seguridad, cuya existencia y composición es definida y aprobada por la Corte de Justicia de San Juan, es responsable de garantizar que los activos de la organización estén protegidos y que el SGS sea eficaz, eficiente y alineado con los objetivos de la organización.
- Continuidad operacional: refiere a la continuidad de los procesos operativos en el Poder Judicial de San Juan y su recuperación ante la ocurrencia de un incidente de seguridad.
- Criptografía: técnicas de cifrado o codificado destinadas a transformar un mensaje o pieza de información con el fin de hacerlo ininteligible a receptores no autorizados.
- Criptografía simétrica: técnica de cifrado que emplea una misma clave tanto para cifrado como para descifrado.
- Criptografía asimétrica: técnica de cifrado que emplea una clave privada para codificar y una clave pública para el descifrado.
- Disponibilidad : garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma cada vez que lo requieran.
- Evaluación de Riesgos: refiere a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que alguna de estas vulnerabilidades sean explotadas, y su potencial impacto en la operatoria del Poder Judicial de San Juan.
- Gestión de Riesgos: actividades implementadas para dirigir y controlar una organización en lo que concierne al riesgo. La gestión de riesgos usualmente incluye la evaluación de

riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

- Hardware: equipamiento informático.
- Incidente de Seguridad: evento adverso en un sistema o red de computadoras, que puede comprometer la confidencialidad, integridad o disponibilidad de la información pudiendo ser causado por la explotación de alguna vulnerabilidad y que atenta contra los mecanismos de seguridad existentes.
- Información: toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- Integridad: atributo de la información que refiere a un estado de no haber sido alterada y encontrarse completa.
- Legalidad: Refiere al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Poder Judicial de San Juan.
- No Repudio: Término que refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- ONTI: Oficina Nacional de Tecnologías de Información, es el órgano rector que acompaña a los organismos públicos en el proceso de innovación tecnológica proponiendo diversos objetivos.
- Propietario de la Información: define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.
- Principio de mínimo privilegio o PoLP: concepto de seguridad de la información referente a entregar a un usuario los niveles (o permisos) de acceso mínimos necesarios para que pueda desempeñar sus funciones laborales
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- Remediación: Proceso que conduce al restablecimiento total o parcial del nivel de seguridad de un sistema, producto de la implementación de una contramedida que disminuye, mitiga o elimina una amenaza. Por ejemplo, la instalación de actualizaciones de seguridad en un sistema operativo
- Riesgo: Es la combinación de la probabilidad de ocurrencia de una amenaza y su impacto si la misma tuviera éxito.
- Seguridad de la Información: se entiende como la preservación de la confidencialidad, disponibilidad e integridad de la información.
- Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- Sistema antimalware: Sistema que tiene como propósito la detección y eliminación de código malicioso.
- Software: programa informático.
- Tecnología de la Información: refiere al hardware y software operados por el Poder

Judicial de San Juan o por un tercero que procese información en su nombre, para llevar a cabo una función propia del mismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

- Tratamiento de Riesgos: Proceso de selección e implementación de medidas para mitigar los mismos.
- Vulnerabilidad: Debilidad, falencia o ausencia de un control en un activo o grupo de activos que puede ser aprovechada por una amenaza.

Gestión de Políticas y Normativas de Seguridad

Siguiendo los lineamientos de la política modelo establecida por la ONTI, la Dirección Nacional de Ciberseguridad (CERT.ar) y los dominios definidos en la norma ISO/IEC 27002:2013, se establecen los catorce dominios para organizar el presente, a saber:

- Políticas y Normativas de Seguridad

  Se establece el "Protocolo de Seguridad Informática" (PSI), aprobado por la Corte de Justicia de San Juan, publicado y comunicado a todo el personal.

  Se establece el "Protocolo de Uso de Recursos Informáticos y Telecomunicaciones", que establece las normas de conducta razonable que deben observar los agentes y funcionarios del Poder Judicial de San Juan cuando utilicen los recursos tecnológicos puestos a su disposición para el desempeño de sus tareas.

  Se establecen, además, políticas y normativas complementarias que al igual que las anteriores, deberán ser de cumplimiento de carácter obligatorio y sujetas a revisiones de forma regular.

- Política Organizativa

  Se establece el "Comité de Seguridad" el cual será responsable de apoyar e impulsar las políticas, planes y programas referidos al Protocolo de Seguridad Informática.

  Se conforma el "Área de Ciberseguridad", que dependerá de la Dirección de Informática, la cual tendrá a su cargo las funciones relativas a la seguridad de los sistemas de información y procesos del Poder Judicial de San Juan, como también la supervisión de todos los aspectos inherentes a la seguridad tratados en la presente política.

  Se establecen responsables en el cumplimiento de los distintos procesos de seguridad.

  Se designan Propietarios de la Información y Propietarios de Activos, quienes serán responsables por el resguardo de los mismos.

  Se fomenta el contacto con otros organismos públicos y entidades privadas para el intercambio de experiencias en materias de seguridad con el objeto de actualizar e intercambiar conocimientos relativos a seguridad y promover la capacitación continua.

  Se contempla la Seguridad de la Información en todos los proyectos del Poder Judicial de San Juan.

  Se establecen "Requisitos de Seguridad para el Uso de Dispositivos Móviles y el Trabajo a Distancia", los cuales deben cumplir con ciertas directrices de seguridad antes de que estos puedan acceder a los recursos del Poder Judicial de San Juan, como también ciertas consideraciones de uso fuera de las instalaciones

- Política de Recursos Humanos

  Se considera fundamental la gestión del ciclo de vida del vínculo laboral de las personas, por lo cual se establecerá la revisión de los antecedentes del postulante antes del empleo, la aceptación de los documentos "Acuerdo de Confidencialidad" y "Protocolo de Uso de Recursos Informáticos y Telecomunicaciones" y "Protocolo de Seguridad Informática" al inicio del mismo y la devolución de activos al finalizar el vínculo laboral con el Poder Judicial de San Juan.

  Los responsables del área de pertenencia del empleado velarán por el cumplimiento de este protocolo y toda la normativa vigente e informarán que el incumplimiento podrá ser pasible del inicio de un proceso administrativo disciplinario.

  Se declara el compromiso de concientizar y capacitar al personal en temas referidos a las políticas, procedimientos y buenas prácticas en Seguridad de la Información.

  Se establece la existencia de un proceso disciplinario para todos aquellos agentes que, sea cual fuere su situación de revista en el Poder Judicial de San Juan, violen las políticas, normativas y procedimientos de seguridad vigentes.

- Política de Gestión de Activos

  Se establece la identificación , clasificación y criticidad de los activos de información, físicos y de recursos humanos, mediante un inventario actualizado, designándose responsable de los mismos a los Propietarios de Activos.

  Se identifican, documentan y definen normativas de uso de los activos de tecnología según las pautas declaradas en el Protocolo de Uso de Recursos Informáticos y Telecomunicaciones.

  Se definen directrices de clasificación, etiquetado y manipulación de activos de información. Se establece que el tratamiento de la información, respecto a su almacenamiento, transporte y eliminación se realizará de forma segura.

- Política de Control de Accesos

  Se controla el acceso a la información y a los recursos tecnológicos del Poder Judicial de San Juan, por ello se establece la existencia de pautas y procedimientos que reglamentan la gestión de usuarios y la gestión de permisos de acceso a la información y a los recursos tecnológicos del Poder Judicial de San Juan.

  Se restringe el acceso a la información, en concordancia con la clasificación de la misma, sobre la base de la premisa rectora, "Todo acceso está prohibido, a menos que se permita explícitamente" (primado del "Principio de Mínimo Privilegio" o "PoLP").

  Se establece la gestión segura de las contraseñas, como también las responsabilidades de los usuarios, sobre el uso de las mismas.

Se revisa, inspecciona y controla el tráfico de datos en las redes del Poder Judicial de San Juan, como también toda comunicación externa entrante hacia las redes del Poder Judicial de San Juan y toda comunicación saliente hacia Internet con el objeto de verificar que no se violen las políticas de seguridad establecidas.

- Política de Criptografía

  Se establece el uso de criptografía para asegurar la información y las comunicaciones, como ser contraseñas, almacenamiento de las copias de resguardo, cifrado de dispositivos móviles, servicios expuestos a Internet y transmisión de datos, dentro y fuera del ámbito del Poder Judicial de San Juan.

- Política Físico y Ambiental

  Refiere al control del acceso físico a las dependencias del Poder Judicial de San Juan. Se definen, además, perímetros de seguridad y medidas para proteger las áreas consideradas como críticas.

  Se asegura la continuidad operacional del suministro de energía eléctrica y del control ambiental en el centro de procesamiento de datos y sala de comunicaciones, como también se prevé la existencia de controles de seguridad para garantizar la protección de los medios de transmisión de datos.

  Prevé realizar el mantenimiento periódico del equipamiento informático, control de su entrada y salida de las dependencias del Poder Judicial de San Juan y destrucción segura cuando el equipamiento no pueda ser reutilizado, con el objeto de no exponer información residual, considerada privada o confidencial que permanezca en el equipo informático.

- Política de Seguridad en las Operaciones

  Establece la evaluación periódica de las necesidades de capacidad operacional de los sistemas y la proyección de futuras demandas, con el objeto de garantizar que el crecimiento no ponga en riesgo las actividades operativas ante la falta de recursos.

  Se implementan procedimientos para gestionar tareas operativas y responsables para la ejecución de las mismas.

  En los procesos de desarrollo de software se definen entornos separados entre sí: Desarrollo, Pruebas Funcionales, Pruebas de Seguridad y Producción, con el objeto de generar sistemas seguros.

  Se protegen los sistemas tecnológicos contra todo tipo de código malicioso mediante la implementación de sistemas antimalware que prevengan el ingreso de códigos maliciosos, permitan la ejecución de análisis periódicos preventivos y controles de detección en las estaciones de trabajo, servidores, conexiones de Internet y correo electrónico

- Política en la Gestión de las Comunicaciones

  Se monitorea, controla, segrega y restringe el tráfico de red, independientemente del medio de transmisión implementado, en todas las infraestructuras de comunicación de datos del Poder Judicial de San Juan.

  La utilización de servicios de Internet, al igual que el uso del correo electrónico laboral, estarán sujetos a las condiciones de uso descritas en el Protocolo de Uso de Recursos Informáticos y Telecomunicaciones.

- Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

  En toda adquisición de sistemas informáticos como también en todos los proyectos de desarrollo de software, tanto propios o de terceros, se establece la inclusión de requerimientos de seguridad.

  Se considera a la seguridad de la información como una parte integral en los ciclos de vida de los procesos de desarrollo y adquisición de software.

  Se protegen todos los sistemas expuestos a Internet contra actividades fraudulentas, modificaciones y divulgación de datos no autorizados, intercepción, vulneración de la confidencialidad, suplantación de identidad o cualquier otra amenaza existente.

  Se realizan pruebas de evaluación de vulnerabilidades en los sistemas e infraestructura del Poder Judicial de San Juan con el objeto de detectar debilidades para luego remediarlas.

  Se usan datos de prueba de manera segura siguiendo requisitos de seguridad estipulados en los entornos de desarrollo y pruebas funcionales y de seguridad.

- Política en Relación a los Proveedores

  Se establecen una serie de requisitos de seguridad para proteger los activos de información que son accedidos por los proveedores, como también los riesgos asociados a los servicios provistos por parte de terceros.

  Se controlan las implementaciones de los proveedores, se monitorea su cumplimiento y la gestión de cambios con el fin de asegurar que los servicios que se presten, cumplan con todos los requerimientos acordados previamente.

- Política de Gestión de Incidentes de Seguridad

  Todo el personal del Poder Judicial de San Juan, es responsable de informar los incidentes de seguridad cuando se detecten, como también de comunicar las fallas o debilidades descubiertas en los sistemas tecnológicos que usan.

  Se establecen responsabilidades y procedimientos para gestionar los incidentes de seguridad con el fin de garantizar una respuesta rápida, eficaz y sistemática, ante la

aparición de los mismos.

Se aplicará un proceso disciplinario contemplado en las normas estatutarias, para los empleados que violen el Protocolo de Seguridad Informática y el Protocolo de Uso de Recursos Informáticos y Telecomunicaciones.

Cuando la respuesta a un incidente de seguridad de la información, implique medidas administrativas o legales se establecerán procedimientos complementarios de identificación, adquisición y almacenamiento de evidencia forense.

- Política de Gestión de la Continuidad de Operaciones

  A fin de mitigar los efectos de incidentes graves, se formulan e implementan planes de contingencia que permitan garantizar la continuidad de los procesos del Poder Judicial de San Juan permitiendo la restauración de las actividades críticas en los plazos requeridos y manteniendo los requerimientos de seguridad.

- Política de Gestión de Configuraciones

  El propósito de la Política de Gestión de la Configuración es garantizar que todos los activos de Tecnología de Información estén documentados con sus interdependencias y relaciones conocidas para que se puedan ejecutar las actividades de gestión de cambios, análisis de impacto y cumplimiento.

  La Política de Gestión de Configuraciones se aplica a todos los activos, sistemas, redes y hosts de datos de tecnología de la información que son propiedad, están administrados y/o patrocinados por el Poder Judicial de la Provincia de San Juan.

  Todo activo de hardware que esté en funcionamiento, sirva este para recopilar, transmitir, procesar, almacenar o alojar datos debe ser inventariado y administrado para garantizar que no sea susceptible de acceso, distribución o uso indebido no autorizado Cuanto mayor sea el valor del activo o cuanto más se considere susceptible de riesgo o explotación, mayor será el nivel de protección requerido para su gestión.

- Política de Cumplimiento

  Se respetan los requisitos contractuales, regulatorios y legales vigentes.

  Se aboga por el cumplimiento de las leyes relacionadas a la propiedad intelectual, protección de datos personales, firma digital, delitos informáticos, así como también todo el marco normativo interno de Seguridad de la Información para lo cual se establece realizar revisiones de cumplimiento y de auditoría en los sistemas de información, infraestructura tecnológica y en los procesos existentes.

Políticas y Normativas de Seguridad

Objetivo

Proteger los recursos de información del Poder Judicial de San Juan y la tecnología utilizada para su procesamiento frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Proporcionar a La Corte de Justicia de San Juan los lineamientos y el soporte necesarios para garantizar la Seguridad de la Información en concordancia con los requerimientos y las leyes y regulaciones relevantes. La Corte de Justicia de San Juan debe establecer claramente la dirección de la política en línea con los objetivos.

Protocolo de Seguridad Informática

El presente Protocolo de Seguridad Informática, una vez aprobado por las máximas autoridades del Poder Judicial de la Provincia de San Juan, será publicado y comunicado a todos los agentes del Poder Judicial de San Juan y terceras partes relevantes, entrando en vigencia a partir de su aprobación mediante Acuerdo (Acordada) de La Corte de Justicia de San Juan.

