POLÍTICA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

No. PÁGINA:	FECHA:	VERSIÓN:
17	18/12/2019	1

Preparado por:	Revisado por:	Aprobado por:
Director de tecnología informática y de comunicaciones	Gerente administrativo	Presidente

CONTROL DE CAMBIOS

FECHA	MOTIVO DE CAMBIO	VERSIÓN
18/12/2019	Estandarización del documento.	1

CONTENIDO

POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

TERMOBARRANQUILA S.A. ESP (en adelante y para efectos de esta política se identificará como TEBSA), en cumplimiento del deber de seguridad respecto de la infraestructura crítica y activos de información, adopta y declara la siguiente Política de Seguridad de la Información y Ciberseguridad.

1. Considerandos

a. Que la finalidad de este documento es establecer los parámetros generales que en materia de seguridad de la información y ciberseguridad tendrá presente esta organización para gestionar las redes y sistemas de información que soportan sus procesos empresariales.

b. Que esta organización en su operación tiene como objeto la prestación de un servicio público como es la generación de energía la cual soporta el sistema eléctrico nacional de la República de Colombia.

c. Que la actividad empresarial que en materia de servicios públicos desarrolla esta organización determina que intervenga en la prestación de un servicio público esencial, entendiendo por este aquel servicio necesario para el mantenimiento de las necesidades básicas de la población, cuya no disponibilidad tiene el riesgo de generar efectos nocivos para la ciudadania y por tanto para la seguridad nacional.

d. Que la prestación de un servicio público esencial, como es el caso de la generación de energía, hace que la operación empresarial de esta organización sea considerada una infraestructura crítica para el Estado, lo que determina un serio compromiso por parte de todas las personas que laboran y/o prestan servicios a esta organización, considerando en cada caso, la relación de estos con las redes, sistemas de información, tecnologías de operación y tecnologías de información y comunicaciones que intervengan en la prestación del mencionado servicio público esencial.

e. Que en esta organización se consideran como infraestructura crítica vinculada la generación de energía los siguientes activos: instalaciones físicas, redes, sistemas de información, equipos físicos, dispositivos electrónicos, tecnologías de operación, servicios soportados en tecnologías de información y comunicaciones, entre otros, que intervinen en la generación de energía y/o soportan el funcionamiento del servicio público que presta esta organización.

f. Que dentro de los activos vinculados a la infraestructura crítica que tiene esta organización existen ciertas zonas críticas que merecen la adopción y gestión de una seguridad más rigurosa como son aquellas en las cuales se controla la generación de energía y la conexión con el sistema elécrico nacional.

g. Que esta organización en virtud de la importancia que tiene su actividad en el sistema eléctrico nacional entiende el deber que tiene de proteger, gestionar y fortalecer la seguridad de la infraestructura crítica que administra y para ello desplegará estrategias y acciones orientadas a asegurar la funcionalidad, continuidad e integridad del servicio público de generación de energía con el fin de prevenir, mitigar y neutralizar posibles ataques y/o daños causados por ataques intencionales o no contra la infraestructura que soporta la operación de la infraestructura crítica.

h. Que esta organización es consciente del incremento, magnitud, frecuencia y gravedad de los incidentes de seguridad que tienen como objetivo las infraestructuras críticas que soportan los servicios esenciales que presta el Estado y particulares autorizados por la ley; en este sentido, se requiere desarrollar capacidades en el personal que gestiona la prestación del servicio público de generación de energía con el fin de garantizar de forma incremental la seguridad en los activos que hacen parte de la infraestructrura crítica gestionada por esta organización.

i. Que esta organización identificará y mantendrá actualizado el inventario de activos que hacen parte de la infraestructura crítica que soporta la prestación del servicio público de generación de energía, siguiendo para ello no solo los parámetros que establezca la ley, sino también las buenas prácticas en materia de seguridad de la información y ciberseguridad.

j. Que además del inventario de activos que hacen parte de la infraestructura crítica mencionada es indispensable identificar y gestionar riesgos de seguridad en la relación con aquellos proveedores que intervienen de forma directa en la prestación del servicio público de generación de energía; esto sin perjuicio de la necesidad de gestionar los riesgos con otros proveedores que intervengan en menor escala en la prestación del mencionado servicio público.

