Política General de Seguridad de la Información y Protección de Datos Personales

Comité Ejecutivo Nacional

29 de septiembre de 2021

Primera Parte

SEGURIDAD DE LA INFORMACIÓN

Glosario

Activos de información[1]: Los activos los podemos separar en dos grandes grupos: tangibles e intangibles. Los activos tangibles son aquellos activos materiales que contienen información, y sobre los que tomaremos medidas preventivas para protegerlos principalmente de riesgos físicos: golpes, agua, fuego, etc. Los activos intangibles son aquellos que soportan la información dentro de un activo material, y pueden inutilizar la información, pese a que el activo físico no haya sufrido daño alguno. Por ejemplo: Un listado de personal (información) puede estar incluido en una hoja Excel (activo intangible), que se encuentra en un ordenador de sobremesa (activo tangible).

Agencia de Protección de Datos de los Habitantes (PRODHAB): órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz denominado Agencia de Protección de Datos de los habitantes.

Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable. Se puede encontrar en formato digital o no digital, cualquier que sea la forma o modalidad de su creación, registro, almacenamiento, organización y acceso.

Base de datos interna, personal o doméstica: Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales públicos o privados, mantenidos por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos.

Consentimiento informado: Poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles datos proporcionar a un tercero.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Datos de acceso irrestricto: Son aquellos contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

Datos de acceso restringido: Los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

Encargado del tratamiento: Persona física que, sola o conjuntamente con otras, trate datos personales por cuenta del responsable del tratamiento, como consecuencia de la existencia de una relación jurídica que le vincula

[1] Basado en la norma ISO 27001, 2017

con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Gestión de medios removibles. Usos y permisos que tienen los usuarios y/o funcionarios de la organización respecto del uso de los medios removibles.

Ley de Protección de la persona frente al tratamiento de sus datos personales: Ley No. 8969 del 5 de septiembre de 2011, que regula el tratamiento de los datos personales en Costa Rica.

Medios removibles: Se comprenderá como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de las computadoras. Ejemplo: llave maya.

Política: Declaración de alto nivel que describe la posición de la organización sobre un tema específico.

Principio de autodeterminación informativa: Conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales. Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias.

Principio de minimización de los datos: Los datos solicitados al titular deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Procedimiento: Tratamiento o método que define específicamente como se van a implementar distintas herramientas.

Protocolo de actuación: Documento que establece los pasos que se deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en la ley n° 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales.

Receptor: Cualquier tercero autorizado para recibir datos transferidos por cuenta de un responsable o encargado del tratamiento de los mismos.

Responsable del tratamiento: El responsable del tratamiento es la persona jurídica, que decide sobre el tratamiento de los datos personales, determinando los fines y los medios de dicho tratamiento.

Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de la organización.

Seguridad de la información[2]: Es el conjunto de medidas preventivas y

[2] Diaz, Matias (25 de julio de 2019). «Mapa de riesgos de una empresa». *TU ECONOMÍA FÁCIL*. Consultado el 25 de julio de 2019.

reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos. 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, y no solo en medios informáticos.

Terceros: Personas que tengan relación con el Partido, por ejemplo: proveedores.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Transferencia: Comunicación de la información o los datos personales a un receptor, que a su vez es responsable del tratamiento de los datos.

1. Objetivo

El objetivo de esta Política es proporcionar una visión general de los requisitos de seguridad del Partido Acción Ciudadana y describir los controles en el lugar o los previstos para cumplir esos requisitos. Esta política pretende también delinear las responsabilidades y el comportamientos esperados de todas las personas que realizan tratamiento de información con el fin de mantener un entorno controlado, minimizando los mismos hasta niveles aceptables.

2. Principios

I. El Partido Acción Ciudadana protegerá la información creada, procesada, transmitida o resguardada a partir de sus procesos políticos, con el fin de minimizar impactos operativos o legales debido a un uso inadecuado de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

II. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los colaboradores y terceros que hagan dicho tratamiento.

III. El Partido Acción Ciudadana implementará control de acceso a la información, sistemas y recursos de red.

IV. El Partido Acción Ciudadana garantizará una mejora efectiva de su modelo de seguridad, a través de una adecuada gestión de los incidentes de seguridad y las debilidades asociadas con los sistemas de información.