Políticas y Normativas Complementarias

Deberá existir un "Protocolo de Uso de Recursos Informáticos y Telecomunicaciones", que establecerá las normas de conducta razonable que deben observar los agentes y funcionarios del Poder Judicial de San Juan cuando utilicen los recursos informáticos puestos a su disposición, con la finalidad de minimizar todos aquellos riesgos producto del mal uso de los mismos.

De la misma manera, podrán existir otra serie de políticas y normativas más detalladas, aplicables en áreas específicas. Por ello se establecerán las siguientes jerarquías respecto a la documentación de seguridad, a fin de garantizar que los objetivos y medidas establecidos en la presente política de seguridad cuente con un orden establecido:

1. Primer nivel: Protocolo de Seguridad Informática (PSI).
2. Segundo nivel: Protocolo de Uso de Recursos Informáticos y Telecomunicaciones y otras políticas y normativas relacionadas a éste.
3. Tercer nivel: Documentación de buenas prácticas, recomendaciones y guías de apoyo referidos a aspectos de Seguridad de la Información.
4. Cuarto nivel: Procedimientos de seguridad.

Revisión de Políticas

El Protocolo de Seguridad Informática y el Protocolo de Uso de Recursos Informáticos y Telecomunicaciones, deberán ser revisados regularmente cada dos años o cuando ocurran cambios significativos referidos a las políticas adoptadas y deben ser aprobadas por el Comité de

Seguridad.

Ambas deben poseer un dueño, responsable de las actividades de desarrollo, evaluación y revisión de las mismas.

La actividad de revisión debe incluir las oportunidades de mejoras, en respuesta a los cambios, entre otros, organizacionales, normativos, legales, de terceros o tecnológicos.

Política Organizativa

Objetivos

Administrar la seguridad de la información dentro del Poder Judicial de San Juan y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de Seguridad de la Información. Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Poder Judicial de San Juan.

Organización Interna

Compromiso de La Corte de Justicia de San Juan

La Corte de Justicia de San Juan apoyará la Seguridad de la Información a través de una orientación clara, mostrando compromiso, asignando roles y reconociendo responsabilidades explícitas.

Deberá revisar y aprobar el Protocolo de Seguridad Informática, como asimismo revisar los beneficios de la implementación de la misma, que fuera elevada previamente por el Comité de Seguridad.

El Comité de Seguridad

La Seguridad de la Información es una responsabilidad del Poder Judicial de San Juan compartida por todas las autoridades y miembros del mismo.

Por esto se crea el "*Comité de Seguridad*". Este comité se conforma de las autoridades relevantes del Poder Judicial de San Juan como partes interesadas en la promoción de las iniciativas de Seguridad de la Información y en el impulso y la puesta en vigor del presente protocolo.

El Comité de Seguridad tendrá entre sus funciones:

- Revisar el Protocolo, los objetivos de seguridad y las funciones generales en materia de Seguridad de la Información, y proponer a la máxima autoridad del Poder Judicial de San Juan para su aprobación.
- Controlar, evaluar y gestionar cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

- Tomar conocimiento y supervisar la investigación y monitoreo de aquellos incidentes relevantes relativos a la seguridad.
- Evaluar y aprobar las principales iniciativas para incrementar la Seguridad de la Información, de acuerdo con las competencias y responsabilidades asignadas a cada área, incluyendo el Plan Director de Seguridad.
- Acordar y aprobar metodologías, procesos y políticas específicos relativos a la Seguridad de la Información.
- Garantizar que la seguridad sea parte del proceso de planificación informática del Poder Judicial de San Juan.
- Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información para nuevos sistemas o servicios.
- Promover la difusión y concientización de la Seguridad de la Información dentro del Poder Judicial de San Juan.
- Coordinar el proceso de administración de la continuidad operativa de los sistemas de tratamiento de la información del Poder Judicial de San Juan frente a interrupciones imprevistas.
- Confeccionar, ejecutar y reportar un Plan de Inversiones que garantice a la organización la disminución sistemática de los riesgos identificados y una mejora general de la postura de seguridad.
- Delegar la autoridad a los agentes correspondientes para ejecutar las tareas asociadas a la Seguridad de la Información.
- Asumir la responsabilidad final de los asuntos asociados a la Seguridad de la Información de la Organización.

Área de Ciberseguridad

Se designarán funciones relativas de Seguridad de la Información al Área de Ciberseguridad. El Área tendrá a cargo la supervisión de todos los aspectos inherentes a la seguridad tratados en la presente Política y será responsable de asegurar que las actividades de seguridad sean ejecutadas en conformidad con el Protocolo de Seguridad Informática.

Entre sus ocupaciones están:

- Identificar cómo manejar las no-conformidades.
- Aprobar las metodologías y procesos referentes a la Seguridad de la Información; por ejemplo, la evaluación del riesgo y la clasificación de la información.
- Identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas.
- Promover de manera eficiente la capacitación y concientización de la Seguridad de la Información en el Poder Judicial de San Juan.
- Evaluar la información recibida del monitoreo y revisar los incidentes de Seguridad de la Información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.
- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI).
- Identificar, evaluar y proponer el tratamiento de los riesgos y amenazas a los que se

expone la información y los recursos tecnológicos del Poder Judicial de San Juan.

- Controlar el acceso a los recursos tecnológicos.
- Detectar, analizar, remediar y recolectar evidencia forense de incidentes de seguridad de la Organización, ante actuaciones que ameriten intervención administrativa o judicial.

Asignación de Responsabilidades de la Seguridad de la Información

Se asignan responsabilidades en los procesos de seguridad indicados en el presente cuadro:

Proceso de Seguridad	Responsable
Apoyo e impulso de la implementación del Protocolo de Seguridad Informática	Comité de Seguridad
Gestión de Incidentes de Seguridad	Área de Ciberseguridad
Seguridad Electrónica	Área de Ciberseguridad
Seguridad en las Comunicaciones	Área de Ciberseguridad
Seguridad en el Ciclo de Vida del Desarrollo de Software de Sistemas	Dirección de Informática
Planificación de la Continuidad Operativa	Comité de Seguridad
Seguridad en la provisión de suministro eléctrico	Dirección de Servicios Generales
Seguridad Ambiental	Dirección de Servicios Generales
Cumplimiento Legal y Normativo	Corte de Justicia de San Juan
Auditorías Internas	Auditoría Interna/Dirección de Control de Gestión
Seguridad Física	Comité de Seguridad
Difusión y Cumplimiento	Directores, coordinadores y empleados
Seguridad de las Personas	Dirección de Servicios Generales (Oficina Higiene y Seguridad Laboral) y Dirección de Recursos Humanos

Propietarios de la Información

Se designarán propietarios de la información que se procesa y almacena en el Poder Judicial de San Juan, los cuales deberían ser generalmente los responsables de las Direcciones o Coordinaciones que utilizan dicha información.

Los propietarios tendrán la función de identificar la criticidad de la información que gestionan, definir y autorizar sus accesos y, si bien podrán delegar la administración de sus funciones a personal idóneo, seguirán conservando la responsabilidad sobre la misma.

La asignación de la responsabilidad de la información deberá ser formalmente documentada y proporcionada al Área de Ciberseguridad, debiendo registrarse descripción de la información, propietario, procesos involucrados, área, recursos asociados, responsable técnico y cualquier otra información que sea relevante.

Autorización de equipamiento para procesamiento de información

Los nuevos recursos de procesamiento de información deberán ser autorizados por la Dirección de Informática en conjunto con el Área de Ciberseguridad, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad existentes.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede

ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado y autorizado por la Dirección de Informática en conjunto con el Área de Ciberseguridad, siguiendo las directrices del punto.

Acuerdo de Confidencialidad

Se definirán, implementarán y revisarán regularmente los acuerdos de confidencialidad o de no divulgación para asegurar la protección de la información los cuales deberán ser firmado por la totalidad del personal del Poder Judicial de San Juan, cualquiera sea su situación de revista como también por terceros que tengan relaciones contractuales con el Poder Judicial de San Juan.

Mediante este instrumento la persona se compromete a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate.

Dicho acuerdo debe responder a los requerimientos de confidencialidad o no divulgación, asimismo, deben cumplir con toda legislación o normativa que alcance al Poder Judicial de San Juan en materia de confidencialidad de la información.

Contacto con otros organismos

A efectos de intercambiar experiencias, obtener asesoramiento o capacitación para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con otros organismos especializados en temas relativos a la Seguridad de la Información.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permitirá cuando se haya firmado previamente un Acuerdo de Confidencialidad con aquellas organizaciones públicas y privadas especializadas en temas relativos a la Seguridad de la Información.

Contacto con grupos especializados en Seguridad de la Información

El Área de Ciberseguridad gestionará el intercambio de conocimientos entre pares en materia de Seguridad de la Información, promoviendo su capacitación continua.

Para ello fomentará la asistencia y contacto con eventos, grupos, foros o asociaciones especializados de Seguridad de la Información, con el fin de actualizar los conocimientos en materia de Seguridad de la Información del área, como también poder recibir alertas tempranas, avisos y/o recomendaciones ante la aparición de nuevas vulnerabilidades o formas de violar la seguridad implementada.

Seguridad de la información en la gestión de proyectos

Se deberá considerar al Área de Ciberseguridad en la gestión de proyectos, a efectos de garantizar que se reflejen adecuadamente las disposiciones del Protocolo de Seguridad Informática en los mismos.

Segregación de funciones

Se deberá diseñar el esquema de roles, segregando funciones y áreas de responsabilidades en todas las tareas inherentes que atañen a la gestión de Seguridad de la Información para evitar el conflicto de intereses con el objeto de reducir modificaciones no autorizadas o el mal uso de la información o servicios.

Dispositivos móviles y trabajo remoto

Dispositivos móviles del Poder Judicial de San Juan

Todo dispositivo móvil perteneciente al Poder Judicial de San Juan (laptops, notebooks, netbooks tablets, teléfonos celulares, etc.), que pudiera contener información del Poder Judicial de San Juan, deberá cumplir con medidas seguridad adecuadas para proteger el dispositivo móvil y la información que contiene, contra todos los riesgos derivados del uso del mismo.

Para esto se deberán desarrollar procedimientos destinados a asegurar al dispositivo móvil y la información contenida, debiendo tener en cuenta los siguientes conceptos:

- Protección contra software malicioso del dispositivo móvil.
- Cifrado de la información en el dispositivo móvil.
- Mecanismos de borrado seguro de la información en caso de robo o pérdida.
- Cifrado de las comunicaciones para acceder a los servicios del Poder Judicial de San Juan.
- Control de acceso a los recursos a los que accede el dispositivo móvil.
- Aplicación de las mismas políticas de seguridad que a los equipos no móviles del Poder Judicial de San Juan.

La utilización de dispositivos móviles en la vía pública, incrementa la probabilidad de ocurrencia de incidentes de pérdida, robo o hurto. En consecuencia, deberá comunicarse al personal que los utilice sobre los cuidados especiales a observar ante el uso de los mismos, contemplando las siguientes recomendaciones:

- Permanecer cerca del dispositivo, no dejando el mismo desatendido.
- No llamar la atención acerca de portar un equipo móvil.
- No poner identificaciones referidas al Poder Judicial de San Juan en el dispositivo móvil, salvo los estrictamente necesarios.
- Colocar un teléfono de contacto sin identificación para su recupero.
- Mantener cifrada la información del dispositivo móvil.

Se confeccionará un procedimiento que permita al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y de esta manera mitigar los riesgos a los que eventualmente estuviera expuesto el Poder Judicial de San Juan ante la ocurrencia del incidente, los que incluirán:

- Revocación de las credenciales afectadas
- Notificación al Área de Ciberseguridad.
- Notificación a los grupos de trabajo donde potencialmente podría haber comprometido

dicho incidente.

Dispositivos móviles personales

Cuando sea necesario la utilización de equipamiento personal, en las instalaciones del Poder Judicial de San Juan, este deberá ser evaluado y autorizado por el Área de Ciberseguridad en conjunto con la Dirección de Informática.

Todo dispositivo móvil no perteneciente al Poder Judicial de San Juan (laptops, notebooks, netbooks, tablets, etc.) deberá cumplir con las medidas de seguridad adecuadas con el fin de proteger los recursos informáticos a los cuales accede. Se deberán desarrollar procedimientos para estos dispositivos, que abarquen los siguientes conceptos:

- Protección contra software malicioso del dispositivo móvil.
- Cifrado de las comunicaciones para acceder a los servicios del Poder Judicial de San Juan.
- Control de acceso a los recursos a los que se accede desde el dispositivo móvil.
- Concientización del usuario de las restricciones a las cuales debe adecuarse para que el dispositivo móvil pueda conectarse a los recursos informáticos del Poder Judicial de San Juan.
- Auditorías y monitoreo de las actividades efectuadas.
- Registro de las personas que usan dispositivos no pertenecientes al Poder Judicial de San Juan.

Trabajo a distancia

El trabajo a distancia deberá ser solicitado y autorizado por la dirección a la cual pertenezca el usuario para luego ser comunicado a la Dirección de Informática quien validará el requerimiento en conjunto con el Área de Ciberseguridad.

Los controles y disposiciones que deben contemplarse incluyen :

- Asegurar el cifrado de las comunicaciones
- Concientizar sobre la amenaza de acceso no autorizado a la información o recursos por parte de otras personas que utilizan el espacio de trabajo remoto, por ejemplo, familiar o amigo.
- Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto cuando sea necesario
- Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Poder Judicial de San Juan y los sistemas internos y servicio a los cuales el trabajador remoto solo estará autorizado a acceder.
- Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
- Proveer el hardware y el soporte y mantenimiento del software, cuando sea necesario.
- Efectuar auditorías y monitoreo de las actividades efectuadas remotamente.
- Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

- Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.
- Se deberán implementar regularmente procesos de auditoría específicos para los casos de accesos remotos. Se deberá llevar un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

Política de Recursos Humanos

Objetivos

- Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en el "Acuerdo de Confidencialidad", al cual el empleado debe allanarse y firmar en conformidad. Así también debe verificarse el cumplimiento de este último durante su estancia laboral.
- Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren dispuestos a respetar el Protocolo de Seguridad Informática del Poder Judicial de San Juan en el transcurso de sus tareas normales.
- Establecer Acuerdos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Antes del empleo

Funciones y responsabilidades del puesto de trabajo

Las funciones y responsabilidades en materia de seguridad deberán ser incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Además, se incluirán las responsabilidades generales relacionadas con la implementación del Protocolo de Seguridad Informática, el Protocolo de Uso de Recursos Informáticos y Telecomunicaciones y las responsabilidades específicas vinculadas a la protección de cada uno de los activos. así como también, a la ejecución de procesos o actividades a realizar en los puestos de trabajo.