k. Que un aspecto de manifiesta importancia en la estrategia de seguridad de la información y la ciberseguridad en esta organización es la adecuada identificación y gestión de incidentes de seguridad que puedan afectar la integridad, disponibilidad, confidencialidad y estabilidad de la infraestructura crítica gestionada de forma directa y/o através de terceros proveedores de esta organización.

l. Que las buenas prácticas en materia de seguridad y ciberseguridad destacan la relevancia que tiene la formación, capacitación y entrenamiento en materia de seguridad de la información, ciberseguridad y gestión de incidentes de seguridad que

puedan y/o lleguen a comprometer no solo los activos de información que gestiona esta organización sino también la infraestructura crítica que soporta la prestación del servicio público de generación de energia que presta la organización.

m. Que esta organización tendrá presente en la relación con los proveedores que participen de forma directa en la gestión de los activos bajo su gestión, sean parte o no de la infraestructura crítica, los riesgos de diferente naturaleza que puedan emerger de los servicios de computación en la nube en relación con la seguridad de la información, ciberseguridad y prestación del servicio público de generación de energía, considerando el entorno geopolítico, la seguridad y defensa nacional y el interés general de la población colombiana.

n. Que los objetivos de seguridad de la información y ciberseguridad que adopte esta organización serán logrados en la medida que exista un fuerte relacionamiento con los grupos de interés que permitan, a partir de una temprana notificación de un evento y/o incidente de seguridad de la información y/o ciberseguridad realizar una debida gestión de tales incidentes notificar, de ser necesario, a las partes interesadas.

o. Que esta organización en la medida que hace parte del sistema eléctrico nacional entiende la necesidad de mantener comunicación permanente con los demás agentes que hacen parte de este sistema que también gestiona infraestructura crítica, y en particular con las autoridades colombianas que intervienen en la gestión de riesgos cibernéticos, ciberseguridad y ciberdefensa. Lo anterior, sin perjuicio de otras autoridades y/o terceros que se consideren necesarios para la protección de la infraestructura crítica administrada por esta organización.

p. Que esta organización entiende que la adopción de esta política de seguridad debe aplicarse de forma armónica y sistémica con las disposiciones legales aplicables en materia de seguridad de la información, ciberseguridad y derechos consagrados en la Constitución Política de la República de Colombia.

q. Que mediante esta política se pretende fortalecer de forma más robusta e integral las prácticas de seguridad de la información existentes en la organización que han sido desplegadas de forma razonable y diligente por la Dirección de Tecnología Informática y de Comunicaciones (TIC).

r. Que estos considerandos tienen como finalidad expresar los objetivos generales que persigue esta organización con la adopción de esta Política y servir como criterio de interpretación de tales objetivos.

s. Que esta Política será desarrollada a través de normas normas, procedimientos y/o instructivos, los cuales serán objeto de revisión y mejoramiento permanente, acorde con los requisitos de seguridad de esta organización y dinámica de los objetivos estratégicos que a nivel nacional se establezcan en materia de seguridad de la información y ciberseguridad considerando no solo la importancia de la infraestructura crítica

gestionada, sino también la relevante importancia que tienen los datos, la información y los conocimientos como activos creadores de valor en el economía digital.

2. Objetivo

El objetivo o propósito de esta Política de Seguridad de la Información y Ciberseguridad aplicable tanto a los activos que hacen parte de la infraestructura crítica que gestiona esta organización así como a los demás activos de información en su poder y/o bajo su custodia, incluidos los datos personales, es declarar que tales activos, conforme su variada naturaleza son objeto de protección y gestión segura por parte de esta organización en virtud de la importancia que revisten para la prestación del servicio público de generación de energia y de la creación de valor que tienen para TEBSA; razón por la cual, de acuerdo con los objetivos estratégicos y requisitos del negocio, se adoptará un esquema sistemático de gestión segura basado en riesgos con el fin de preservar los atributos de Integridad, Confidencialidad y Disponibilidad para fortalecer la confianza con sus grupos de interés, incluido el Estado Colombiano considerando el carácter de infraestructura crítica que tiene esta organización.

