PODER JUDICIAL
REPUBLICA DE CHILE









POLÍTICA

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

DE LA CORPORACIÓN ADMINISTRATIVA

DEL PODER JUDICIAL

Aprobado por Consejo Superior en sesión de 28 de Marzo de 2019, Acta Nº 687.

PODER JUDICIAL
REPUBLICA DE CHILE

ÍNDICE

1. INTRODUCCION 3
   1.1 Conceptos principales: 3
   1.2 Conceptos complementarios: 3
2. OBJETIVO 5
3. ALCANCE 6
4. ROLES 7
   4.1 Rol General. 7
   4.2 Roles Específicos. 7
   4.3 Otros Roles sobre los Activos de la Información. 8
5. NORMATIVAS Y PROCEDIMIENTOS EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. 9
6. MANTENIMIENTO Y DIFUSIÓN DE LAS NORMATIVAS DE SEGURIDAD DE LA INFORMACIÓN. 10
7. INCUMPLIMIENTOS. 10
8. APROBACIÓN Y ACTUALIZACIÓN 11
9. VIGENCIA 11
10. DIVULGACIÓN 11

1. INTRODUCCION

La presente Política de Seguridad de la Información de la Corporación Administrativa del Poder Judicial (en adelante CAPJ), en cuanto al buen uso de los recursos tecnológicos, así como el cuidado de la información, para resguardar la disponibilidad, confidencialidad e integridad de los datos de la Institución, propendiendo a generar una disminución en el riesgo sobre los activos de la información de la institución.

1.1 Conceptos principales:

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener confidencialidad, disponibilidad e integridad de la misma.

Las directrices de seguridad de la información son:

Disponibilidad: Resguardar que los usuarios autorizados tengan acceso a la información en forma oportuna.

Integridad: Mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Confidencialidad: Asegurar que la información sea conocida sólo por quienes estén debidamente autorizados.

1.2 Conceptos complementarios:

Riesgo: Posibilidad de que una amenaza pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Impacto: Es la consecuencia de la materialización de una amenaza.

Control: Medio para mitigar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales.

Riesgo inherente: Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan en la organización.

Riesgo residual: El nivel de riesgo restante después de aplicado el control.

Activos de información: Se entiende cualquier componente (sea humano, tecnológico, software, información en papel, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio.

Evento de seguridad de la información: Una ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. Ejemplos de eventos: usuarios que se conecta a un sistema, un intento fallido de un usuario para ingresar a una aplicación, un dispositivo de seguridad que permite o bloquea un acceso, una notificación de cambio de contraseña de un usuario privilegiado. Se debe destacar que un Evento de Seguridad de la Información, no es necesariamente una ocurrencia maliciosa o adversa.

Incidente de seguridad de la Información: Es indicado por un único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información en algunas de sus tres directrices confidencialidad, disponibilidad e integridad. Ejemplos de incidentes: Accesos no autorizado, robo de contraseñas, utilizar fallas en los procesos de autenticación para obtener accesos indebidos, robo de información, abusar y/o mal usar los servicios informáticos internos o externos de una organización, introducir código malicioso en la infraestructura tecnológica (virus, troyanos, gusanos, malware en general), denegar el servicio o eventos que ocasionen pérdidas, tiempos de respuesta no aceptables o no cumplimiento de Acuerdos de Niveles de Servicio existentes de determinado servicio.

Sistema de Gestión de Seguridad de la Información (SGSI): Un SGSI es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar la seguridad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información. Como todo proceso de gestión, un SGSI debe ser eficiente en el transcurso del tiempo adaptándose a los cambios internos y externos de la organización.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas (papel), y no solo en medios digitales.

La información puede ser divulgada, mal utilizada, robada, borrada o saboteada; atentando su disponibilidad, integridad y confidencialidad.

La información es clasificada por la Corporación Administrativa del Poder Judicial como:

Secreta: Información con la que se soportan los servicios críticos de la organización y que al ser conocida por entes no autorizados, pondrían en riesgo la operación del servicio. Ejemplo de esto es el uso de contraseñas en los sistemas.

Reservada: Información que puede ser conocidas solo por algunos entes de la organización, con uso restringido de sus acceso.

Interna: Información de carácter interna para la operación del servicio de la Institución.

Pública: Toda Información que no ha sido clasificada con alguna de la tres clasificaciones anteriores.

2. OBJETIVO

La Política de Seguridad de la Información, constituye una declaración de la postura, tanto, de la Dirección y del Consejo Superior de la Corporación Administrativa del Poder Judicial, con relación a la Seguridad de la Información.

La Corporación Administrativa del Poder Judicial considera que la protección de sus activos, y con ello la continuidad del servicio, deben ser gestionados y administrados.