3. Alcances

La política de seguridad de la información y protección de datos personales será de acatamiento obligatorio para todas las personas que trabajan para el

Partido Acción Ciudadana. En concordancia con lo estipulado en el artículo 31 del Estatuto Orgánico del Partido, su alcance incluye a: a. La Comisión Política, b. La Comisión de Finanzas, c. El Tribunal de Ética, d. El Tribunal de Alzada del Tribunal de Ética, e. Tribunal Electoral Interno (TEI), f. La Fiscalía de Equidad de Género, g. La Comisión de Estudios y Programas, h. La Comisión de Capacitación y Formación Ciudadana, i. La Comisión de Reglamentos y Regulación Interna, j. La Comisión Nacional de las Mujeres, k. El Congreso Ciudadano., además de otras estructuras formales, voluntariado y terceros.

4. Deber de cumplimiento

Todas las personas señaladas por el alcance y aplicabilidad deberán dar cumplimiento pleno de la política. El incumplimiento a la política de Seguridad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa interna del Partido, así como lo establecido en las normas de carácter nacional, como lo es la ley 8968 Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, normas complementarias y conexas.

En caso de incumplimiento que pueda generar alguna vulneración o riesgo de seguridad, el CEN deberá informar a la Agencia de Protección de Datos de los Habitantes de acuerdo al procedimiento que se indica más adelante.

5. Organización de la seguridad de la información

I. Conformación del Comité Directivo de Seguridad de la Información

Estará conformado por la Secretaría General, la Dirección Ejecutiva y la persona encargada de Tecnologías de la Información.

II. Objetivos: Los objetivos del Comité son:

1. Elaborar propuestas de modificación y actualización permanente de la política de la seguridad de la información y protección de datos.
2. Establecer criterios para el procedimiento de análisis de riesgos y vulnerabilidades.
3. Proponer al CEN aprobar procedimientos para garantizar la seguridad de la información.
4. Promover recursos y medios para la concienciación y capacitación del personal en materia de seguridad de la información y protección de datos personales.
5. Velar por el cumplimiento de la política de la seguridad de la información y protección de datos personales.
6. Supervisar avances de los proyectos y de las iniciativas y acciones de mejora de la seguridad requeridas.
7. Revisar la información aportada en relación a los incidentes de seguridad.

8. Participar en la toma de decisiones que garanticen la seguridad de la información y los servicios

III. Administración:

La administración de la seguridad de la información del Partido Acción Ciudadana, corre a cargo de la dirección ejecutiva, o en su defecto la Secretaría General quien tiene la responsabilidad de promover la seguridad de la información organizacional mediante la emisión de lineamientos específicos.

La persona encargada de Tecnologías de la Información, es responsable del cumplimiento de las normativas aplicables a la seguridad de la información de la organización. Es responsable además de asegurar la alineación operativa de TIC a la normativa aplicable en materia de seguridad de la información. Esta persona debe asegurarse de que los contratos de prestación de servicios TIC, cuenten con cláusulas que promuevan el cumplimiento de esta política y la Política de Protección de Datos Personales.

Todos los colaboradores en general que presten sus servicios al Partido Acción Ciudadana, son responsables de conocer y cumplir las disposiciones de esta Política que les corresponda.

6. Gestión de activos

I. Acceso a redes inalámbricas: Podrán tener acceso a las redes inalámbricas del Partido, mediante el uso de celulares, computadoras, tablets, y demás dispositivos electrónicos, los colaboradores directos, así como miembros de los órganos e instancias oficiales del Partido. De igual manera tendrá acceso la militancia por medio de la red configurada como “invitados”.

II. Equipos de la organización: Es responsabilidad del personal, proteger los equipos que se le han asignado para el desempeño de sus funciones siguiendo las medidas de seguridad que a continuación se describen, como mínimo:

A. No exponer el equipo a condiciones de inseguridad física y/o ambiental.

B. Utilizar claves de acceso seguras y proteger las que le han sido asignadas.

C. No dejar el equipo desatendido en lugares donde pueda ser sustraído o dañado con relativa facilidad, como autos, maletas de viaje, cerca de ventanas, en el piso, mesas de comida o bebida, etc (aplica solo si se tienen portátiles).