Deberán definirse y comunicarse claramente los roles y responsabilidades de seguridad a los candidatos para el puesto de trabajo durante el proceso de preselección.

Revisión de antecedentes

Se deberán realizar revisiones de antecedentes referidas a su currículum, referencias laborales, títulos académicos, etc., de los postulantes al empleo, en concordancia con el puesto y activos a los cuales tendrá acceso, teniendo en consideración las regulaciones vigentes, ética y leyes

relevantes.

Inicio del empleo

Aceptación de Términos y Condiciones de Contratación

Los nuevos empleados deberán aceptar firmar los documentos "Acuerdo de Confidencialidad" y "Protocolo de Uso de Recursos Informáticos y Telecomunicaciones", por lo cual el empleado declarará conocer y aceptar el control y monitoreo del uso de los recursos tecnológicos que utilizará en el desempeño de sus tareas. Las copias firmadas deberán ser retenidas en forma segura por la Dirección de Recursos Humanos.

Durante el empleo

Responsabilidades de las Direcciones

Las Direcciones en todos los niveles impulsarán que se aplique el Protocolo de Seguridad Informática en concordancia con las pautas y procedimientos establecidos, por lo que se deberá también informar de su existencia y las expectativas de cumplimiento en el desempeño de sus funciones.

Concientización, formación y capacitación en Seguridad de la Información

Se deberán realizar tareas de capacitación y concientización de las políticas, normativas y procedimientos dirigidos a todos los empleados del Poder Judicial de San Juan. Dicha capacitación comprenderá requerimientos de seguridad, responsabilidades legales, uso correcto de los dispositivos tecnológicos asignados y el uso correcto de los recursos en general.

Procedimiento disciplinario

El Poder Judicial de San Juan podrá iniciar un procedimiento administrativo disciplinario con el objeto de sancionar a quienes, según las normativas estatutarias, escalafonarias y convencionales que rigen al personal de la entidad, a todos aquellos empleados o terceros que, sea cual fuere su situación de revista, violen lo establecido en el "Protocolo de Seguridad Informática".

Aquellos empleados o terceros que incumplieran sus obligaciones, ocasionando daños que obliguen a una indemnización, deriven en responsabilidad penal y/o cuando su conducta se encuentre tipificada constituyendo un comportamiento considerado delito por la Ley 26.388 de Delitos Informáticos y demás leyes especiales, será la Secretaría Administrativa de la Corte de Justicia de San Juan quien asesore sobre las sanciones a ser aplicadas por dicho incumplimiento.

Cese del empleo o cambio de puesto de trabajo

Responsabilidad del cese o cambio

Se deberán definir procedimientos y asignar responsabilidades para controlar que los procesos de cambio de función y desvinculación laboral de los empleados, contratistas o terceras personas no afecte el normal desempeño de las actividades del Poder Judicial de San Juan.

Transferencia de Conocimientos

Todos los empleados, contratistas y usuarios que tengan conocimiento relevante de ciertas operaciones y dicho conocimiento sea desconocido por el personal restante del área donde prestan servicios, deberán documentar dicha información y transferirla al Poder Judicial de San Juan antes de proceder a su desvinculación.

Política de Gestión de Activos

Objetivos

- Garantizar que los activos de información reciban un apropiado nivel de protección.
- Clasificar la información para señalar su sensibilidad y criticidad. Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Responsabilidad sobre los activos

Inventario de activos

Se deberá mantener un inventario de activos preciso y actualizado, debiendo ser revisado con una periodicidad no mayor de tres meses, cada activo deberá poseer un propietario asignado. Todos los activos deberán estar claramente identificados y tipificados según sea:

- Información: bases de datos, archivos de datos, documentación, contratos, acuerdos.
- Activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios.
- Activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos.
- Instalaciones: tendido eléctrico, red de agua y gas, etc.
- Servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, energía, y aire acondicionado.
- Personas: sus calificaciones, habilidades y experiencia.
- Activos intangibles: tales como la reputación y la imagen del Poder Judicial de San Juan.

Propietarios de activos

Deberán designarse propietarios de los activos registrados, quienes:

- Informarán sobre cualquier cambio que afecte el activo del cual es propietario.
- Clasificarán los activos en función a su sensibilidad y criticidad.
- Velarán por la implementación de controles de seguridad requeridos para proteger los mismos.

Los propietarios serán responsables de los activos asignados. La implementación de los controles de seguridad podrá ser delegada a personal especializado, como también la gestión técnica u operativa, pero el propietario seguirá siendo responsable por los mismos.

Será menester del Poder Judicial de San Juan el mantener actualizada una ***Matriz de Activos y su***

Propietarios.

Uso aceptable de activos de tecnología de información

Se identificarán, documentarán y definirán normativas generales para el uso de los activos de tecnología, en el documento "Protocolo de Uso de Recursos Informáticos y Telecomunicaciones" (PUA). Todos los empleados, sin importar su situación de revista, contratistas o usuarios de terceras partes, deberán seguir las reglas establecidas en dicho documento. Toda excepción a la normativa deberá ser autorizada por el máximo responsable del área que solicita la excepción al cumplimiento de la misma.

Devolución de activos

Todos los empleados, contratistas y usuarios de terceras partes deberán devolver todos los activos (equipamiento tecnológico, software, documentos, tarjetas de ingreso, token, etc.) que les fueron asignados, inmediatamente a la terminación de su empleo, contrato o acuerdo. Por tal razón deberá existir un "Procedimiento de Recupero de Bienes" , como también un "Procedimiento de Devolución de Dispositivos Digitales Portátiles", que permita el adecuado cumplimiento de esta tarea.

Política de clasificación de la información

Directrices de clasificación de la información

Se deberán definir procedimientos de clasificación para determinar la criticidad de la información que se administra en el Poder Judicial de San Juan, en base a las tres características clave de Seguridad de la Información: Confidencialidad , Integridad y Disponibilidad .

Etiquetado y manipulación de activos de información

Se deberán definir procedimientos de etiquetado y de manejo de los activos de información de acuerdo al esquema de clasificación establecido y criticidad de la información.

Los mismos contemplarán los recursos de información tanto en formatos físicos como digitales e incorporarán las actividades de procesamiento de la información referidos a copias, almacenamiento, transmisión por correo electrónico, telefonía o transmisiones de datos a través de sistemas de intercambio de archivos.

Para cada uno de los niveles de clasificación, se deben definir los procedimientos de manejo seguro, incluyendo las actividades anteriormente mencionadas así como también las de desclasificación y destrucción.

Gestión de soportes de almacenamiento

Soportes removibles

Se deberán implementar procedimientos para la gestión de los soportes informáticos extraíbles, debiendo considerarse aspectos tales como la autorización y registro del retiro de soportes de almacenamiento removibles fuera de los edificios del Poder Judicial de San Juan.

Se deberán almacenar los soportes de medio extraíbles (dispositivos USB, cintas magnéticas, discos externos, etc.) en un ambiente seguro y protegido, teniendo en cuenta la criticidad de la información contenida y las especificaciones de los fabricantes o proveedores del soporte de almacenamiento.

Eliminación segura de soportes de información

Se deberán implementar procedimientos para el borrado seguro de la información al declararse la baja del soporte de almacenamiento que lo contiene, como también procedimientos de borrado seguro para las operaciones de reciclado de los dispositivos de almacenamiento teniendo en cuenta que el mecanismo de eliminación debe contemplar el tipo de dispositivo y la criticidad de la información contenida.

Los procedimientos de eliminación segura deberán considerar elementos de soporte de información, tales como papeles, cintas magnéticas (datos, audio y video), discos magnéticos, dispositivos de almacenamientos ópticos, unidades extraíbles de estado sólido y cualquier otra tecnología o soporte de almacenamiento de datos.

Los medios de almacenamiento que no puedan ser reutilizados deberán ser destruidos físicamente de manera apropiada para que la información contenida no pueda ser recuperada utilizando técnicas forenses.

Tránsito de soportes de almacenamiento

Se deberá proteger la información y los soportes de almacenamiento en tránsito conforme a la sensibilidad y criticidad de la información a transportar, razón por la cual se deben definir procedimientos de transporte de soportes de almacenamiento teniendo en cuenta el cifrado de la información contenida en el soporte, utilización de servicios de mensajería confiables, la adopción de embalajes sellados, entrega en mano, o cualquier otro mecanismo para asegurar el mismo durante su traslado.

Política de control de accesos

Objetivos

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red del Poder Judicial de San Juan y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la Seguridad de la Información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Requerimientos para el control de accesos

Política de gestión de accesos

Se controlará el acceso a la información y a los recursos tecnológicos del Poder Judicial de San Juan. Se definirán procedimientos que tengan en cuenta aspectos tales como:

- Segregación de las funciones referidas a quien solicita, quien autoriza y quien concede operativamente el acceso.
- Identificación del propietario de la información, del usuario que requiere el acceso y la aplicación a la cual se desea acceder.
- Identificación de los requerimientos de seguridad de las aplicaciones y toda información relevante de seguridad, relacionada a las mismas.
- Existencia de criterios políticas de acceso coherentes con el punto 7.2 (Política de clasificación de la información)
- Definición de perfiles de acceso de usuarios en las aplicaciones.
- Tipos de accesos, informando si son internos o externos, públicos o privados.
- Requerimientos de revisión periódica de los accesos concedidos.
- Revocación de los derechos de acceso
- Administración de cuentas de usuarios y permisos de acceso de los mismos a los sistemas y dispositivos de red del Poder Judicial de San Juan.

Control de acceso a las redes

Se establecerán todas las reglas de acceso, sobre la premisa "Todo acceso a la información y recursos tecnológicos está prohibido, a menos que se permita explícitamente".

Siendo así todos los casos de accesos negativos salvo expresamente que se indique lo contrario. Los usuarios tendrán acceso solo a la red y a los servicios de red que hubieran sido específicamente autorizados.

Gestión de acceso de usuarios

Creación y eliminación de cuentas de usuario

Cada usuario deberá tener un identificador único (unívoco) denominado "cuenta de usuario" , el cual será de uso personal y exclusivo, cuyo fin será garantizar la trazabilidad de las operaciones efectuadas por él.

Se deberán definir procedimientos que permitan crear y eliminar cuentas de usuarios con el fin de otorgar y revocar el acceso a los sistemas, bases de datos y servicios de información. Dichos procedimientos deberán:

- Utilizar nombre de cuentas de usuario identificables, de manera tal que se pueda determinar inequívocamente las actividades realizadas por las mismas, ya sean cuentas de usuario o cuentas de servicio.
- Evitar que existan múltiples cuentas de usuario asociadas a un solo individuo salvo excepciones por cuestiones de seguridad, según se indica en el punto 8.2.3 ("Gestión de

asignación de permisos de acceso con privilegios especiales").

- Evitar la creación y uso de cuentas de usuario genéricas, compartidas para un grupo de usuarios o una tarea específica. Esto, será permitido únicamente por razones operativas, debiendo requerir un profundo análisis y autorización del Área de Ciberseguridad antes de su creación.
- Los nombres de cuenta de usuario no deberán dar indicios del nivel de privilegios de la misma.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron de funciones, de áreas de pertenencia o se desvincularon del Poder Judicial de San Juan.
- Incluir cláusulas en los contratos de personal y de servicios que se especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados en caso de corresponder, según lo dispuesto en el punto 6.3.3 ("Procedimiento disciplinario").
- Efectuar revisiones periódicas con el objeto de:
    - Inhabilitar cuentas de usuarios inactivas por más de tres meses.
    - Inhabilitar cuentas de usuarios desvinculados del Poder Judicial de San Juan.
    - Eliminar cuentas de usuarios inactivas por más de dos años.
    - Eliminar las cuentas de usuarios redundantes o no identificables, previo análisis de sus actividades.
- Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

En el caso de existir excepciones para evitar inhabilitar o eliminar cuentas de usuario, estas deberán ser debidamente justificadas y aprobadas por el Área de Ciberseguridad.

Gestión de asignación de permisos de acceso

Se controlará la asignación y uso de privilegios a todas las cuentas de todos los sistemas y servicios.

Los Propietarios de Información serán los encargados de aprobar la asignación de los permisos de acceso y solicitar su implementación, que también deberá ser autorizada por el Área de Ciberseguridad.

El proceso de autorización deberá tener en cuenta los siguientes aspectos:

- Se deberá aplicar el principio de asignación de mínimos privilegios.
- Identificar los niveles de acceso existentes en los sistemas, bases de datos y aplicaciones.
- Verificar que el nivel de acceso a otorgar sea adecuado al rol del usuario y que no comprometa la segregación de funciones.
- Establecer un proceso de autorización que registre todos los derechos de acceso asignados.
- Priorizar que los permisos de acceso se apliquen a "roles" en los sistemas, antes de aplicarlos directamente a los usuarios.

Gestión de asignación de permisos de acceso con privilegios especiales

La asignación y uso de derechos de acceso con privilegios especiales deberá seguir la misma política de permisos de acceso definida previamente, pero además se considerarán los siguientes aspectos:

- No deberán utilizarse cuentas de usuarios con derechos de acceso privilegiados para realizar actividades regulares, sino que sólo serán utilizadas ante la necesidad de realizar tareas específicas que lo requieran. Solo deberán ser utilizadas ante necesidades específicas para realizar tareas de contingencia, recupero o reconfiguración que lo requieran.
- Un usuario con privilegios especiales debería poseer dos cuentas de usuario, una para sus tareas habituales y otra para realizar estrictamente actividades que requieran permisos especiales.
- Solo deberán asignarse en caso de necesidad de uso, basado en los requisitos mínimos necesarios para realizar las tareas y estar debidamente documentadas.
- Se deberá revisar periódicamente la actividad de los usuarios con derechos de accesos privilegiados, para verificar que solo sean utilizados para las actividades que dieron motivo a su asignación.

Distribución de contraseñas y de dispositivos de acceso

Se deberá establecer un procedimiento para la distribución segura de contraseñas o de cualquier otro tipo de dispositivos o mecanismos de autenticación, por lo que no se deberá enviar por correo electrónico la credencial compuesta por usuario y contraseña en texto plano; en igual sentido, no podrán usarse herramientas de mensajería instantánea para la distribución de las mismas.

Revisión de derechos de acceso de los usuarios

A fin de mantener un control eficiente del acceso a los datos y servicios de información, el Área de Ciberseguridad podrá llevar a cabo procesos formales de revisión de todos los accesos.

Se deberán revisar periódicamente los derechos de acceso y privilegios asignados a los usuarios a fin de verificar que los mismos hayan sido autorizados debidamente y aún requieran vigencia.

Revocación y cambios de derechos de acceso

Se deberán implementar procedimientos formales para la revocación y cambios de derechos de acceso de los usuarios en todos los sistemas y servicios.

