Empresa de Servicios Públicos de Cajicá S.A. E.S.P.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EMPRESA DE SERVICIOS PÚBLICOS DE CAJICÁ SA ESP

VIGENCIA 2025-2027

Actualizado 2024

Profesional Universitario Sistemas

Contenido

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P. tiene en cuenta la información como el activos más importantes de la entidad, además que la infraestructura informática está conformada por hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la empresa, este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así confrontar contingencias y desastres de diversos tipos. Como también tiene el propósito de salvaguardar la información generada dentro de la empresa, garantizando así la seguridad de los datos y dando cumplimiento a la normatividad legal vigente, para poder realizar un Plan de Seguridad y Privacidad de la información con el fin de que no se presenten robos, perdidas de información, accesos no autorizados y duplicación de información que puedan ocasionar daños a los usuarios tanto internos como externos.
La EPC cumple con tres pilares de seguridad de la información dando prioridad en preservar la integridad, confidencialidad y disponibilidad de la información como esencia de los servicios que provee:

- Disponibilidad: Dar capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran.
- Confidencialidad: Es un principio fundamental de la seguridad de la información que garantiza el necesario nivel de secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito.
- Integridad: Garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.

2. OBJETIVO

Establecer lineamientos para la implementación de políticas de seguridad de la información, que garanticen la administración, tratamiento, manejo y control de la seguridad y privacidad de la información de la Empresa de servicios Públicos de Cajicá S.A. E.S.P.

3. OBJETIVOS ESPECÍFICOS

- Implementar políticas y procedimientos enfocados en la de seguridad de la información.
- Mitigar los riesgos asociados a la seguridad de la Información que afecten la integridad, confidencialidad, disponibilidad y privacidad de la Información de la Empresa.
- Definir y formalizar los documentos normativos sobre temas de protección de la información.
- Mitigar el riesgo digital de forma eficiente, eficaz y efectiva para salvaguardar la seguridad y privacidad de la información.
- Generar un cambio organizacional a través de la apropiación de la información y seguridad digital.

4. ALCANCE DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

El plan de Seguridad y Privacidad de la información de EPC, tiene como alcance los recursos, procesos, procedimientos y demás actividades relacionadas, incluyendo a los funcionarios, contratistas y demás partes interesadas que usen los activos de información generados dentro de la empresa.

5. TÉRMINOS Y DEFINICIONES

La normatividad aplicable en Colombia, se implementa los siguientes términos:

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y obligados. (Ley 1712 de 2014, art 4)
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de total.
- Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)

- Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000)
- Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).
- Partes interesadas: Se refieren a individuos o grupos que tienen interés o se ven afectados por la recopilación, gestión, procesamiento, intercambio o uso de datos e información digitales.
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC27000).
- Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de gobierno digital la correlativa obligación.
- Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- Riesgo: Posibilidad de que una amenaza concreta 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. (ISO/IEC 27000).
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Vulnerabilidad: Cualquier debilidad que pudiera explotarse con el fin de violar un sistema o de la información que contiene".

Como también se tiene en cuenta el siguiente marco normativo:

Ley 527/99 “Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos”

Ley 1266/08 “Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países”.

Ley 1581/12 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.”

Decreto 1499 del 11 de septiembre de 2017 “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015”

Decreto 612 del 04 de abril de 2018 “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.”

Decreto 1008 del 14 de junio de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2

del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones."

6. PRINCIPIOS GENERALES DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En la Empresa de servicios Públicos de Cajicá S.A. E.S.P., es importante generar políticas de la Seguridad de la Información, para brindar orientación y soporte por parte de la alta dirección y así, dar cumplimiento con los requisitos, normatividad vigente y demás reglamentarios pertinentes.

Los funcionarios y contratistas de EPC, deben asumir las responsabilidades y roles asignados de la seguridad de la información antes, durante y terminando con su empleo o actividades asignadas por la alta dirección y/o supervisor de contrato.

La Integridad de la información de EPC, debe preservar siempre su autenticidad, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones, ni alteraciones por parte de terceros.

La Disponibilidad de la Información de EPC, debe estar disponible cuando sea requerida por cualquier parte interesada.