3. Destinatarios

Esta Política aplica a las relaciones que tiene esta organización con sus grupos de interés; a saber:

- Accionistas
- Junta Directiva
- Empleados
- Prestadores de Servicios
- Proveedores
- Clientes
- Comunidad
- Autoridades

4. Ámbito de Aplicación

Esta Política de Seguridad de la Información y ciberseguridad será criterio rector de carácter obligatorio aplicable por los empleados en los diferentes procesos empresariales que soportan la ejecución del objeto social, así como en el relacionamiento con los grupos de interés.

Igualmente será exigible en las relaciones estatutarias, contractuales y/o legales con terceros, accionistas, proveedores, clientes, y/o autoridades; sin perjuicio de lo aplicable a otros destinatarios de esta política.

5. Enfoque

Acorde a la naturaleza de esta organización como prestador del servicio público de generación de energía, el cumplimiento de los requisitos legales, estatutarios y contractuales constituye una fuente de riesgos en relación con el cumplimiento de las obligaciones de diversa naturaleza; los cuales adquieren mayor relevancia cuando un porcentaje muy alto de la operación y prestación de los servicios de la organización están soportados en Tecnologías de Operaciones (TO) y Tecnologías de Información y de Comunicaciones (TIC), lo que incrementa de forma importante los riesgos para la organización y el Estado colombiano en relación con el logro de los objetivos estratégicos, los cuales incluyen la protección de activos que hacen parte de la infraestructura crítica, así como respecto de los activos de información como datos, información, conocimiento y derechos en poder de esta organización.

Esta realidad no sólo es predicable de esta organización, sino que constituye una preocupación a nivel público y privado presente también a nivel internacional; lo que ha determinado la expedición a nivel mundial de normas legales y de industria orientadas a proteger a las personas y organizaciones respecto de los riesgos cibernéticos originados en la presencia incremental de las TIC en la vida social, máxime en el caso de esta organización cuya infraestructura crítica soporta la prestación de un servicio público esencial como es la generación de energia y su relevancia en el sistema eléctrico nacional.

A nivel público el Estado Colombiano, con acento en el interés general de la población, ha establecido objetivos y lineamientos en materia de seguridad de la información, ciberdefensa, ciberseguridad y seguridad digital que impactan la operación de esta organización en virtud del servicio público prestado y su rol en el sistema eléctrico nacional.

Desde otra dimensión, el régimen de protección de datos personales vigente en Colombia incorpora el principio de Responsabilidad Demostrada[1] mediante el cual se exige la adopción de un programa integral de protección de datos personales basado en riesgos. Este programa integral de protección de datos personales, gradualmente irá siendo extendido en esta organización a otros activos de información como datos, información, conocimiento y derechos no relacionados con datos personales.

Desde las orillas antes mencionadas, sin perjuicio de otras que sean relevantes en materia de seguridad de la información y ciberseguridad, es necesario que esta organización adopte un esquema de riesgos respecto de la prestación del servicio público de generación de energía, asi como en relación con los demás servicios que soportan su operación empresarial, considerando la naturaleza de los diferentes activos y amenazas que recaen sobre estos.

El enfoque de riesgos aplicable a la gestión de la seguridad de la información y ciberseguridad, cualquiera que sean los activos, comprende los cuatro (4) momentos fundamentales de todo sistema de gestión, como son:

Planear: Esta etapa comprende la identificación de los activos vinculados a la infraestructura crítica y/o demás activos, entiéndase datos personales o no, información, conocimientos y/o derechos que representen un valor estratégico para la organización en relación con los objetivos

[1] Superintendencia de Industria y Comercio. Guía para la implementación del principio de responsabilidad demostrada. Recuperado de http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf.

estratégicos de esta y los respectivos servicios que presta la organización a terceros, para así identificar los riesgos en relación con el cumplimiento de las obligaciones legales, estatutaria y contractuales teniendo como referencia la normatividad legal y las normas de industria o buenas prácticas aplicables según el caso. A partir de estos establecer los objetivos de control, controles y análisis sobre la declaración de aplicabilidad.