Tras la desvinculación del usuario, se deberán eliminar los derechos de acceso a todos los sistemas y servicios de información utilizados por el individuo, verificando previamente que se pudiera seguir accediendo con otras credenciales activas al sistema o servicio referido.

Ante un cambio de función, se deberán remover todos los derechos de acceso que no fueron aprobados para la nueva función, comprendiendo todos los derechos de accesos lógicos y físicos, como ser llaves, tarjetas de identificación y accesos a instalaciones de procesamiento de la información.

Se deberán cambiar las contraseñas de acceso que pudieran conocer el empleado, contratista o usuario de tercera parte tras la finalización de su contrato o ante un cambio de función cuando dicha contraseña formará parte de una credencial de acceso de administración aún activa.

Responsabilidades del usuario

Responsabilidad en el uso de las contraseñas

Los usuarios deberán seguir las buenas prácticas de seguridad referidas al uso de contraseñas en concordancia con el apartado "Gestión de contraseñas de usuarios", debiendo cumplir con las siguientes premisas:

- Mantener las contraseñas en secreto: los usuarios deberán mantener la confidencialidad de las mismas ya que las contraseñas son consideradas información personal, no debiendo ser compartidas, ni aún con su personal jerárquico.
- Cuando existiera indicio de que la confidencialidad de la contraseña hubiera sido comprometida, esto se deberá informar y solicitar el cambio de la misma inmediatamente.
- Seleccionar contraseñas que no estén basadas en datos que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, como ser nombres, números de teléfono, número de oficina, fechas de cumpleaños, etc.
- No reutilizar o reciclar viejas contraseñas.
- No incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- No almacenar contraseñas en papel, archivos de texto, planillas de cálculo o cualquier aplicación cuya función no sea expresamente el almacenamiento seguro de contraseñas.
- No usar gestores de contraseñas que almacenan las contraseñas en Internet.

Control de acceso a sistemas y aplicaciones

Política de utilización de los servicios de red

Se restringirá y controlará el acceso a los servicios de red tanto internos como externos, en concordancia con el apartado Gestión de acceso de usuarios, para garantizar que los usuarios que accedan a las redes y a sus servicios no comprometan la seguridad de los mismos.

Se deberán desarrollar procedimientos para conceder o derogar derechos de acceso a la información, identificando las redes y servicios a los cuales se concedió el mismo y teniendo en cuenta los apartados de Gestión de asignación de permisos de acceso y Gestión de asignación de permisos de acceso con privilegios especiales.

Procedimientos seguros de inicio de sesión

El acceso a los servicios de información deberá ser posible solo a través de un proceso de inicio de sesión seguro; no deberá divulgar ningún indicio que provea asistencia a usuarios no autorizados.

El proceso de inicio seguro deberá:

- Desplegar un aviso informativo, advirtiendo que sólo los usuarios autorizados pueden iniciar sesión en el equipo informático.
- Evitar mostrar mensajes de ayuda que pudieran asistir al usuario durante el procedimiento de conexión, que diera indicio del dato erróneo (usuario o contraseña) ante una autenticación incorrecta.
- Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
- Será condición obligatoria de los usuarios firmar el "Protocolo de Uso de Recursos Informáticos y Telecomunicaciones" antes de acceder a los recursos tecnológicos del Poder Judicial de San Juan, consintiendo mediante esta firma su conocimiento y aceptación.
- Evitar configurar el equipo informático con credenciales almacenadas que provoquen el inicio de sesión de forma automática.
- Registrar todas las conexiones exitosas y los intentos de conexión fallidas.
- Evitar implementaciones que transmitan las contraseñas en texto plano sobre la red de datos.
- Implementar medidas para la protección ante ataques de fuerza bruta, como ser:
    - Bloqueo de la cuenta del usuario, inmediatamente luego de cierto número de intentos fallidos. Por ejemplo, bloqueo de la cuenta del usuario luego de 5 (cinco) intentos fallidos.
    - Desbloqueo automático de la cuenta luego de cierto tiempo de haberse bloqueado. Por ejemplo, desbloqueo de la cuenta del usuario luego de 10 (diez) minutos de haberse bloqueado

Autentificación de usuarios para conexiones externas

Las conexiones externas representan un gran riesgo a la infraestructura tecnológica del Poder Judicial de San Juan. Por consiguiente, el acceso de usuarios remotos estará estrictamente limitado y sujeto al cumplimiento de procesos de aprobación, los cuales deberán requerir de la expresa autorización del director del área de pertenencia y del Área de Ciberseguridad.

Se deberá considerar la implementación de mecanismos de autenticación extras a la credencial de acceso (usuario y contraseña), es decir, el uso de más de un factor de autenticación ya sea mediante métodos de autenticación física (tokens), tarjetas coordenadas, o bien cualquier otro mecanismo que refuerce la identificación de la conexión externa.

Cuando se utilicen mecanismos de autenticación físicos, deben implementarse procedimientos que incluyan asignación de la herramienta de autenticación, registro de los poseedores de dichos autenticadores, mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó y procedimiento de revocación de acceso del autenticador en caso de compromiso de seguridad (pérdida o robo).

Las conexiones externas deberán estar cifradas, con algoritmos actualizados, pudiendo ser de los tipos:

- Conexión cifrada por medio de una Red Privada Virtual (VPN) a la red del Poder Judicial de San Juan.
- Conexión cifrada con Protocolo TLS.
- Conexión cifrada con Protocolo SSH.

Gestión de contraseñas de usuarios

Se deberán implementar sistemas de gestión de contraseñas que garanticen la confidencialidad y eficiencia en la administración de las mismas, en concordancia con los apartados Responsabilidad en el uso de las contraseñas y Distribución de contraseñas y de dispositivos de acceso de la presente política.

Se deberá controlar la gestión de contraseñas mediante un proceso formal que tendrá en consideración los siguientes aspectos:

- Se deberán generar mecanismos que permitan a los usuarios cambiar las contraseñas asignadas inicialmente la primera vez que ingresan al sistema. Es decir que los usuarios estarán obligados a cambiar las contraseñas recibidas inicialmente por parte de los administradores.
- Cuando se requiera resguardar las contraseñas se deberán utilizar aplicaciones especialmente diseñadas para el almacenamiento seguro de las mismas, teniendo en cuenta no utilizar aplicaciones que alojan su base de datos de contraseñas en repositorios de Internet.
- Se establecerán como mínimo las siguientes características básicas de complejidad: longitud mínima de 8 (ocho) caracteres, compuesta por mayúsculas, minúsculas y números en su conformación.
- Se deberá establecer un proceso que solicite el cambio de la contraseña cada 1 (un) año impidiendo la reutilización de las mismas.
- No se deberán distribuir ni almacenar las contraseñas en texto plano.
- Las contraseñas deberán almacenarse en sistemas diseñados para tal fin, denominados "gestores de contraseñas".
- Se deberán cambiar las contraseñas por defecto de los sistemas y dispositivos luego que hubiera finalizado su instalación inicial.
- Se deberán cambiar las contraseñas de las cuentas utilizadas por los servicios de soporte externos a la planta del Poder Judicial de San Juan luego que la tarea de los mismos haya finalizado.
- Se deberá implementar el cifrado mediante contraseña en operaciones de "Copias de resguardo y restauración".
- Para asegurar el adecuado uso de las contraseñas, se deberán registrar y auditar las actividades relativas a la gestión de las mismas.

Gestión de contraseñas críticas

Las cuentas administrativas genéricas (administrador, root, admin, etc.) con privilegios especiales para efectuar actividades críticas serán resguardadas de manera especial y sólo serán utilizadas ante necesidades específicas para realizar tareas de contingencia, recupero o reconfiguración

que lo requieran y solo por un determinado período de tiempo.

El Área de Ciberseguridad definirá el procedimiento para la administración de contraseñas críticas que contemplará, por lo menos, los siguientes aspectos.

- La conformación de la contraseña crítica deberá poseer un mayor nivel de complejidad que la definida en el apartado Gestión de contraseñas de usuarios.
- La definición de la misma será efectuada como mínimo por dos personas, de tal manera que ninguna de ellas conozca la contraseña completa.
- Las partes de las contraseñas serán resguardadas físicamente, en sobres cerrados por duplicado.
- La utilización de las contraseñas críticas será formalmente registrada, documentando las causas que determinaron su uso, usuario que hizo uso de la misma y las actividades que se realizaron con ella.
- Las contraseñas críticas se renovarán una vez utilizada, procediendo luego a su resguardo nuevamente.

Detección de aplicaciones de riesgo

Se deberán implementar controles para detectar y restringir el uso de sistemas, aplicaciones y utilidades de software que pudieran anular o evitar los controles de seguridad o que pudieran usarse para evaluar la seguridad de la infraestructura tecnológica del Poder Judicial de San Juan sin haber sido debidamente autorizados.

Acceso a Internet

El acceso a Internet deberá ser utilizado para propósitos laborales. Se habilitará el acceso básico a Internet a todos los usuarios que cuenten con una cuenta habilitada, estableciéndose pautas de utilización de Internet conforme al documento "Protocolo de Uso de Recursos Informáticos y Telecomunicaciones".

Se deberán definir procedimientos para solicitar y aprobar acceso a sitios restringidos de Internet. Dichos accesos deberán ser solicitados por el responsable de la dirección a cargo del personal que lo requiera. Se llevará registro de los accesos de todos los usuarios a Internet con el objeto de realizar revisiones de auditoría o análisis forense ante incidentes de seguridad.

Control de acceso al código fuente

Acerca del tema de referencia :

- Se deberá restringir y gestionar el acceso al código fuente de las aplicaciones de software desarrolladas por el Poder Judicial de San Juan, con el fin de evitar que sean introducidos cambios sin la debida autorización y control de las áreas involucradas o copia no autorizada del código fuente.
- Se deberá definir un responsable de la función de "Administrador de código fuente", quien tendrá a cargo la custodia de los programas fuente y deberá llevar un registro actualizado de todos los módulos en uso, indicando nombre del módulo, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).

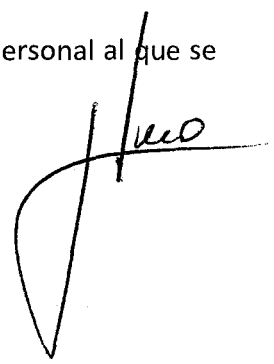
- Se deberá establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen, es decir que exista trazabilidad de versión entre el programa objeto y el código fuente.
- Se deberá establecer la existencia de un "Implementador de Producción", el cual será el responsable del pase a dicho ámbito.
- Se deberá desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
- Se deberá prohibir el resguardo de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.
- Se deberá prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
- Se deberán realizar copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por el Poder Judicial de San Juan en los procedimientos que surgen de la presente política, teniendo para ello presente, el apartado Copia de Resguardo y Restauración.
- Por defecto se define que la licencia de uso será *MIT*, salvo en los casos que se determine lo contrario.

Identificación automática de estaciones de trabajo

Se deberá tener en cuenta la identificación automática de las estaciones de trabajo conectadas a la red interna del Poder Judicial de San Juan, con el objeto de validar las conexiones generadas, debiendo segregarse de la red aquellas estaciones de trabajo que no estuvieran normalizadas según las directivas de seguridad preestablecidas o que no pudieran identificarse debidamente.

Identificación y autenticación de los usuarios

- Se deberán seguir expresamente las siguientes directivas:
- Todos los usuarios (incluido el personal de soporte técnico, operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador unívoco (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable y a fin de garantizar la trazabilidad de las transacciones.
- Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.
- En circunstancias excepcionales, cuando existe un claro beneficio para el Poder Judicial de San Juan, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de la que se trate.
- Si se utilizara un método de autenticación físico (por ejemplo, autenticadores de hardware), debe implementarse un procedimiento que incluya:
    - Asignar la herramienta de autenticación.
    - Registrar los poseedores de autenticadores.
    - Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.



- Revocar el acceso del autenticador, en caso de compromiso de seguridad.

Política de criptografía

Objetivo

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, no repudio, la autenticidad y/o la integridad de la información.

Cumplimiento de requisitos

Política de uso de controles criptográficos

Se utilizarán sistemas y técnicas criptográficas para el resguardo de la información con el fin de asegurar una adecuada protección de su confidencialidad, tales son los casos de :

- Contraseñas de acceso a sistemas.
- Almacenamiento de datos, cuando el nivel de protección sea requerido.
- Cifrado de dispositivos móviles.
- Transmisión de información, dentro y fuera del ámbito del Poder Judicial de San Juan.
- Copias de resguardo de la información.
- O bien, producto de la evaluación de riesgo sobre el activo de información que se desea asegurar su confidencialidad.

Se deberán utilizar algoritmos de cifrado robustos que se validarán periódicamente por el Área de Ciberseguridad, evitando el uso de algoritmos de cifrado obsoletos permeables al avance de las técnicas de descifrado.

Al implementar la Política de Criptografía en el Poder Judicial de San Juan se considerarán, cuando sea necesario, los controles aplicables a la exportación e importación de tecnología criptográfica.

Firma digital

Cuando sea necesario asegurar la autenticidad e integridad de los documentos electrónicos, los mismos deberán firmarse digitalmente.

Se deberán tomar los recaudos pertinentes para proteger la confidencialidad de las claves privadas; dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Asimismo, es importante proteger la integridad de la clave pública mediante el uso de un certificado de clave pública .

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información.

Al utilizar firmas y certificados digitales deberá supeditarse a lo dispuesto por la Ley N° 25.506 , el Decreto N° 2628/02 y al conjunto de normas complementarias que fijan o modifican

competencias y establecen procedimientos que describen las condiciones bajo las cuales una firma digital es legalmente válida.

Servicios de No Repudio

Se deberán utilizar los servicios de "No Repudio", cuando sea necesario garantizar transacciones electrónicas que pudieran generar disputas acerca de la ocurrencia y participación en las mismas. Es decir, que el individuo que envía el mensaje no pueda negar que es el emisor del mismo (no repudio en origen) y que el receptor no puede negar que recibió dicho mensaje (no repudio en destino) garantizando, de este modo, la participación de las partes en dicha comunicación.

Procedimientos para la gestión de claves criptográficas

Se deberá implementar un proceso seguro de administración de claves criptográficas para respaldar la utilización por parte del Poder Judicial de San Juan de las claves secretas (en criptografía simétrica) y las claves privadas (en criptografía asimétrica) para protegerlas contra modificación, destrucción, copia y divulgación no autorizada.