D. La persona encargada de Tecnologías de Información y Comunicaciones, en su ámbito, debe asegurar que todos los equipos móviles que el Partido Acción Ciudadana asigne al personal para el cumplimiento de sus funciones, cuenten con las herramientas necesarias para propiciar la seguridad de la información. Estas herramientas, incluyen, en forma enunciativa, más no limitativa: antivirus, software de cifrado, aplicaciones seguras, entre otras.

E. Todo equipo que almacene, procese o transmita información esencial para la operación del Partido Acción Ciudadana, debe ser protegido para disminuir el riesgo de amenazas ambientales o físicas; tales como, inundaciones, rayos, sismos, terremotos, radiaciones, polvo, humedad, vandalismo, explosión, humo, entre otras. Se debe contar con un centro de datos primario, que garantice la protección de los equipos que soportan los procesos de la organización, así como, los servicios de soporte.

III. Gestión de medios removibles

Usos y permisos que tienen los usuarios y/o funcionarios de la Organización frente a los medios removibles: Se autoriza el uso de medios removibles cuando sea estrictamente necesarios para el traslado de información de un activo a otro. Este procedimiento deberá ser autorizado por la Dirección Ejecutiva en los supuestos que se considere necesario. Las personas a las que se otorgue autorización para el uso de dicho medio de almacenamiento, serán responsables del adecuado manejo y tratamiento de la información.

IV. Control de acceso con usuario y contraseña

Se debe elaborar un lineamiento sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la organización, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas. El lineamiento debe enunciar las responsabilidades que los colaboradores y terceros tienen al contar con un usuario o contraseña de la organización, se debe estipular que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La organización debe establecer que por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña segura para el acceso.

V. Gestión de Contraseñas

Esto implica definir lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la organización. Se debe indicar a los colaboradores, terceros y contratistas, los parámetros mínimos para que una contraseña sea considerada como segura. Se debe determinar que los accesos a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña

fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.

VI. Devolución de activos

Todo personal que preste sus servicios al Partido Acción Ciudadana, al concluir sus funciones, tiene la obligación de entregar los activos informáticos asignados en buen estado físico y de operación, así como los activos de información y la documentación correspondiente.

Con respecto a la entrega de la cuenta de correo electrónico creada por el Partido, la persona tiene la obligación de transferir el usuario y contraseña una vez que deje de trabajar para la organización y se le otorgará un recibido conforme.

Toda devolución deberá ser dirigida a la persona Encargada de Tecnologías de la Información que es quien controla el inventario.

VII. Información para la autenticación

Cada colaborador del Partido Acción Ciudadana es responsable de su contraseña, la cual es confidencial y debe mantenerse secreta. Para hacer uso de la infraestructura tecnológica del Partido Acción Ciudadana, los usuarios deben aceptar los términos y condiciones de la Política. Solo deben tener acceso a los aplicativos del Partido, los usuarios autorizados, con la cuenta asignada para tal efecto; en ningún caso deben acceder usando una cuenta diferente. La administración de los derechos de acceso a los aplicativos, directorio activo y bases de datos internas, se realiza mediante roles y/o perfiles. Todos los usuarios con acceso a los aplicativos internos deben identificarse en forma única y contar con los derechos de acceso asignados previamente, de acuerdo a su rol y perfil.

VIII. Control de acceso a las redes y servicios asociados

A. Los controles de acceso a los servicios de información, deben asignarse con base en los roles y perfiles de los usuarios, según el servicio requerido.
B. La autentificación de usuarios, debe hacerse a través de canales cifrados y haciendo uso de contraseñas encriptadas.
C. Todos los accesos a servicios TIC y aplicativos deben ser asignados de acuerdo a su función, mediante roles y perfiles, propiciando una correcta segregación de funciones.

IX. Entrada y salida de equipos de cómputo

Se debe establecer un procedimiento para el registro de entrada y salida de equipos de cómputo. Todo equipo que almacene, procese, transmita

información crítica del Partido Acción Ciudadana debe operar dentro de las instalaciones del Partido o de las empresas contratadas para tal efecto.