Hacer: En esta etapa, previa identificación de los riesgos y definición de la declaración de aplicabilidad, se desplegarán los planes de acción orientados a prevenir, mitigar, eliminar y/o aceptar el riesgo, previo análisis y justificación de las razones por las cuales se asume este. En el plan de acción para gestionar los riesgos se determinará el responsable de la gestión, acciones a desplegar, los controles, los recursos asignados de acuerdo con su impacto y probabilidad, métricas, sin perjuicios de demás aspectos relevantes para la gestión de los riesgos vinculados.

Verificar: En esta etapa se evaluará el resultado de la gestión de la seguridad de la información y ciberseguridad respecto de los activos que hacen parte de la infraestructura crítica y demás activos de información, sean datos personales o no, aplicando para ello técnicas de auditoría razonables que permitan identificar debilidades en la gestión, recomendaciones y nuevos riesgos, para así fortalecer la seguridad de la información y ciberseguridad en la organización.

Actuar: En esta etapa a partir de los hallazgos y recomendaciones se realizarán actualizará el plan de acción para gestionar los riesgos identificados respecto de los activos que gestiona esta organización vinculados a la seguridad de la información y ciberseguridad en esta organización.

Dentro del esquema de seguridad de la información cobra relevancia considerar como aspectos de importancia los siguientes:

Documentación: Es importante en términos de evaluar la debida diligencia de la Alta Dirección y demás empleados responsables[2] de la gestión segura de la información la documentación y conservación de las evidencias físicas y/o electrónicas que permitan establecer que la organización ha cumplido y gestionado de forma eficaz la infraestructura crítica y demás activos de información como datos personales o no, información, conocimientos y/o derechos.
Comunicación: Para la gestión segura de los activos de información es un elemento fundamental la comunicación interna y externa con el fin de crear, promover, mantener y fortalecer la cultura de seguridad respecto de los activos de la infraestructura crítica y activos de información en poder y/o bajo custodia de la organización.

Educación y formación: El logro del objetivo de crear una cultura de seguridad de la información y ciberseguridad alrededor de la infraestructura crítica y demás activos de información en poder y/o bajo custodia de la organización exige que la formación considere la dimensión de los riesgos que a nivel personal pueda experimentar cada empleado y/o prestador de servicios para construir al interior de la organización una cultura colectiva de seguridad de la información, ciberseguridad, protección de datos personales y cumplimiento.

6. Compromiso de la Alta Dirección

[2] Organización de Estándares Internacionales. (2013). Anexo A Dominio 6.1 Organización Interna de la seguridad de la información. Sistemas de Gestión de Seguridad de la Información. [ISO 27001 de 2013].

El régimen de responsabilidad de los administradores societarios consagrado en la Ley 222 de 1995 enuncia un conjunto deberes a cargo de estos dentro de los cuales se destacan en su artículo 23 los siguientes: (i) Realizar los esfuerzos conducentes al adecuado desarrollo del objeto social: (ii) Velar por el estricto cumplimiento de las disposiciones legales o estatutarias y (iii) Guardar y proteger la reserva comercial e industrial de la sociedad. Estos deberes son de destacada importancia cuando la operación empresarial implica la gestión de la seguridad de la información, la prestación de un servicio público esencial, la gestión segura de una infraestructura crítica, y la relevancia de la debida diligencia cuando la operación empresarial esta vinculada de forma directa a la seguridad, defensa nacional y estrategia de ciberseguridad adoptada por el Estado Colombiano.

De forma particular, el régimen colombiano de protección de datos personales en Colombia incorpora el principio de seguridad y el principio de responsabilidad demostrada, sin perjuicio de los demás principios establecidos en la ley y la jurisprudencia. Este régimen establece una serie de obligaciones legales en materia de seguridad de la información aplicable a datos personales, disposiciones que en virtud de la visión holística en materia de seguridad y ciberseguridad se pueden extender a los activos que hacen parte de la infraestructura crítica y demás activos de información gestionados por esta organización, máxime cuando su operación principal en la prestación de un servicio público como es la generación de energía.

Estos deberes se replican en las buenas practicas en la materia que regula esta política como es el estándar de industria ISO 27002:2015 sobre gestión segura de la información la cual señala como parte de ese deber la definición de una política que guía la gestión segura de la información basada en riesgo, la que habrá de incorporar los requisitos de cumplimiento y articular estos con el logro de los objetivos estratégicos trazados por la organización.