Se deberán implementar los mecanismos y tomar los recaudos necesarios para proteger la confidencialidad de las claves privadas, por lo cual se deberán redactar procedimientos que estipulen operaciones de:

- Almacenamiento de claves secretas y privadas , incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
- Renovación y actualización de claves , incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
- Eliminación de claves , incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo, cuando las claves hayan caducado.
- Utilización de claves como parte de la administración de la continuidad de las operaciones, por ejemplo, para la recuperación de la información cifrada.
- Generación e implementación de claves en operaciones de "Copia de resguardo y restauración".

Política físico y ambiental

Objetivos

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Poder Judicial de San Juan.

Proteger el equipamiento de procesamiento de información crítica del Poder Judicial de San Juan ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección de dicho equipamiento en su traslado y permanencia fuera de las áreas protegidas por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del

equipamiento informático que alberga la información del Poder Judicial de San Juan.

Implementar medidas para proteger la información manejada por el personal en las oficinas en el marco normal de sus labores habituales. Proporcionar protección acorde a los riesgos identificados.

Áreas Seguras

Perímetro de seguridad física

Se deberán definir perímetros de seguridad, para proteger las áreas que contienen instalaciones de procesamiento y almacenamiento de información, sala de los equipos de comunicaciones, instalaciones de suministro de energía eléctrica, instalaciones de aire acondicionado y cualquier otra área considerada crítica tales que su puesta fuera de servicio o mal funcionamiento pueda entorpecer el normal funcionamiento de los sistemas de información del Poder Judicial de San Juan.

Controles físicos de entrada

Todas las instalaciones edilicias del Poder Judicial de San Juan deberán implementar controles de acceso físico y monitoreo mediante cámaras de seguridad para supervisar la entrada y salida de personas y materiales.

Se deberá registrar fecha, horario y motivo de la visita al ingresar a las áreas protegidas, ya que sólo se permitirá el acceso por propósitos específicos y autorizados. También se deberá registrar fecha y hora de egreso de las mismas.

Se deberán almacenar debidamente los registros de acceso a los efectos de auditorías o investigación de incidentes.

Se controlará y limitará el acceso a la información clasificada y a las instalaciones de procesamiento de información exclusivamente a las personas autorizadas.

Se mantendrá un registro protegido para permitir auditar todos los accesos. Se deberá usar una identificación unívoca visible para todo el personal del área protegida e instruir al mismo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado así como también de cualquier persona que no exhiba una identificación visible.

Se revisarán y actualizarán cada 6 meses los derechos de acceso a las áreas protegidas: dichos procesos serán documentados y firmados por el responsable de la Unidad Organizativa de la que dependa. Se revisarán los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad.

Seguridad de oficinas, despachos e instalaciones

Se aplicarán mecanismos extra de control de acceso de seguridad física y/o electrónica a las oficinas y salas del Poder Judicial de San Juan definidas como áreas críticas, considerando la actividad desempeñada o el activo que administran. Se definirán los siguientes sitios como áreas críticas, dada la actividad desarrollada en las mismas:

- Oficinas principales de La Corte de Justicia de San Juan
- Oficinas de Tesorería.
- Piso de la Dirección de Informática.
- Oficina de liquidación de haberes
- Sala de los equipos de comunicaciones
- Sala de servidores

Protección contra amenazas de origen ambiental y externas

Deberán existir controles, adecuadamente ubicados, de protección física contra incendios. Deberá existir personal de seguridad física para contrarrestar amenazas de revueltas internas o externas y resguardo las áreas protegidas definidas en los puntos 10.1.2 (Controles físicos de entrada) y 10.1.3 (Seguridad de oficinas, despachos e instalaciones).

Trabajo en áreas críticas

Para incrementar la seguridad de las áreas críticas, se deberán establecer controles y lineamientos adicionales, tanto para el personal del Poder Judicial de San Juan, como para las actividades desarrolladas por terceros que tengan lugar en dichas áreas, como ser:

- Implementar controles extras mediante monitoreo con cámaras de seguridad.
- Evitar la ejecución de trabajos por parte de terceros sin supervisión de personal del Poder Judicial de San Juan.
- Limitar el acceso a las áreas protegidas solo al personal perteneciente a dichas áreas o cuando sean autorizados por personal responsable de las mismas.
- Considerar impedir el ingreso de dispositivos de almacenamiento portable a menos que sea necesario para el desempeño de sus funciones.

Áreas de acceso público, de carga y descarga

Se deberán establecer controles en las áreas de recepción, carga y descarga a fin de impedir accesos no autorizados a las instalaciones edilicias del Poder Judicial de San Juan. Las áreas de recepción, carga y descarga deberán estar aisladas de las instalaciones de procesamiento de información y de las áreas protegidas.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

- Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Poder Judicial de San Juan, sólo al personal previamente identificado y autorizado.
- Diseñar el área de depósito de manera tal, que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
- Verificar y registrar el material entrante al ingresar a las instalaciones edilicias del Poder Judicial de San Juan.
- Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

Seguridad de los equipos

Emplazamiento y protección de equipos

El equipamiento deberá ser será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas, peligros ambientales y acceso no autorizado, teniendo en cuenta los siguientes puntos:

- Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
- Ubicar las instalaciones de procesamiento y almacenamiento de información que procesan datos clasificados en un sitio que permita la supervisión constante.
- Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales por robo, hurto, incendio, polvo, calor y radiaciones electromagnéticas.
- No se deberá comer, beber o fumar en proximidad de los equipos de procesamiento de la información como ser el centro de cómputos o la sala de comunicaciones.

Seguridad en el suministro eléctrico

El equipamiento de procesamiento de datos deberá estar protegido ante posibles fallas en el suministro de energía u otras anomalías eléctricas. Para asegurar la continuidad del suministro de energía, se deberá contar con equipamiento de Suministro de Energía Ininterrumpible (UPS) y grupo Generador de Energía Eléctrica de respaldo.

Se deberá proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se deberá implementar, además, protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo con las normativas vigentes, adicionando filtros de protección contra descargas eléctricas naturales a todas las líneas de ingreso de energía eléctrica y comunicaciones.

Seguridad del cableado

El cableado de comunicaciones que transporta datos y brinda apoyo a los servicios de información deberá estar protegido contra intercepción o daño. Por ello, el mismo deberá:

- Cumplir con los requisitos técnicos vigentes de la República Argentina.
- Separar los cables de energía de los cables de comunicaciones de datos para evitar interferencias.
- Proteger el tendido del cableado de red troncal entre los pisos, mediante la utilización de ductos blindados y/o con controles de acceso físicos.
- Utilizar piso técnico y/o cableado embutido en la pared, siempre que sea posible.
- Utilizar medios de transmisión alternativos seguros cuando no sea posible garantizar la seguridad en el cableado.

Mantenimiento del equipamiento informático

Se deberán realizar tareas periódicas de mantenimiento preventivo del equipamiento de procesamiento de datos y comunicaciones para asegurar su disponibilidad e integridad permanentes, de acuerdo con los intervalos de servicio y especificaciones recomendados por el

proveedor y con la autorización formal del responsable de la Dirección de Informática.

La Dirección de Informática deberá mantener un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo. Se deberá eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

Seguridad de los equipos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información fuera del ámbito del Poder Judicial de San Juan deberá ser autorizado por el responsable patrimonial.

En el caso de que en el mismo se almacene información clasificada, su empleo en esta modalidad debe ser aprobado, además, por el propietario de la misma.

Cuando se autorice el uso de equipamiento informático fuera del ámbito de las dependencias del Poder Judicial de San Juan, el mismo deberá contar con controles de seguridad preventivos ante pérdida, robo, daño o intercepción.

Se deberán respetar permanentemente las instrucciones del fabricante respecto del cuidado del activo. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Poder Judicial de San Juan cuando el activo lo amerite.

Reutilización o baja de equipamiento informático

Se deberán aplicar operaciones de borrado seguro a todo equipamiento informático antes de que el mismo sea normalizado para su reutilización, previo resguardo de la información útil y licencias alojadas en el mismo y teniendo en cuenta las directivas mencionadas en el apartado Eliminación Segura de Soportes de Información.

Retiro de propiedad del Poder Judicial de San Juan

El equipamiento, soportes de almacenamiento, información y software no se deberán retirar o transmitir fuera del ámbito de las dependencias del Poder Judicial de San Juan sin previa autorización formal de la correspondiente Dirección a la cual pertenezca.

Se deberán llevar a cabo comprobaciones periódicas para detectar el retiro no autorizado de activos del Poder Judicial de San Juan.

Sesiones activas en la estación de trabajo

Los usuarios deberán cerrar las sesiones de las aplicaciones, sistemas y servicios de red cuando no estén siendo usadas.

Al ausentarse momentáneamente de su puesto de trabajo, deberán cerrar la sesión activa o en su defecto, bloquear el equipo informático para evitar el acceso indebido al mismo durante su ausencia.

Se deberá establecer el bloqueo automático de las pantallas cuando el equipo se encuentre desatendido por más de 5 (cinco) minutos con el objeto de evitar accesos no autorizados a los

mismos.

Apagado de la estación de trabajo

Los usuarios deberán cerrar las sesiones activas al finalizar su jornada laboral y apagar el equipo informático o en su defecto cerrar las sesiones de servicios abiertos y activar el bloqueo del mismo cuando el Área de Ciberseguridad solite dejar encendido el mismo para realizar tareas de mantenimiento fuera del horario laboral o cuando cuente de una autorización expresa previamente solicitada a la Dirección de Informática exponiendo los motivos de justificación.

Escritorios Limpios

Los usuarios deberán proteger la información no pública que utilizan en sus tareas, no dejando documentación en papel u otro medio de almacenamiento (pendrives, unidades removibles, cd, etc.) sobre su escritorio sin ningún tipo de control. Se deberá almacenar bajo llave en gabinetes seguros o cajas fuertes cuando corresponda, los documentos en papel y soportes de almacenamiento que posean información sensible o crítica cuando no estén siendo utilizados, especialmente fuera del horario de trabajo.

Se deberá retirar inmediatamente la información sensible o confidencial una vez impresa. Se deberán bloquear las fotocopiadoras e impresoras fuera del horario normal de trabajo y proteger los puntos de recepción y envío de correo postal.

Política de Seguridad en las Operaciones

Objetivos

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Procedimientos y Responsabilidades Operativas

Documentación de los Procedimientos Operativos

Los procedimientos operativos deberán ser identificados, documentados, actualizados y puestos a disposición de todos los usuarios que lo requieran.

Las responsabilidades referidas a las tareas operativas deberán estar formalmente asignadas. Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

- Información que gestiona.
- Requerimientos o interdependencias con otros sistemas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan

surgir durante la ejecución de tareas.

- Personal de asistencia a quienes contactar en caso de dificultades operativas o técnicas imprevistas.

Cambios en las Operaciones

- Se deberán definir procedimientos para controlar los cambios en los procesos operativos que pudieran afectar la seguridad en los sistemas de procesamiento del Poder Judicial de San Juan.
- Se deberá almacenar un registro detallado de los cambios para operaciones de auditoría y respuesta de incidentes, conteniendo el mismo toda información relevante a cada cambio implementado.
- Se deberá controlar que los cambios a implementar no afecten la seguridad de los procesos asociados ni de la información gestionada.
- Se deberán definir procedimientos para el control de cambios en los ambientes operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.
- Se deberá controlar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan, razón por la cual se deberá evaluar el posible impacto de los cambios previstos y verificar su correcta implementación.
- Se mantendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

- Identificación y registro de cambios significativos.
- Evaluación del posible impacto de dichos cambios.
- Aprobación formal de los cambios propuestos.
- Planificación del proceso de cambio.
- Prueba del nuevo escenario.
- Comunicación de detalles de cambios a todas las personas pertinentes.
- Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

Planificación de la capacidad

Se deberán monitorear y evaluar las necesidades de capacidad operacional actuales de los sistemas y proyectar las futuras demandas, con el objeto de garantizar que el crecimiento no ponga en riesgo las actividades operativas ante la falta de recursos.

Separación de entornos de desarrollo, pruebas y producción

Deberán existir al menos tres ambientes diferenciados de trabajo: desarrollo , pruebas y producción, los cuales deberán estar separados y ser independientes.

Deberán existir procedimientos formales para el traspaso entre estos ambientes con el fin de reducir el riesgo de cambios no autorizados en los mismos y garantizar la producción de sistemas

seguros.

Estos controles deberán tener en cuenta los siguientes aspectos:

- El personal de desarrollo no tendrá acceso al ambiente productivo, oficiando solo como asesor del personal de producción cuando lo requieran.
- Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
- Ante extrema necesidad, se establecerá un procedimiento formal de emergencia que permita registrar la autorización, acceso y cambio efectuado en el servidor de producción por el personal de desarrollo.
- El ambiente de producción deberá contar solo con el software necesario para el funcionamiento del sistema al que sirve, evitando la existencia de compiladores u otros utilitarios del sistema que pudieran alterar el correcto funcionamiento del mismo.

Protección contra Códigos Maliciosos

Controles contra Código Malicioso

Se deberán proteger los sistemas informáticos mediante la implementación de controles para prevenir, detectar, eliminar y recuperar los sistemas afectados por códigos maliciosos.

Dichos sistemas de detección deberán estar instalados y actualizados en todas las estaciones de trabajo y servidores que conforman la infraestructura tecnológica del Poder Judicial de San Juan.

Para evitar la ejecución de código malicioso, se deberá controlar toda actividad de lectura y grabación de archivos en estaciones de trabajo y servidores, todo tráfico de carga y descarga de archivos en los servidores de conexión a Internet y el tráfico y almacenamiento de los correos electrónicos con archivos adjuntos o enlaces a sitios web.

Se deberá realizar periódicamente análisis preventivos para la detección y eliminación de códigos maliciosos en los servidores y estaciones de trabajo, así como también implementar otras directivas que, en este sentido, pudieran derivar del Protocolo de Uso de Recursos Informáticos y Telecomunicaciones.

Copias de Seguridad

Copia de Resguardo y Restauración

Se definirán procedimientos para el resguardo de la información que deberán considerar:

- Cumplir, como mínimo, con la regla 3-2-1 y recomendar la adopción de la regla 3-2-1-0.
- Definir un esquema de rotulado o nomenclado de las copias de resguardo que permita contar con toda la información necesaria para identificar y administrar cada una de ellas debidamente.
- Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de

resguardo una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor y asegurando la destrucción de los medios desechados.

- Almacenar en una ubicación remota copias de resguardo junto con registros exactos y completos de las mismas y procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal y teniendo en cuenta el nivel de clasificación otorgado a la información resguardada.

- Asignar a la información de resguardo un nivel de protección física y ambiental según los requisitos del proveedor del medio de almacenamiento y las normas aplicadas en el sitio principal.

- Verificar periódicamente la efectividad de los procedimientos de copias y restauración, asegurándose que cumplan con los requerimientos de los planes de continuidad de las actividades del Poder Judicial de San Juan, según lo establecido en el Objetivo de la política.