Como objetivo de esta política se pretenden describir los parámetros de acción con relación a la seguridad de la información y proveer un marco de referencia para que:

Las instalaciones y activos de información se encuentren adecuadamente protegidas.

La información refleje el resultado de aplicar procesos autorizados sobre datos oficiales.

Sólo personas autorizadas ejecuten o intervengan, en los procesos de información automáticos.

Se ejecuten transacciones legítimas, por personas autorizadas y a través de procesos establecidos.

Se realiza un proceso de revisión y mejora en el ambiente de la seguridad de la información.

La pérdida o degradación de un activo de información puede tener para la Institución consecuencias tales como:

- Pérdida de continuidad de los servicios.
- Daño a la imagen institucional.
- Incumplimiento de las metas institucionales.
- Infracción a la normativa interna o leyes vigentes.

3. ALCANCE

Esta Política es de obligado cumplimiento para todos los funcionarios de la Corporación Administrativa del Poder Judicial, incorporando tanto a proveedores externos que prestan servicios, como a las instituciones en convenio.

Asimismo, constituye una responsabilidad de la Corporación Administrativa del Poder Judicial, resguardar los datos de los ciudadanos, entidades u organizaciones, que han sido utilizados en los procesos judiciales de las distintas competencias.

El alcance de esta política, cubre todo tipo de información independiente del medio en que se encuentre almacenada y establece que:

La Información es un bien valioso y un recurso imprescindible para la gestión y operación de la Corporación Administrativa del Poder Judicial.

La información es clasificada de acuerdo a criterios de valoración en relación a la importancia que posee para la Corporación Administrativa del Poder Judicial.

Las directrices de la Política de Seguridad de la Información de la Corporación Administrativa del Poder Judicial, han sido definidas de acuerdo con el estándar ISO/IEC 27002 que establece un marco de referencia de seguridad respaldado y reconocido internacionalmente. Este marco regulatorio, organizativo y procedimental de seguridad se soportará en un conjunto de manuales de procedimientos, reglamentos, estándares, instructivos y herramientas de seguridad para la protección de activos de información.

4. ROLES

4.1 Rol General

La seguridad de la información es responsabilidad de todos los funcionarios, proveedores y otras entidades relacionadas que tengan acceso a ella (digital o impresa), ya sea que la registren, procesen, almacenen o tomen conocimiento. Debiendo tener siempre presente en el ejercicio de sus labores, las medidas necesarias que aseguren la adecuada protección de la información y de los activos de información a los que tenga acceso o de los cuales sea responsable.

4.2 Roles Específicos

Se establece una función específica de protección de la información, mediante la asignación de responsabilidades y funciones para los distintos roles que mitigaran el riesgo de seguridad e la información en la Institución.

Dicha infraestructura organizativa estará liderada por el Director de la Corporación Administrativa del PJUD, que supervisará la gestión efectiva y eficiente de los riesgos e incidentes de seguridad y coordinará a los diferentes Departamentos y Unidades pertenecientes a la Institución.

Director: tendrá por responsabilidad general gestionar la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) que velará por la protección de la información, mediante la asignación de responsabilidades específicas en materia de definición, utilidad, uso y reporte de los controles de seguridad, por una parte, y de la implantación, operación y gestión de los mismos, por otra.

Oficial de Seguridad de la Información: es responsable de gestionar las políticas, normas, estándares y procedimientos de Seguridad de la Información de la Corporación Administrativa del Poder Judicial, además de apoyar la implementación de controles de seguridad de la información para mejorar el cumplimiento de la organización, con respecto a la seguridad de la información y la continuidad del servicio.

4.3 Otros Roles sobre los Activos de la Información

4.3.1 Propietario de la información

El propietario de la información es el dueño del proceso que utiliza o genera dicha información y debe autorizar el acceso a esta, la designación de los dueños de la información, es realizada por la Comisión de Seguridad de la Información.

4.3.2 Usuarios de la información

El usuario de la información, es aquella persona, funcionario o proveedor, que con la debida autorización introduce, borra, cambia o lee información de la Institución. El propietario puede ser también usuario y por tanto estar sujeto a las mismas responsabilidades que éste.

Los usuarios sólo deben tener acceso a la información a la que están autorizados para ver o procesar, por tanto, a las autorizaciones que se otorguen deben limitar su capacidad, de forma que no puedan realizar actividades distintas de aquellas para las que se otorgó el permiso.

4.3.3 Custodios de la información

Se denominan custodios de la información, al funcionario, departamento o proveedor, que recibe la responsabilidad de materializar las definiciones y disposiciones realizadas por el propietario de la información. Normalmente, los custodios no necesitan la información para la realización de su trabajo, sino sólo se limitan a procesarla, gestionar su almacenamiento y hacerla accesible.