7. Rendición de Informes.

Un componente fundamental en la seguridad de la información es propender por un proceso de comunicación efectivo que permita mantener informada a la Alta Dirección. En este orden de ideas, desde la Dirección de Tecnología Informática y de Comunicaciones (TIC) como responsable de la seguridad de la información y ciberseguridad, de forma periódica y/o excepcional, se rendirán informes respecto del estado de la seguridad de la información y de ciberseguridad.

De igual forma, deberá existir una comunicación fluida desde las diferentes dependencias que soportan los servicios que presta esta organización hacia la Dirección de Tecnología Informáticas y de Comunicaciones (TIC) con el fin de informar sobre las necesidades de seguridad que deben ser consideradas por la organización para su operación.

8. Política de Seguridad de la Información

La Presidencia de esta organización mediante esta política declara a los grupos de interés el firme compromiso que tiene respecto del deber legal de proteger los activos que hacen parte de la infraestructura crítica que soporta la presentación del servicio público de generación de energia y demás activos de información de su propiedad y/o entregados para su custodia en virtud de una obligación legal, estatutaria y/o contractual.

Resultado del valor estratégico que tiene para esta organización la infraestructura crítica y los datos personales o no, información, conocimientos y derechos, se precisan en esta política los parámetros generales que deben tenerse presentes en el logro de los objetivos estratégicos en relación con la integridad, disponibilidad y confidencialidad, sin perjuicio de los otros atributos que se predican respecto de tales activos.

9. Objetivos Específicos de la Política de Seguridad de la Información

La norma ISO 27002 y las demás que hacen parte de este estándar para la gestión segura de la información definen un conjunto de objetivos específicos que contribuyen de forma armónica y sistémica a la protección de los activos que hacen parte de la infraestructura crítica y demás activos de información, como son datos personales o no, información, conocimientos y derechos como pueden ser los originados en la propiedad intelectual.

En el cumplimiento de la gestión segura de la información se dará prioridad a los objetivos específicos exigidos por la normatividad legal vigente en materia de gestión de infraestructura crítica, seguridad de la información, ciberseguridad, datos personales, sin que ello signifique que dejarán de atenderse aquellos otros que de forma indirecta contribuyan al objetivo general señalado en esta Política.

9.1. *Organización de la Seguridad de la Información*

La Alta Dirección de esta organización velará por la existencia, implementación, funcionamiento e incorporación de buenas prácticas de seguridad de la información y ciberseguridad en los procesos empresariales que soportan la ejecución del objeto social y su relacionamiento con los diferentes grupos de interés.

La Gerencia Administrativa, a través de la Dirección de Tecnología Informática y de Comunicaciones (TIC), liderará y velará por la incorporación de las buenas prácticas de seguridad de la información y ciberseguridad y para ello, con apoyo en otros procesos organizacionales, se encargará en relación con el objeto de esta política de: establecer los roles, límites y responsabilidades respecto del acceso, tratamiento y gestión de los activos mencionados en esta política; mantener contacto con las autoridades según las necesidades de la organización en esta materia; establecer los controles que protejan la infraestructura crítica y activos de información de forma segura según los riesgos de cada activo.

9.2. *Seguridad de los Recursos Humanos*

La gestión segura de la información es una obligación que debe estar presente en todos los procesos organizacional que soportan la operación de esta organización, lo cual constituye una obligación para todo empleado.

Corresponde a la Dirección de Talento Humano y Gestión Social, en coordinación con los propietarios de los activos de información y/o bases de datos con información personal a su

cargo, lograr que la seguridad de la información en esta organización se gestione en los siguientes momentos: antes de la relación laboral, durante la relación laboral y después de la relación laboral.

En cualquiera de los tres momentos antes descritos, esta dependencia definirá los lineamientos que contribuyan a la seguridad de la información, ciberseguridad y a la protección de los datos personales con el fin de mitigar riesgos y asegurar que en estos se cumplen los requisitos legales, estatutarios y contractuales vinculados al logro de los objetivos empresariales y objetivos de ciberseguridad establecidos por las autoridades competentes.