- Minimizar los efectos de las posibles interrupciones de las actividades normales del Poder Judicial de San Juan (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

- Maximizar la efectividad de las operaciones de contingencia del Poder Judicial de San Juan con la formulación de planes que incluyan al menos las siguientes etapas:

    - Notificación/Activación: Consistente en la detección y determinación del daño y la activación del plan.

    - Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

    - Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

- Asegurar la coordinación con el personal del Poder Judicial de San Juan y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

- Cifrar la copia de resguardo, de acuerdo al apartado Política de Uso de Controles Criptográficos.

- El período de retención de las copias de resguardo deberá ser establecido por medio de una política de retención de acuerdo al tipo de información resguardada y en concordancia con el apartado Protección de los Registros del Poder Judicial de San Juan.

Registro de Actividad y Monitoreo

Registro de eventos

Se deberán registrar los eventos referidos a la actividad de usuarios y sistemas así como también eventos asociados a errores y seguridad.

Se deberán almacenar remotamente los eventos de las estaciones de trabajo críticas y servidores, con el objeto de garantizar su integridad y disponibilidad para la detección e investigación de incidentes de seguridad.

Los registros de auditoría se almacenarán localmente para las estaciones de trabajo y servidores considerados no críticos. Se deberán registrar, por lo menos, los siguientes datos:

- Inicio y cierre de sesión
- Identificación del usuario
- Identificación del equipo
- Direcciones de redes y protocolos
- Fecha y hora del evento
- Descripción del evento
- Registros de intentos de acceso al sistema exitosos y fallidos
- Registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados
- Cambios de configuración del sistema
- Ejecución de aplicaciones de sistemas
- Archivos accedidos y el tipo de acceso, cambios en los archivos
- Uso de privilegios
- Activación y desactivación de los sistemas de protección

Para el registro de los eventos se debe considerar el apartado Protección de los Registros del Poder Judicial de San Juan.

Protección del registro de información de auditoría

Se implementarán controles para la protección de los registros de auditoría almacenados contra cambios no autorizados, como ser alteración o eliminación de los mismos. Se deberán implementar controles para evitar fallas por falta de espacio de almacenamiento.

Actividad de los Administradores y Operadores

Se deberá controlar periódicamente la actividad de los usuarios administradores y operadores de sistemas que manejen información confidencial, privada o secreta.

Se deberán definir alertas automáticas que informen actividades catalogadas sospechosas, ya sea debido a accesos u operaciones indebidas o fallas de los sistemas.

Sincronización de Relojes

Se deberán sincronizar los relojes de todos los sistemas y equipos informáticos en relación a una o varias fuentes de sincronización únicas de referencia a fin de garantizar la exactitud de los

registros de auditoría.

Control en la Instalación de Software

Instalación de Software en Producción

Se deberán definir procedimientos para controlar la instalación de software en sistemas operacionales en producción que establezcan los pasos a seguir para validar autorizaciones, conformidades y pruebas previas pertinentes.

Toda aplicación, desarrollada por el Poder Judicial de San Juan o por un tercero, deberá tener un único responsable designado formalmente por la Dirección de Informática.

Ningún programador o analista de desarrollo podrá acceder a los ambientes de producción, en concordancia con el apartado Separación de entornos de desarrollo, pruebas y producción.

Se deberá conservar la versión previa del sistema como medida de contingencia y control, llevar un registro de auditoría de las actualizaciones efectuadas e instalar sólo los ejecutables en el ambiente de producción.

Se designará formalmente a los implementadores de los sistemas en producción, evitando que sean los mismos programadores o analistas de desarrollo del software que se desea poner en producción.

Gestión de Vulnerabilidades Técnicas

Vulnerabilidades Técnicas y Remediación

Se deberán efectuar pruebas técnicas y de seguridad con el objeto de conocer el grado de exposición del sistema antes de desplegarlo en producción y a fin de adoptar las medidas necesarias para minimizar los riesgos asociados. Esto también aplica para todo sistema de software desarrollado en el Poder Judicial de San Juan teniendo en cuenta las directivas del apartado Evaluación de Vulnerabilidades de Seguridad.

Se deberán minimizar los riesgos de actualización mediante la implementación de control de cambios, imponiendo la obligatoriedad de procedimientos formales que garanticen el cumplimiento de las pautas de seguridad y control. Se deberá verificar que los cambios cumplan con los requisitos solicitados y se cuente con las autorizaciones necesarias.

Se deberán establecer roles y responsabilidades asociadas a los procesos de identificación de vulnerabilidades técnicas, procedimientos de remediación mediante la instalación de actualizaciones de seguridad, implementación de directrices de configuraciones seguras y controles para asegurar su cumplimiento.

Restricciones en la Instalación de Software

Se declara la prohibición de toda instalación de software no autorizado por el Área de Ciberseguridad, ya que la instalación no controlada en los sistemas informáticos puede propiciar la exposición a vulnerabilidades, fuga de información, falta de integridad, incidentes de seguridad

de información o bien a la transgresión de derechos de propiedad intelectual.

La instalación de software deberá respetar la Ley de Propiedad Intelectual N° 11.723 y sus decretos asociados, como así también el tipo de licenciamiento designado por el autor del mismo, por lo que se prohíbe la instalación y uso de cualquier tipo de aplicación y utilidades que active licencias de manera indebida (ver apartado Derechos de Propiedad Intelectual).

Auditoría de los Sistemas en Producción

Controles de auditoría en los sistemas de información

Se deberán planificar y definir cuidadosamente las actividades de auditoría a realizar sobre los sistemas en producción, con el objeto de minimizar el impacto de interrupciones en los procesos del Poder Judicial de San Juan, por lo que deberán existir procedimientos formales para tales efectos.

Las actividades de auditoría sobre los sistemas en producción deberán tomar los recaudos necesarios que permitan revertir los cambios efectuados en los sistemas auditados.

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, ya sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos. Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo y se les otorgará el nivel de protección requerido.

Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Dirección de Informática.

Política en la Gestión de Comunicaciones

Objetivo

Evitar el uso indebido de los servicios de red e Internet permitiendo garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Gestión en la Seguridad en las Redes de Datos

Controles en las Redes de Datos

Se deberán restringir las conexiones a los dispositivos de red, permitiéndoles conectarse únicamente a los aquellos con direcciones físicas y puertos de servicios autorizados.

Se deberán definir controles que inspeccionen los paquetes de datos que circulan por la red, con el objeto de detectar tráfico sospechoso donde se intente vulnerar los sistemas informáticos.

Se deberá controlar la navegación ilimitada de Internet para evitar comprometer el rendimiento y/o estabilidad del acceso a la misma.

Se deberá controlar que los equipos informáticos que se conecten hacia y desde Internet se

efectúe a través de dispositivos de seguridad que inspeccionan el tráfico saliente y entrante, con el objeto de evitar que la navegación transgreda las normas establecidas en el Protocolo de Uso de Recursos Informáticos y Telecomunicaciones.

Se deberá controlar el tráfico de datos interno y externo de la red informática mediante dispositivos de seguridad que permitan monitorear y gestionar activamente las comunicaciones, estableciendo la autorización sobre origen y destino de las mismas.

Se deberá implementar controles para mantener la alta disponibilidad de los servicios de red y equipamiento informático interconectado.

Se deberá controlar el acceso, administración y uso de los servicios web publicados.

Se deberán mantener instalados y habilitados sólo aquellos servicios que hayan sido autorizados.

Seguridad de los Servicios Activos

El Área de Ciberseguridad definirá las pautas para garantizar la seguridad de los servicios de red del Poder Judicial de San Juan; dichos servicios activos deberán ser revisados periódicamente proponiendo recomendaciones cuando sea necesario.

Asimismo, propiciará el cumplimiento de las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto en su uso como en su administración.
- Configurar cada servicio de manera segura, siguiendo las recomendaciones de buenas prácticas de seguridad del servicio en cuestión.
- Instalar periódicamente las actualizaciones de seguridad correspondientes.
- Evaluar periódicamente la seguridad de los servicios.

Segmentación de redes

Con el fin de restringir el acceso indebido a los datos, se deberá segmentar el tráfico de datos que circulan por las redes del Poder Judicial de San Juan en función de criterios como ser, estructura organizacional, grupos de servicios utilizados, ubicación u otros. Una vez establecidos dichos ámbitos, deberán ser formalmente definidos y documentados.

Intercambio de información con actores externos

Procedimientos y Controles de Intercambio de la Información

Se deberán establecer procedimientos para solicitar y aprobar accesos especiales a Internet.

El uso de Internet estará sujeto a el Protocolo de Uso de Recursos Informáticos y Telecomunicaciones el cual considera aspectos tales como responsabilidades de los empleados con respecto a la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación de correo electrónico, redes sociales y otros.

La información intercambiada hacia y desde Internet deberá ser protegida contra la intercepción,

copiado o modificación.

Los servicios que se exponen hacia Internet deberán estar protegidos ante amenazas externas.

Se deberán implementar controles para la detección de actividades maliciosas que puedan provenir de Internet con destino hacia las redes internas del Poder Judicial de San Juan.

Se deberá hacer uso de técnicas criptográficas actualizadas para proteger la confidencialidad , integridad y la autenticidad de la información que se transmite hacia redes externas.

Acuerdos en los Intercambios de Información con Entidades Externas

Cuando se realicen acuerdos entre el Poder Judicial de San Juan y otros entes, relativos al intercambio de información y software, se deberán especificar e implementar las consideraciones de seguridad para la transferencia segura de datos entre ambas partes.

Seguridad del Correo Electrónico

El uso del servicio de correo electrónico laboral estará sujeto a el Protocolo de Uso de Recursos Informáticos y Telecomunicaciones por lo cual todos los empleados del Poder Judicial de San Juan deberán aceptar y firmar las pautas de uso declaradas en dicha política antes de acceder a la cuenta de correo electrónica asignada.

Se deberá proteger el sistema de correo electrónico para evitar accesos no autorizados, denegación de servicio, correos no deseados, suplantación de identidad del remitente y demás amenazas existentes.

El tráfico del sistema de correo electrónico laboral será analizado por sistemas antimalware con el objeto de detectar códigos maliciosos adjuntos que pusieran en peligro a la infraestructura tecnológica del Poder Judicial de San Juan.

Se prohíbe adjuntar en la cuenta de correo electrónico laboral binarios ejecutables, cifrados, multimedia de audio y/o video o archivos de gran tamaño que pudieran degradar la performance y/o capacidad del sistema.

Acuerdo de Confidencialidad en el Intercambio de Información

Se deberán identificar, revisar y documentar los Acuerdos de Confidencialidad para la protección de la información del Poder Judicial de San Juan que es transferida a entidades externas. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación del Poder Judicial de San Juan, así como cumplir con toda legislación o normativa vigente de la Administración Pública.

Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

Objetivos

Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición, desarrollo y mantenimiento de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan. Definir los métodos de protección de la información crítica o sensible.

Esta política se aplica a todos los sistemas informáticos, tanto los desarrollos propios como los de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el Poder Judicial de San Juan en donde residan los desarrollos mencionados.

El Área de Ciberseguridad junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros en función de una evaluación de riesgos.

El Área de Ciberseguridad cumplirá las siguientes funciones:

- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para:
    - El control de cambios en los sistemas
    - La verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas
    - El control de códigos maliciosos
    - La definición de las funciones del personal involucrado en el proceso de entrada de datos.

La Dirección de Informática propondrá la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere idóneo y cuyas responsabilidades se detallan en la presente cláusula. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas. El responsable del área a la que está destinado el software, incorporará aspectos relacionados con el licenciamiento , la calidad del software y la Seguridad de la Información en los contratos con terceros por el desarrollo del mismo. El responsable del Área Jurídica debe participar también en dicha tarea.

Requerimientos de Seguridad de los Sistemas

Análisis y Especificaciones de los Requerimientos de Seguridad

Se deberán especificar requisitos de seguridad en los sistemas de información (ya sean desarrollos propios o de terceros) y en todas las mejoras o actualizaciones que se les incorporen, razón por la cual, el Área de Ciberseguridad deberá formar parte del ciclo de vida de desarrollo o contratación de los sistemas informáticos según corresponda. Así también, se deben tener en cuenta las siguientes consideraciones:

- Definir un procedimiento para que durante las etapas de análisis y diseño del sistema se incorporen a los requerimientos los correspondientes controles de seguridad . Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de Sistemas, de Seguridad de la Información y Auditoría, especificando y aprobando los controles automáticos a incorporar al mismo y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.
- Evaluar los requerimientos de seguridad y los controles requeridos teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
- Considerar y evaluar que los controles en la etapa de diseño son significativamente menos costosos para implementar y mantener que aquellos incluidos durante o después de la implementación de los sistemas.

Seguridad en los Servicios accedidos desde redes públicas

Se deberán implementar controles de seguridad que den soporte a todos los sistemas del Poder Judicial de San Juan.

Dichos controles deberán ser los seguidamente detallados:

- Control de vulnerabilidades de la información en los sistemas de oficina, por ejemplo, la grabación de llamadas telefónicas o videoconferencias, la confidencialidad de las llamadas o el acceso al correo electrónico.
- Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo, el uso de boletines electrónicos institucionales.
- Exclusión de categorías de información sensible del Poder Judicial de San Juan si el sistema no brinda un adecuado nivel de protección.
- Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo, aquellas que trabajan en proyectos sensibles.
- La aptitud del sistema para dar soporte a las aplicaciones del Poder Judicial de San Juan, como la comunicación de órdenes o autorizaciones.
- Categorización del personal, contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.
- Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.
- Identificación de la posición o categoría de los usuarios, por ejemplo, empleados del

Poder Judicial de San Juan o contratistas, en directorios accesibles por otros usuarios.

Protección de la Información en servicios de aplicativos

Se tomarán recaudos para la protección de la integridad de la información publicada digitalmente a fin de prevenir la modificación no autorizada que podría dañar la reputación del Poder Judicial de San Juan. Es posible que la información de un sistema de acceso público, por ejemplo, la información en un servidor Web accesible desde Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica. Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación. Todos los sistemas de acceso público deberán prever que:

- La información se obtenga, procese y proporcione de acuerdo con la normativa vigente, en especial la Ley de Protección de Datos Personales.
- La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.
- La información sensible o confidencial sea protegida durante el proceso de recolección y su almacenamiento.
- El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.
- El responsable de la publicación de información en sistemas de acceso público esté claramente identificado.
- La información se publique teniendo en cuenta las normas establecidas al respecto.
- Se garantice la validez y vigencia de la información publicada.

Seguridad en los Procesos de Desarrollo

Desarrollo Seguro de Software

Se deberá establecer una política de requisitos de seguridad para el desarrollo seguro de software aplicable a todo desarrollo de aplicaciones y sistemas de información dentro del Poder Judicial de San Juan, como así también el contratado a terceros.