El Departamento de Informática y Computación es el principal custodio de la información existente en soporte informático. En los casos de información que se gestione en forma de papel o digital, que no esté afecta a la gestión del Departamento de Informática y Computación, será responsable de su custodia cada área propietaria de la misma.

4.3.4 Personal externo a la CAPJ

La política de externalización de servicios que la Corporación Administrativa del Poder Judicial emita, debe incluir las cláusulas correspondientes por la que los proveedores de servicios se obligan a cumplir los requerimientos de la Política de Seguridad de la Información, normativas, estándares y procedimientos de la Institución. De esta forma, cualquier incumplimiento por su parte en este sentido, deberá permitir al amparo del contrato, tomar las medidas legales que se consideren oportunas. Esto se aplicará en el dominio Seguridad en las Relaciones con los Proveedores, el cual contendrá normativas y manuales de procedimientos que velarán por la correcta ejecución de los controles de seguridad definidos.

4.3.5 Departamento de Informática y Computación.

El Departamento de Informática y Computación, es responsable de velar por la seguridad física y lógica de las instalaciones en donde se localice el procesamiento centralizado de la información, y contar con las herramientas, sistemas y procedimientos que garanticen que tanto las instalaciones, los aplicativos como los archivos de datos tengan la protección adecuada que permita mantener razonablemente la integridad, confidencialidad y disponibilidad de los datos de la organización y sus usuarios.

5. NORMATIVAS Y PROCEDIMIENTOS EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La Política de Seguridad de la Información1, contendrá varios anexos, tales como normativas y procedimientos que complementarán este documento:

- Seguridad en la Administración de Activos
- Seguridad en los Recursos Humanos
- Seguridad Física y Ambiental de las instalaciones de procesamiento de la información (Datacenter) y en las instalaciones de la Institución
- Seguridad de Operaciones Tecnológicas
- Seguridad en las Telecomunicaciones
- Control de Acceso a los Sistemas
- Seguridad en la Adquisición, Desarrollo y Mantención de Sistemas
- Respuesta a Incidentes de Seguridad de la Información
- Gestión de Continuidad de Servicio
- Seguridad en las Relaciones con los Proveedores
- Seguridad en el Cumplimiento Legal e Interno

Se ejecutará la difusión del marco regulatorio, comunicando a los funcionarios y proveedores, en un contexto de educación y capacitación, con el objetivo que sea conocido y aplicado por todos los usuarios dentro del ámbito de aplicación del presente documento.

[1] Estas normativas y procedimientos se agrupan según los controles de la norma NCh ISO 27001:2013 vigente en nuestro país.

6. MANTENIMIENTO Y DIFUSIÓN DE LAS NORMATIVAS DE SEGURIDAD DE LA INFORMACIÓN.

Se establece un grupo de Políticas, Normativas, Estándares y Procedimientos de Seguridad de la Información, cuya responsabilidad de creación, revisión periódica, adecuación y alineamiento de su contenido con los planes estratégicos de la Corporación Administrativa del Poder Judicial, recae sobre el Oficial de Seguridad de la Información de la Corporación Administrativa del Poder Judicial.

La revisión formal de la presente Política se efectúa al menos una vez cada dos años. Adicionalmente se deben considerar los cambios que se produzcan en la normativa nacional vigente, la inclusión de resultados relevantes de auditorías o análisis de riesgos y las sugerencias de mejora al marco regulatorio.

El proceso de difusión de la siguiente política y sus normativas asociadas se realizarán a través de la publicación en los medios de comunicación, que han sido definidos por la Comisión de Seguridad de la Información de la Corporación Administrativa del Poder Judicial.

7. INCUMPLIMIENTOS.

En caso de no cumplimiento de la presente Política de Seguridad de la Información y todas las normativas y manuales de procedimientos asociados, será reportado al Director, por parte del Oficial de Seguridad de la Información, para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario.

8. APROBACIÓN Y ACTUALIZACIÓN

La presente Política de Gestión de Seguridad de la información, fue aprobada por el Consejo Superior en su sesión del 28 / Marzo / 2019.

Las actualizaciones deberán consignarse en el cuadro de control de cambios, al inicio de este documento y deberán ser aprobadas por el Consejo Superior.

9. VIGENCIA

La presente Política rige a contar del 28 / Marzo / 2019, tendrá duración indefinida.

10. DIVULGACIÓN

La versión actualizada de la presente Política de Gestión de Seguridad de la Información, debe ser publicada y mantenida en la correspondiente dirección de la página de intranet de laCAPJ.