La confidencialidad de la información de EPC, debe garantizar que la información personal, será protegida y no será divulgada sin consentimiento alguno.

La privacidad de la Información de EPC, debe estar preservada con el fin de que sea utilizada, para los propósitos que fue generada.

7. RESPONSABLES

La EPC, tiene como responsables de la implementación, seguimiento y mantenimiento del Plan de Seguridad y Privacidad de la información:

1. El representante de la Alta dirección de EPC, quien velara por el cumplimiento del Plan de Seguridad y Privacidad de la Información, mediate sus directores y directoras.
2. Encargados de la gestión de TI, serán los encargados de desarrollar la implementación del Plan de Seguridad y Privacidad de la Información.
3. Todos los funcionarios y/o contratistas y demás partes interesadas de EPC, son responsables del Plan de Seguridad y Privacidad de la Información y en caso de no cumplir, se reserva el derecho de tomar las medidas correspondientes según el caso.

4. La divulgación de este plan se dará a conocer a través del personal a cargo del proceso TI mediante la socialización a todos los funcionarios, contratista y partes interesadas de EPC, quien dará a conocer la existencia, contenido y obligatoriedad de dicho documento.
5. La custodia y ubicación física del documento estará a cargo del Sistema Integrado de Gestión y el líder de TI.

8. POLÍTICAS

La EPC, divulga los objetivos y alcances de la seguridad de la información, con el fin de mantener, gestionar y mitigar el riesgo como se estable en el Plan de Tratamiento de Riesgos, garantizando así la continuidad de los servicios y disminuyendo la probabilidad de amenazas que puedan afectar los procesos internos para el cumplimiento de las metas de la Entidad.

8.1. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Cada proceso, bajo supervisión y con base en el inventario de activos de la EPC, siempre debe estar actualizando e incorporado de acuerdo a la clasificación, valoración, ubicación y acceso de la información y demás características identificas por la gerencia, garantizando la disponibilidad, integridad y confidencialidad de dicha información.

8.2. SEGURIDAD DE LA INFORMACIÓN

Todas y todos los servidores públicos de la EPC, independiente del tipo de vinculación laboral o contractual, o de los procesos al que pertenezca y del nivel de funciones o actividades que desempeñe, deben contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. Por ende, se debe contar con un directorio completo y actualizado de los perfiles creados.
La responsabilidad de custodia de cualquier documento o archivo generado dentro de la empresa, usado o producido por algún funcionario y/o contratista que se retira, o cambia de cargo, recae en la dependencia o supervisor del contrato, aclarando que el proceso de cadena de custodia de la información debe hacer parte integral de un procedimiento de terminación de la relación contractual o de cambio de cargo.

8.3. USUARIO INVITADO Y SERVICIOS DE ACCESO PÚBLICO.

El acceso a la red de usuarios no registrados solo debe estar autorizado por la Gerencia, de manera de información institucional. Igualmente, el servicio de internet al que pueden acceder, debe estar protegido con una contraseña, contando con una restricción de sitios web no autorizados. Si los usuarios invitados no realizaron el debido proceso de registro, no se permitirá el acceso a cualquier otro tipo de recursos de información, aplicación y/o herramientas TIC.

8.4. SEGURIDAD FÍSICA Y DEL ENTORNO

La EPC cuenta con una edificación de dos niveles los cuales se ajustarán a la red de datos mediante los siguientes mecanismos:

- Seguridad en los equipos: Los servidores o equipos de cómputo que contengan información institucional debe estar en un ambiente seguro y protegido por lo menos con:
    - Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).
    - Toda la información institucional en formato digital, debe ser mantenida en los servidores internos de la Empresa y/o unidades extraíbles aprobados por la alta gerencia y los responsables de la TI.
    - Se debe asegurar que la infraestructura esté cubierta, con mantenimiento y soporte adecuado, tanto para el hardware y software.
- Las estaciones de trabajo deben ser operadas por funcionarios de la institución, los cuales deben estar capacitados sobre el contenido de la política de seguridad y privacidad de la información y de las responsabilidades personales en el uso y administración de la información institucional.