Se deberá involucrar al Área de Ciberseguridad en el ciclo de vida de desarrollo de los Sistemas de Información desde el inicio con el objeto de validar la arquitectura de seguridad. Los requisitos mínimos que se deberán considerar son los siguientes:

- Validación de datos de entrada (en el cliente y en el servidor).
- Validación de los datos de salida.
- Identificación de usuarios y origen de las conexiones de accesos.
- Control y gestión de errores.
- Registro de actividades realizadas.
- Integridad de las transacciones.
- Cifrado de datos.
- Implementación de controles criptográficos cuando se desee transmitir mensajes con información clasificada.

Además de los detallados, se deberán implementar los siguientes controles :

- Controles de procesamiento interno: Se definirá un procedimiento para que durante la etapa de diseño se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores. Para ello se implementarán:
  - Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
  - Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
  - Procedimientos que establezcan la revisión periódica de los registros de auditoría o alertas de forma de detectar cualquier anomalía en la ejecución de las transacciones.
  - Procedimientos que realicen la validación de los datos generados por el sistema.
  - Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
  - Procedimientos que controlen la integridad de registros y archivos.
  - Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
  - Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

- Controles de validación de datos de salida: Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:
  - Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.
  - Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
  - Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
  - Procedimientos para responder a las pruebas de validación de salidas.
  - Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

- Control de software operativo: Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.
  - Toda aplicación, desarrollada por el Poder Judicial de San Juan o por un tercero

tendrá un único responsable designado formalmente por el responsable de la Dirección de Informática.

- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- La Dirección de Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:
    - Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
    - Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
    - Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
    - Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida

Procedimiento de Control de Cambios

Para el ciclo de vida de desarrollo de software se deberá elaborar el procedimiento de gestión de cambios con el objeto de minimizar los riesgos de alteración de los sistemas de información. Esto garantizará que se cumplan los procedimientos de seguridad y control, respetando la segregación de funciones. Para ello, se deberán tener las siguientes consideraciones:

- Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
- Mantener un registro de los niveles de autorización acordados.
- Solicitar la autorización del Propietario de la Información en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- Efectuar un análisis de riesgo acerca del cambio.
- Determinar los requisitos de seguridad para el cambio.
- Analizar el impacto de los cambios sobre los controles de seguridad existentes.
- Obtener aprobación formal por parte del responsable de la Dirección de Informática para las tareas detalladas, antes que comiencen las tareas.
- Solicitar la revisión del responsable de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
- Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de software.
- Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las

actividades y sin alterar los procesos involucrados.
- Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

Revisión después de cambios en los Sistemas Operativos

Deberán existir procedimientos de revisión y control para asegurar que no se produzca ningún impacto negativo en el funcionamiento o degradación en la seguridad de las aplicaciones y sistemas que contiene cuando se realicen cambios en los Sistemas Operativos por actualizaciones o instalación de componentes.

Restricción del Cambio de Paquetes de Software

Todo cambio en los paquetes de software suministrados por terceros deberá ser controlado de manera estricta. Para ello se deberá:

- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Determinar la conveniencia de que la modificación sea aplicada o no.
- Evaluar el impacto que produciría el cambio.
- Retener una versión del software original realizando los cambios sobre una copia perfectamente identificada.

Principios de Arquitectura de Ingeniería Segura

- Se deberán establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en los sistemas de información.
- Se deberá diseñar contemplando la seguridad en todos los niveles de la arquitectura: operativo, datos, aplicaciones y tecnología, equilibrando la necesidad de seguridad con la de accesibilidad.
- Se deberá analizar la tecnología nueva para conocer sus riesgos de seguridad antes de incluirla como parte del diseño.

Seguridad en los Entornos de Desarrollo

Se deberá implementar controles para proteger adecuadamente los entornos en los que se efectuarán labores de desarrollo e integración de software, abarcando todo el ciclo de vida del desarrollo del sistema y contemplando los recursos humanos, los procesos y las tecnologías asociadas. Dichos controles deberán considerar los siguientes aspectos:

- Segregación entre distintos entornos de desarrollo, según lo señalado en el apartado Separación de entornos de desarrollo, pruebas y producción.
- Seguridad en los datos de prueba y datos en producción que el sistema procesará, almacenará y transmitirá, según los apartados Protección de los Datos de Prueba y Cambios a Datos Operativos.
- Control de acceso al código fuente, según el apartado Control de Acceso al Código Fuente.
- Monitoreo del cambio en el código y en el entorno que lo almacena, de acuerdo con los apartados Procedimiento de Control de Cambios, Revisión después de cambios en los

Sistemas Operativos y Restricción del Cambio de Paquetes de Software.

- Control de los aspectos de seguridad en el desarrollo de sistemas, incluidos en los apartados Principios de Arquitectura de Ingeniería Segura y Evaluación de Vulnerabilidades de Seguridad.
- Seguridad en la externalización asociada al desarrollo de sistemas según las pautas del apartado Tercerización del Desarrollo de Software.
- Copias de respaldo según lo establecido en el apartado Copia de Resguardo y Restauración.

Tercerización del Desarrollo de Software

Se deberán establecer los requerimientos contractuales de calidad y seguridad del código que incluyan auditorías, una revisión del código para detectar código malicioso, como así también el cumplimiento de los requerimientos de desarrollo mencionados en el apartado Desarrollo Seguro de Software.

Se deberán elaborar acuerdos de licencias, propiedad de código y derechos conferidos. Se deberá considerar el establecimiento de acuerdos de custodia del código fuente del software por parte de un tercero en caso de quiebra y/o inhabilidad por parte del proveedor del servicio de desarrollo de software.

Evaluación de Requisitos Funcionales

Se deberá establecer programas de ejecución de pruebas funcionales que permitan evaluar los requisitos funcionales y el cumplimiento de estos en los sistemas desarrollados.

Evaluación de Vulnerabilidades de Seguridad

Se deberá realizar evaluaciones de seguridad en búsqueda de vulnerabilidades sobre los nuevos sistemas a implementar, incluyendo desarrollos propios y de terceros, como también a las plataformas de sistemas operativos sobre los cuales están implementados los mismos, con el objeto de detectar canales encubiertos de transmisión de datos no autorizados o cualquier otra vulnerabilidad que atente contra alguno de sus principios.

Datos de Prueba y Operativos

Protección de los Datos de Prueba

Las pruebas de los sistemas desarrollados podrán efectuarse con datos extraídos del ambiente operativo con autorización previa si los mismos son despersonalizados y enmascarados antes de su uso para evitar exponer información que pueda ser sensible.

Los datos de prueba se deberán eliminar inmediatamente al finalizar las mismas.

Cambios en Datos Operativos

La modificación, actualización o eliminación de los datos operativos deberán ser realizadas sólo a través de los sistemas que procesan dichos datos y de acuerdo con el esquema de control de accesos implementado en los mismos.

Cualquier modificación por fuera de los sistemas a un dato almacenado, ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información. Todos los casos en los que no fuera posible la aplicación de esta política serán considerados como excepciones.

El Área de Ciberseguridad es quien definirá los procedimientos para la gestión de dichas excepciones que deberán contemplar lo siguiente:

- Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.
- El Propietario de la Información afectada y el Área de Ciberseguridad aprobarán la ejecución del cambio, evaluando las razones por las cuales se lo solicita.
- Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
- Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo.
- Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Área de Ciberseguridad.

Política en Relación a los Proveedores

Objetivo

Establecer y mantener el nivel acordado de Seguridad de la Información y prestación de los servicios conforme a los acuerdos establecidos con proveedores.

Seguridad en las Relación con los Proveedores

Seguridad de la Información que es Accedida por los Proveedores

Se deberá documentar y acordar los requisitos de seguridad sobre los activos de información que son accedidos por los proveedores, con el objeto de mitigar los riesgos emergentes al tener acceso a la información y los recursos tecnológicos del Poder Judicial de San Juan.

Se deberán analizar y definir los riesgos en la provisión del servicio para establecer todos los requisitos de seguridad pertinentes. Para ello se deberá definir con cada proveedor, que información podrá acceder, procesar, almacenar o transmitir.

Seguridad dentro de los Acuerdos con Proveedores

Se deberán establecer y documentar los acuerdos para garantizar que no existan discrepancias ni ambigüedades entre el Poder Judicial de San Juan y el proveedor en cuanto a las obligaciones de ambas partes para cumplir con los requisitos de Seguridad de la Información establecidos.

Se deberá identificar e incluir en los Acuerdos de Servicio (SLA), los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios contratados a terceros.

A continuación, se definen los términos para incluir en los acuerdos con el fin de poder satisfacer los requisitos de Seguridad de la Información identificados:

- Descripción de la información que se debe proporcionar o a la que se debe acceder y los métodos para proporcionar o acceder a la información.
- Clasificación de la información de acuerdo con el esquema de clasificación del Poder Judicial de San Juan, y de ser necesario eventualmente, realizando el mapeo entre el esquema propio del Poder Judicial de San Juan y el esquema de clasificación del proveedor.
- Requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y una descripción sobre cómo se garantizará si se cumplen.
- Obligación de cada parte contractual de implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría.
- Reglas de uso aceptable de la información, incluido en uso inaceptable en caso de ser necesario.
- Una lista explícita del personal autorizado para acceder a/o recibir la información o los procedimientos o condiciones del Poder Judicial de San Juan para su autorización, y el retiro de la autorización para el acceso a/o la recepción de la información del Poder Judicial de San Juan al personal del proveedor.
- Políticas de Seguridad de la Información pertinentes al contrato específico.
- Requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes).
- Requisitos de capacitación y concientización para procedimientos específicos y requisitos de Seguridad de la Información, es decir, para la respuesta ante incidentes y procedimientos de autorización.
- Normativas pertinentes para la subcontratación, incluidos los controles que se deben implementar.
- Socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de Seguridad de la Información.
- Requisitos de selección, si existe alguno, para el personal del proveedor para realizar los procedimientos de selección y notificación si no se ha completado la selección o si los resultados dan pie a dudas o inquietudes.
- Derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo.
- Procesos de resolución de defectos y resolución de conflictos.
- Obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe.
- Obligaciones del proveedor para cumplir con el Protocolo de Seguridad Informática y demás requisitos de seguridad del Poder Judicial de San Juan.

Cadena de suministro de la tecnología de información y comunicación

Se deben incluir en los acuerdos con los proveedores los requisitos incluyendo en el proceso los riesgos de Seguridad de la Información asociados con la cadena de suministro de los servicios y

productos de tecnología de información y comunicaciones, abordando en los mismos los siguientes puntos:

- Definición de los requisitos de Seguridad de la Información que regirán la adquisición de tecnologías, productos o servicios de información y comunicación además de los requisitos que en ese mismo sentido apliquen para las relaciones con el proveedor.
- Implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación cumplen con los requisitos de seguridad establecidos.
- Implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando se desarrollan fuera del Poder Judicial de San Juan.
- Obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministros.
- Obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado sin ningún comportamiento inesperado o no deseado.
- Definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema, estableciendo un compromiso entre el Poder Judicial de San Juan y los proveedores.
- Implementación de procesos específicos para administrar el ciclo de vida de los componentes de tecnología de información y comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye los riesgos de los componentes que ya no están disponibles debido a que los proveedores pudieran ya no estar en el negocio o a que ya no proporcionan estos componentes debido a los avances de la tecnología.

Administración de la Prestación de Servicios de Proveedores

Supervisión y Revisión de los Servicios

Se deberá llevar a cabo el seguimiento, control y revisión de los servicios prestados por terceras partes, comprobando que se encuentran adheridos a los términos de Seguridad de la Información con las condiciones definidas en los acuerdos y que los incidentes problemas emergentes en ese sentido, sean manejados en forma apropiada.

Se recomienda que el Poder Judicial de San Juan asegure que se mantenga la visibilidad de las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades, y respuestas de incidentes de seguridad de información a través de un proceso de reportes claro y definido con formato y estructura.

Gestión de Cambios en la Prestación de Servicios

Se deberá administrar la gestión de cambios en la provisión de los servicios, incluyendo el mantenimiento y las mejoras de los procedimientos y controles de Seguridad de la Información existentes.

El proceso de gestión de servicios de terceros deberá tener en cuenta los siguientes procesos en el Poder Judicial de San Juan:

- Actualización de las políticas y procedimientos del Poder Judicial de San Juan
- Actualización de los servicios ofrecidos por el Poder Judicial de San Juan.
- Actualización de aplicaciones o nuevos sistemas.
- Implementación de nuevos controles de la Seguridad de la Información.

El proceso de gestión deberá, también tener en cuenta los siguientes cambios en el servicio ofrecido por el proveedor:

- Cambios y mejoras de las redes.
- Uso de nuevas tecnologías.
- Adopción de nuevos productos o nuevas versiones/publicaciones.
- Nuevas herramientas de desarrollo y ambientes.
- Cambios de las ubicaciones físicas de las instalaciones de servicio.
- Cambios en los proveedores.

Política de Gestión de Incidentes de Seguridad

Objetivo

Garantizar que los eventos de Seguridad de la Información y las debilidades asociados a los sistemas de información sean manejados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Gestión de Incidentes de Seguridad y Mejoras

Responsabilidades y Procedimientos

Se establecerán claramente las responsabilidades y los procedimientos para el manejo de incidentes con el fin de garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a la Seguridad de la Información.

Se deberá contemplar la incorporación en los procedimientos de incidentes de seguridad una definición de las primeras medidas a implementar como ser, identificación, clasificación y análisis de la causa del incidente, la planificación de la solución y recupero de los sistemas afectados, la comunicación formal de las áreas afectadas y la notificación formal al Comité de Seguridad y a la Corte de Justicia de San Juan si fuera necesario.

El Área de Ciberseguridad tendrá la autoridad para acceder a todo equipamiento tecnológico involucrado en alertas de seguridad cuando considere que dicho incidente pudiera afectar la disponibilidad , confidencialidad o integridad de la información o los recursos tecnológicos del Poder Judicial de San Juan.

Notificación de los eventos de Seguridad de la Información

Los incidentes relativos a la seguridad deberán ser comunicados tan pronto como sean detectados mediante el registro de estos en los canales formales siguiendo el procedimiento establecido.

Cuando las áreas usuarias detectasen un incidente de seguridad deberán comunicarlo inmediatamente a el Área de Ciberseguridad, quien procederá a dar respuesta al incidente de seguridad informado.