La persona encargada de Tecnologías de Información y Comunicaciones debe establecer un procedimiento que asegure que la información y/o configuraciones no queden expuestas.

Los equipos que por necesidad salgan de las instalaciones, sean propias o arrendadas, deben apegarse al procedimiento de salida de equipos que se elaborará. Los equipos de cómputo móviles (laptops) deben ser protegidos con las medidas y mecanismos de seguridad de la información, con los que cuente el Partido.

X. Equipo informático de usuario desatendido

La persona encargada de Tecnologías de Información, debe implementar en todo equipo informático las configuraciones necesarias para su bloqueo de forma automática en un tiempo máximo de 5 minutos, una vez que éste se encuentre desatendido.

XI. Acuerdo de confidencialidad:

Debe contener un compromiso o acuerdo de confidencialidad, por medio del cual todo colaborador, contratista y/o tercero vinculado a la Organización, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Organización, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo colaborador, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

XII. Gestión de suministro de servicios del proveedor

La Organización debe periódicamente supervisar la provisión de los servicios que ofrecen los terceros. Los proveedores tienen la obligación de entregar a la Organización, oportunamente, la evidencia digital necesaria *en caso de incidentes de seguridad o aquella que les sea requerida*. Los proveedores de servicios de correo electrónico tienen la obligación de entregar al Partido la totalidad de los correos electrónicos y bitácoras, así como, de no conservar información alguna mediante borrado seguro, al término del contrato.

XIII. Gestión de incidentes en la seguridad de la información

Se deben establecer lineamientos mínimos para gestionar los incidentes de seguridad de la información. Para ello el Comité de Seguridad de la Información generará una guía técnica de atención a incidentes. El equipo de respuesta será designado por el mismo Comité de Seguridad de la Información y debe estar capacitado para el uso de las herramientas adquiridas por el Partido Acción Ciudadana para el análisis y la respuesta a

incidentes, trabajará en corresponsabilidad con las áreas afectadas e involucradas en la operación. El equipo designado debe conocer los procedimientos de respuesta a incidentes y tomar en cuenta como mínimo las siguientes etapas:

A. Identificación y reporte.
B. Contención.
C. Recuperación.
D. Solución.
E. Lecciones aprendidas

Además, se deberá tomar en consideración lo estipulado en los artículos 38 y 39 del Reglamento a la Ley 8968, en relación a incidentes de vulnerabilidad de seguridad.

El responsable deberá informar al titular y a la Agencia, en caso de vulnerabilidades de seguridad, al menos lo siguiente:

a) La naturaleza del incidente;

b) Los datos personales comprometidos;

c) Las acciones correctivas realizadas de forma inmediata; y,

d) Los medios o el lugar, donde puede obtener más información al respecto.

Segunda Parte

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

I. Objetivo

Esta política de protección de datos personales tiene por objeto establecer el modo en que se obtienen, se tratan y protegen los datos personales que recolecta el Partido Acción Ciudadana a través de la firma de la boleta de afiliación, y mediante otros procesos organizativos, para que las personas puedan decidir libre y voluntariamente como desean que estos datos sean tratados de acuerdo con el principio de autodeterminación informativa regulado en la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales.

II. Denominación del responsable y encargado del tratamiento de los datos

- *Denominación del responsable superior:* Comité Ejecutivo Nacional del Partido Acción Ciudadana.
- *Denominación del Encargado*: El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste, además de cualquier órgano receptor según lo dispuesto en el Mecanismo de Transferencia de Datos del Partido Acción Ciudadana.
-

III. Finalidades del tratamiento para las cuales se obtienen los datos personales

El Partido Acción Ciudadana compromete a su personal y equipo colaborador a mantener confidencialidad respecto de dicha información. Los datos personales que se ingresen por medio de boletas de afiliación u algún otro formulario de contacto, no serán difundidos, distribuidos o comercializados.

IV. Obtención de datos personales

Los datos se obtendrán a través de la boleta de pre-afiliación, instrumento que las personas suscriben de manera informada, libre y voluntaria, y mediante otros procesos organizativos. Todo lo anterior de acuerdo a la Política de Afiliación del Partido Acción Ciudadana.