- Se deben incluir los medios que alojan copias de seguridad conservados de forma correcta, de acuerdo a las políticas y estándares establecidos.

8.5. ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES

El personal vinculado a la EPC, debe realizar el reporte de manera eficiente y con responsabilidad de las presuntas violaciones de seguridad detectadas y se deben reportar a los responsables del proceso TI y/o a través de los directores o directoras.

Los procedimientos escritos para la operación de dichas actividades no afectaran el desarrollo normal de la prestación del servicio y asegurando la confiabilidad de la información.

8.6. PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING.

Se debe proteger todos los sistemas de información que involucre los controles humanos, físicos, técnicos y administrativos para no incurrir en daños.

Se elaborará y mantendrá un conjunto de políticas, normas, estándares y procedimientos que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking que pueda afectar la prestación del servicio.
Como control básico, todas las estaciones de trabajo de EPC, deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus, adicional a esto se limitará el acceso a paginas o descargas que no sean requeridas para el cumplimiento de las funciones de cada empleado o contratista.

8.7. COPIAS DE SEGURIDAD

Toda información que se encuentre contenida en el inventario de activos de información o que sea de interés para un proceso, siempre debe estar respaldada con copias de seguridad tomadas de acuerdo a los procedimientos documentados y probados por el Sistema de Gestión de Calidad.

El procedimiento debe incluir actividades de almacenamiento, administración y custodia de las copias de seguridad incluyendo lugares seguros y control de registros de dichas copias. Dentro del procedimiento debe quedar claro, que se debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Se debe tener en cuenta que la creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales, debe ser protegida por el dueño del activo de la información de la entidad.

8.8. INTERCAMBIO DE INFORMACIÓN CON ENTIDADES EXTERNAS.

Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por la gerencia, y ser redireccionados a los responsables del manejo y custodia dicha información. Se debe tener en cuenta que la información solicitada por parte de los entes externos debe ser realizada por un medio valido que permita el registro de la solicitud, donde se pueda identificar el remitente, el asunto y la fecha, aclarando que toda información institucional debe ser manejada de acuerdo a la normatividad legal vigente.

8.9. INSTALACIÓN DE SOFTWARE

Todas las instalaciones de software fuera de los establecidos por la empresa que se realicen sobre el sistema operativo, debe ser aprobada por la Gerencia y posteriormente informado al responsable de la gestión de las TI, de acuerdo a los procedimientos establecidos para tal fin.
El funcionario encargado en la Gestión de las TI, debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad, además debe tener un inventario del software autorizado para su uso institucional.

8.10. CONTROL DE CLAVES Y NOMBRES DE USUARIO

Las claves de administrador de los diferentes sistemas deben ser conservadas por el encargado de la gestión de las TI y deben ser cambiadas periódicamente.
Adicionalmente se debe elaborar, mantener y actualizar las actividades de cambio de las claves de usuario de acuerdo al seguimiento de incidentes.

Una vez se termine la relación contractual o laboral del personal con la EPC, se debe cambiar los accesos a este.

8.11. USO ADECUADO DE INTERNET

La EPC, es consciente de la importancia del servicio de Internet como una herramienta fundamental para el desempeño de los procesos que proporcionará los recursos necesarios para asegurar su disponibilidad a los servidores públicos y demás partes de interés que así lo requieran. Lo cual implica:

- El encargado de las TI debe gestionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- El encargado de las TI debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- El encargado de las TI debe monitorear continuamente el canal o canales del servicio de Internet.
- El encargado de TI debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

8.12. PROYECCIÓN DE PRESUPUESTO

La Dirección Administrativa, encargada de la Tecnología e Información tiene asignado un presupuesto para la vigencia 2025, cuya ejecución presupuestal es monitoreada de manera periódica de acuerdo con el Plan Anual de Adquisiciones.

NOTA: El Plan de Seguridad y Privacidad de la Información para la vigencia 2025, se aprobó por Comité Institucional de Gestión y Desempeño realizado el 20 de diciembre de 2024 mediante el acta número 05 de 2024.