Se establecerá un procedimiento formal de comunicación y respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el Área de Ciberseguridad de la Información sea informada tan pronto como se haya tomado conocimiento. Esta indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

Asimismo, se comunicará de manera continua al Comité de Seguridad respecto de la ocurrencia de incidentes de seguridad. Todos los empleados, sea cual fuere su situación contractual, deberán conocer fehacientemente el procedimiento de comunicación de incidentes de seguridad, informando los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

Notificación de puntos débiles de la seguridad

Todos los usuarios de los servicios de información del Poder Judicial de San Juan que detectasen fallas o debilidades de seguridad o tomasen conocimiento indirectamente acerca de la existencia de ellas, serán responsables de comunicarlo formalmente al Área de Ciberseguridad.

Está expresamente prohibido que los usuarios ajenos al Área de Ciberseguridad realicen pruebas para detectar y/o explotar supuestas debilidades o fallas de seguridad.

Comunicación de anomalías en el software instalado

Todos los usuarios de los servicios de información del Poder Judicial de San Juan que detectasen anomalías del software en uso deberán comunicarlo formalmente al Área de Ciberseguridad para determinar si la misma califica como un incidente de Seguridad de la Información o no.

Valoración de los eventos de seguridad

Deberá existir un procedimiento de evaluación de los eventos de seguridad que permita decidir si el evento calificará como incidente de seguridad de la información.

Se deberán registrar los resultados de la evaluación y la decisión en detalle con fines de referencia y verificación futuros.

Respuesta a los incidentes de seguridad

Todo incidente de seguridad deberá ser respondido siguiendo los procedimientos establecidos. Dicho procedimiento de respuesta al incidente de seguridad debería incluir:

- Recopilación de evidencias lo más pronto posible, posterior a la ocurrencia del incidente.

- Realización de análisis forenses, en concordancia con el punto 15.1.8 (Recopilación de evidencias).
- Comprobación de que todas las actividades de respuesta se realicen correctamente para el posterior análisis.
- Comunicación de la existencia del incidente, o cualquier detalle pertinente, a todas las personas y áreas con un incumbencia y necesidad de saber.
- Notificar al Comité de Seguridad ante un escalamiento del incidente.
- Cerrar y registrar formalmente el incidente, una vez gestionado correctamente el mismo.

Restablecido el normal funcionamiento y reanudado el nivel de seguridad normal, se deberá realizar un análisis post-incidente, cuando sea necesario, para profundizar el análisis o confirmación del origen del mismo.

Aprendizaje de los incidentes de la seguridad

Se deberán documentar, cuantificar y monitorear los tipos, volúmenes y costos de las anomalías e incidentes de seguridad. Esta información se utilizará para identificar y evaluar aquellos que sean recurrentes o de alto impacto a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros similares.

Recopilación de evidencias

Se deberán definir procedimientos para la identificación, recopilación, adquisición y preservación de la información que pudiera servir como evidencia válida, ya sea para implementar una medida disciplinaria interna o iniciar una acción legal.

Para lograr la validez de la evidencia, el Poder Judicial de San Juan deberá garantizar que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida, como también se deberá asegurar la disponibilidad de los recursos tecnológicos necesarios para la recopilación, adquisición y preservación de evidencia forense.

Para lograr la calidad y totalidad de la evidencia es necesario la solidez de esta, por lo cual se establecen los siguientes requisitos:

- Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.
- Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal, por lo tanto, se deberán tomar todos los recaudos establecidos para la obtención y preservación de la evidencia. Se debe tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas o similar, procedimiento administrativo especial de naturaleza correctiva interna que constituye garantía suficiente para la protección de los derechos y correcto ejercicio de las

responsabilidades impuestas a los agentes públicos. Este reglamento debe ser complementado por lo dispuesto en la Ley N° 19.549 (Ley de Procedimientos Administrativos) y por toda otra normativa aplicable, incluido el Código Penal, el que sanciona a quien sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público (Art. 255).

Política de Gestión de la Continuidad

Objetivos

Minimizar los efectos de las posibles interrupciones de las actividades normales del Poder Judicial de San Juan (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación. Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro. Maximizar la efectividad de las operaciones de contingencia del Poder Judicial de San Juan con el establecimiento de planes que incluyan al menos las siguientes etapas:

- Notificación/Activación: Consistente en la detección y determinación del daño y la activación del plan.
- Reanudación : Consiste en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- Recuperación : Consiste en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal del Poder Judicial de San Juan y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Gestión de Continuidad de las Operaciones

Proceso de Administración de los Planes de Continuidad

Deberá existir un plan de contingencia, para actuar ante la interrupción de la continuidad de las operaciones en el Poder Judicial de San Juan, a fin de garantizar que los planes operativos de restauración de las operaciones sean ordenados y consistentes entre sí. El proceso de administración de la continuidad de la operatoria deberá tener en cuenta:

- Identificar y priorizar los procesos críticos de las actividades del Poder Judicial de San Juan.
- Asegurar que todos los integrantes del Poder Judicial de San Juan comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Poder Judicial de San Juan.
- Elaborar y documentar una estrategia de continuidad de las actividades del Poder Judicial de San Juan consecuente con los objetivos y prioridades acordados.

- Proponer planes de continuidad de las actividades del Poder Judicial de San Juan de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Poder Judicial de San Juan.
- Proponer las modificaciones que se consideren necesarias a dichos planes.

Continuidad de las actividades y análisis de impacto

Al establecer un Plan de Continuidad de las Actividades del Poder Judicial de San Juan, se deberán contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación, incendio, desastres naturales, destrucción edilicia, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos y el establecimiento de las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo: sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de respaldo de información, registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y por el Área de Ciberseguridad, considerando todos los procesos de las actividades del Poder Judicial de San Juan y no limitándose a las instalaciones de procesamiento de la información. Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Poder Judicial de San Juan. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad a la máxima autoridad del Poder Judicial de San Juan para su aprobación.

Elaboración e implementación de los planes de continuidad de las actividades del Poder Judicial de San Juan

Los propietarios de procesos y recursos de información, con la asistencia del Área de Ciberseguridad, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del Poder Judicial de San Juan.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

- Identificar y acordar respecto a todas las funciones y procedimientos de emergencia
- Analizar los posibles escenarios de contingencia y definir las acciones correctivas a

implementar en cada caso.

- Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
- Documentar los procedimientos y procesos acordados.
- Instruir adecuadamente al personal en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
- Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:
    - Objetivo del plan.
    - Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
    - Procedimientos de divulgación.
    - Requisitos de la seguridad.
    - Procesos específicos para el personal involucrado.
    - Responsabilidades individuales.
- Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades requeridas del Poder Judicial de San Juan, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

Marco para la Planificación de la Continuidad de las Actividades del Poder Judicial de San Juan

Se mantendrá un solo marco para los planes de continuidad de las actividades del Poder Judicial de San Juan, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo.

Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes. El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo. Estas modificaciones deben ser propuestas por el Comité de Seguridad para su aprobación.

El marco para la planificación de la continuidad de las actividades del Poder Judicial de San Juan tendrá en cuenta los siguientes puntos:

- Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en

marcha los mismos.

- Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Poder Judicial de San Juan y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
- Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Poder Judicial de San Juan o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.
- Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Poder Judicial de San Juan.
- Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.
- Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.
- Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

Se deberán definir explícitamente los administradores de los planes de contingencia. El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan.

Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Poder Judicial de San Juan

Debido a que los planes de continuidad de las actividades del Poder Judicial de San Juan pueden fallar por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- El Comité de Seguridad establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quiénes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deben utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

- Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación de las actividades utilizando ejemplos de interrupciones).
- Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
- Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
- Realizar ensayos completos probando que el Poder Judicial de San Juan, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas del Poder Judicial de San Juan se tomarán en cuenta, además, los siguientes mecanismos:

- Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del Poder Judicial de San Juan en paralelo, con operaciones de recuperación fuera del sitio principal).
- Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).

Todas las pruebas efectuadas deben ser documentadas, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos. Los planes de continuidad de las actividades del Poder Judicial de San Juan serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios del Poder Judicial de San Juan para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades. Se deberá definir la periodicidad de revisión de los planes de contingencia es la siguiente, indicando el nombre del plan de contingencia, responsable y periodicidad de revisión. Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades del Poder Judicial de San Juan aún no reflejadas en dichos planes. Debe prestarse atención, especialmente, a los cambios de:

- Personal.
- Direcciones o números telefónicos.
- Estrategia del Poder Judicial de San Juan.
- Ubicación, instalaciones y recursos.
- Legislación.
- Contratistas, proveedores y clientes críticos.
- Procesos, o procesos nuevos / eliminados.
- Tecnologías.
- Requisitos operacionales.
- Requisitos de seguridad.
- Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
- Requerimientos de los sitios alternativos.
- Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad para su aprobación por el superior jerárquico que corresponda. Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

Redundancia

Redundancia en las Instalaciones de Procesamiento y Transmisión de la Información

Se deberá implementar en las instalaciones de procesamiento y transmisión de la información, componentes y/o arquitecturas redundantes, a efectos de cumplir con los requisitos de disponibilidad operativa.

Política de Cumplimiento

Objetivos

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Poder Judicial de San Juan y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con las políticas, normas y procedimientos de seguridad del Poder Judicial de San Juan. Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Poder Judicial de San Juan.

Cumplimiento de Requisitos Legales

Identificación de la Legislación Aplicable

Se deberán identificar y documentar en los sistemas de información del Poder Judicial de San Juan los requisitos normativos, contractuales o legales. Del mismo modo se deberá definir y documentar los controles específicos, las responsabilidades y funciones individuales para cumplir con dichos requisitos.

Derechos de Propiedad Intelectual

Se deberá garantizar el cumplimiento de los requisitos legales y contractuales relacionados con la instalación y uso de software protegido por la legislación relativa a la propiedad intelectual.

Los empleados podrán utilizar únicamente material autorizado por el Poder Judicial de San Juan.

El Poder Judicial de San Juan sólo podrá autorizar el uso de material producido por el mismo o material autorizado o suministrado por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones que podrían iniciar sumarios administrativos internos, hasta acciones legales que podrían derivar en demandas penales, por infracción a la Ley de Propiedad Intelectual N° 11.723, ya que el software es considerado una obra intelectual que goza de la protección de dicha ley.

Los usuarios solo podrán utilizar software autorizado por el Poder Judicial de San Juan según las condiciones de instalación descritas en el apartado Restricciones en la instalación de software.

Protección de los Registros del Poder Judicial de San Juan

Los registros de datos se deberán proteger contra pérdida, destrucción, acceso no autorizado, publicación no autorizada, degradación del medio de almacenamiento, obsolescencia del formato o medio de almacenamiento.

Los registros de datos, correspondientes a las cuentas de correos electrónicos no deberán ser eliminados cuando el propietario de dicha cuenta fuera desvinculado del Poder Judicial de San Juan, sino que deberán ser almacenados por un período mínimo de diez años.

Los sistemas de almacenamiento de datos deberán ser seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera aceptable ante requerimiento de un Tribunal de Justicia.

Se deberán clasificar y detallar los períodos de retención, medios de almacenamiento y responsables de su mantenimiento. Los sistemas de almacenamiento y manipulación deberán garantizar una clara identificación de los registros y de su período de retención legal o normativa. La protección de los datos deberá ser garantizada por el documento "Acuerdo de Confidencialidad".

Asimismo, los funcionarios o empleados que revelen a terceros o utilicen en provecho propio cualquier información individual de carácter estadístico o censal de la cual tengan conocimiento por sus funciones, o que incurran dolosamente en tergiversación, omisión o adulteración de datos de los censos o estadísticas, serán pasibles a acciones penales por infracción a la Ley 17.622.

Protección de Datos y Privacidad de la Información Personal

A través del presente "Protocolo de Seguridad Informática" y de el "Protocolo de Uso de Recursos Informáticos y Telecomunicaciones" se informarán y detallarán las actividades que serán objeto de control y monitoreo, a fin de no violar el derecho a la privacidad del empleado.

Todos los empleados deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

El Poder Judicial de San Juan poseerá un "Acuerdo de Confidencialidad", el cual deberá ser suscrito por todos los funcionarios públicos y contratistas, en concordancia con el apartado Acuerdo de confidencialidad.

Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Toda utilización de los recursos de procesamiento de información, con propósitos no autorizados o ajenos al destino por el cual fueron provistos se considerará como uso indebido.

Todos los empleados deberán conocer el alcance preciso del uso adecuado de los recursos informáticos y deberán respetarlo, según se declara en el Protocolo de Uso de Recursos Informáticos y Telecomunicaciones.

En particular, se deberá respetar lo dispuesto por las siguientes normas:

- Ética en el Ejercicio de la Función Pública. Ley 25.188: Establece que las personas que se desempeñen en la función pública deben proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- Código de Ética de la Función Pública: Dispone que el funcionario público debe proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.
- Código Penal Art. 255: Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
- Decisión Administrativa 43/96: Reglamenta el Art. 30 de la Ley 24.624. Determina su ámbito de aplicación, define conceptos y precisa los requisitos de carácter general, los relacionados con los documentos en particular y con el soporte a utilizar en la redacción, producción o reproducción de aquellos.
- Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo las compilaciones de datos o de otros materiales.
- Ley N° 25.506: Establece que la exigencia legal de conservar documentos, registros o datos también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.
- Código Penal: Sanciona a quien alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183).

Delitos Informáticos

Todos los empleados deberán conocer la existencia de la Ley 26.388 de Delitos Informáticos, la cual, a partir de su promulgación, castiga penalmente ciertas conductas cometidas mediante

medios informáticos.

Cabe señalar que la mayoría de las conductas descritas por dicha norma vinculada ya han sido señaladas en los apartados precedentes.

Revisiones de Cumplimiento de Seguridad

Revisión independiente de la Seguridad de la Información

Deberán efectuarse revisiones independientes de seguridad, para garantizar la eficacia de la implementación de seguridad existente. Esta revisión será independiente al Área de Ciberseguridad y permitirá incluir oportunidades de mejora en los objetivos de control y cambios en el enfoque de seguridad existente. Dicha revisión deberá ser realizada por individuos independientes al Área de Ciberseguridad, por ejemplo, Auditoría Interna o especialistas de seguridad externos al Poder Judicial de San Juan.

Cumplimiento del Protocolo y Procedimientos de Seguridad

Los responsables de cada Dirección, dentro de su área de responsabilidad, deberán velar por el correcto cumplimiento de las normas y procedimientos de seguridad establecidos y brindarán apoyo a las revisiones de cumplimiento, efectuadas por el Área de Ciberseguridad.

El Área de Ciberseguridad tendrá la autoridad de realizar revisiones periódicas en todas las áreas del Poder Judicial de San Juan a efectos de garantizar el cumplimiento de las políticas, normas y procedimientos de seguridad vigentes.

Verificación de Cumplimiento en los Sistemas de Información

Se verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, incluyendo la revisión de los sistemas en producción, a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones pueden contemplar asistencia técnica especializada. El resultado de la evaluación se volcará en un informe técnico para su posterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico. La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema. Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión del Área de Ciberseguridad.