V. Uso de los Datos Personales

El PAC utilizará datos personales para los siguientes fines:

1. Para identificar a las personas afiliadas al Partido Acción Ciudadana.
2. Para gestionar las solicitudes de afiliación presentadas mediante plataformas virtuales.
3. Para conocer quiénes son las personas que ocupan cargos en los órganos y las estructuras nacionales, provinciales, cantonales y distritales, dentro del Partido Acción Ciudadana.
4. Para conocer quiénes son las personas que ocupan o han ocupado puestos o cargos de elección popular en los territorios y estructuras nacionales.
5. Para generar convocatorias oficiales de acuerdo a los procesos que disponen las normas generales del país y los estatutos del Partido.
6. Para remitir invitaciones a talleres, capacitaciones y eventos de formación política.
7. Para remitir comunicados y reglamentos oficiales del partido.
8. Para identificar a las personas que realizan o han realizado aportes económicos al Partido.
9. Para generar padrones para las Asambleas Cantonales o Distritales.
10. Para definir la antigüedad de militancia de los afiliados.
11. Para conocer a sus afiliados y organizar procesos partidarios.

VI. Seguridad en el tratamiento de los datos

En el Partido Acción Ciudadanaa deberá tratar los datos personales con absoluta confidencialidad y se garantiza el deber de mantenerlos adoptando todas las medidas necesarias que eviten su alteración, pérdida, tratamiento o acceso no autorizado, en atención con las obligaciones legales que nos aplican como responsables del tratamiento de sus datos personales.

VII. Sobre la conservación de los datos personales

Los datos personales se conservarán durante el tiempo en que se mantenga la afiliación al Partido Acción Ciudadana. Después de su desafiliación, el PAC podrá conservar el dato del periodo en que una persona estuvo afiliada y el motivo de su desafiliación.

VIII. Mecanismos y medios disponibles para que el titular pueda ejercer sus Derechos ARCO (Acceso, Rectificación, Complementación y Oposición)

En el Partido Acción Ciudadana se están implementando elevados estándares de seguridad exigidos por la legislación costarricense para proteger los datos de carácter personal frente a pérdidas, accesos fortuitos, tratamientos no autorizados, entre otros incidentes relacionados al uso de las tecnologías de la información.

A partir de la información recabada mediante el formulario de consentimiento informado, el Partido Acción Ciudadana podrá ponerse en contacto vía correo electrónico, SMS, mensajería electrónica o cualquier otro medio de comunicación electrónica equivalente, para remitirle comunicaciones oficiales de acuerdo con la finalidad para la cual fueron recabados los datos de sus titulares.

Si en un determinado momento la persona no desea recibir comunicaciones de esta naturaleza, rectificar sus datos o ejercer su derecho de acceso, podrá revocar su consentimiento mediante el envío del formulario que se encuentra publicado en el sitio web, y deberá remitirlo firmado y escaneado o con la debida firma digital a la siguiente dirección: accionciudadana@pac.cr. La revocatoria del consentimiento informado, no implica desafiliación al Partido Acción Ciudadana, toda vez que son figuras distintas con procedimientos distintos

XIV. Capacitación y sensibilización en seguridad de la información y protección de datos personales

El Partido deberá poner en marcha un programa de formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano. Dicho programa debe contener los siguientes parámetros:

A. El compromiso del Comité Ejecutivo Nacional en destinar recursos suficientes en la medida de sus posibilidades, para desarrollar las jornadas de capacitación en la materia.
B. Hacer un plan de quiénes deberán ser entrenados/sensibilizados.
C. Definir los roles y responsabilidades de quienes diseñarán los programa, quienes los comunicarán.
D. La obligación de los colaboradores a asistir a los eventos o cursos de capacitación.
E. Revisión periódica de resultados de capacitaciones para el mejoramiento de los procesos.

F. Compromisos y obligaciones por parte del personal capacitados.

XV. Responsabilidades legales

En caso de que la persona encargada del tratamiento de los datos personales contravenga lo dispuesto en la presente política de Seguridad de la Información y Protección de Datos Personas, incurriendo con ello en un indebido tratamiento de la información, se expone a las sanciones y penas de carácter administrativo y penal contempladas en la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales y a la legislación penal vigente respectivamente.

Aprobado en sesión del CEN, 29 de septiembre del 2021.