Es un propósito de esta organización promover y fortalecer la cultura de la seguridad respecto de la infraestructura crítica, activos de información, incluidos los datos personales, considerando las necesidades de la organización y/o requerimientos de ley.

9.3. Gestión de Activos

La seguridad de la información, la ciberseguridad de la infraestructura crítica y protección de los demás los activos de información, incluidos los datos personales, requiere de la creación y mantenimiento de un inventario de estos, con el fin de gestionarlos de forma segura de acuerdo a las necesidades del negocio y/o requerimientos de ley.

Corresponde a cada propietario del activo de información con el apoyo de la Dirección de Tecnología Informática y de Comunicaciones (TIC) realizar las siguiente acciones: identificar e inventariar los activos que hacen parte de la infraestructura crítica, activos de información, incluidos los datos personales; establecer los criterios de clasificación de estos; adoptar controles para su protección y seguridad cualquiera que sea la forma de su tratamiento, considerando el ciclo de vida de los recursos en los cuales se gestionan estos.

9.4. Control de acceso

La gestión segura de la información, la ciberseguridad, así como la protección de la información personal, exige que los activos que hacen parte la infraestructrua crítica y demás activos de información solo sean tratados por personas autorizadas siendo para ello necesario limitar el acceso de estos a los sistemas de información, centro de procesamiento de datos y centros de gestión documental físicos, aplicando el principio del mínimo necesario.

Corresponderá a la organización, a través de la Dirección de Tecnología Informática y de Comunicaciones (TIC) y respectivo propietario de los activos mencionados, establecer los parámetros y/o directrices para crear usuarios y contraseñas; asignar derechos de acceso y tratamiento a estos; otorgar derechos de acceso privilegiado bajo el principio del mínimo necesario; adoptar mecanismos de autenticación y validación de usuarios; revisar, monitorear y validar los derechos de acceso de forma periódica; y suspender y/o cancelar los accesos a la suspensión o terminación de la relación contractual, respectivamente.

El acceso a los sistemas de información se gestionará cualquiera que sea el ambiente existente para soportar los sistemas de información, sea desarrollo, pruebas, calidad, entrenamiento, pre productivo o productivo.

El derecho de acceso a los sistemas de información cualquiera que sea su naturaleza y centros de procesamiento de datos implica una seria responsabilidad por parte del personal autorizado, por tanto, el derecho concedido es intransferible y por tanto prohibido otorgar este derecho a otra persona.

Se informa que en Colombia el acceso a los sistemas de información sin autorización y/o por fuera de lo acordado puede ser considerado un delito informático según lo dispuesto en la Ley 1273 de 2009[3] que hace parte del Código Penal.

9.5. *Controles criptográficos*

La gestión segura de la información y la protección de datos personales exige el uso de sistemas y técnicas criptográficas como mecanismos de protección de acuerdo con una adecuada gestión de riesgos con el fin de preservar los atributos de integridad, confidencialidad y disponibilidad.

Corresponde a la organización, a través de la Dirección de Tecnología Informática y de Comunicaciones (TIC), la implementación de controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.

El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en el estado del arte en materia de criptografía.

9.6. *Seguridad Física*

La gestión segura de la información, así como la protección de la información personal, involucra el componente físico y ambiental con el fin de prevenir el acceso no autorizado a la información tratada de forma manual, así como el daño y/o destrucción de los centros de procesamiento de datos.

Corresponderá a la organización, a través de la Dirección de Tecnología Informática y de Comunicaciones (TIC), el proceso de Seguridad Física y el respectivo propietario del activo gestionado, establecer los parámetros y/o directrices para establecer controles de acceso, tránsito y salida de las instalaciones de la organización; adoptar controles para proteger los equipos y los activos de información en las instalaciones, oficinas y sedes de la organización;

[3] Congreso de Colombia. (05 de enero de 2009). Ley de protección de la información y de los datos y modificación al código penal. [Ley 1273 de 2009]. DO: 47.223.

proteger los activos vinculados a la infraestructura crítica, definir perímetros de seguridad con el fin de proteger los activos de información y de operaciones sea que se trate estos de forma manual y/o automatizada; adoptar mecanismos que impidan la salida de equipos informáticos u otra naturaleza sin autorización; definir medidas que eviten el deterioro de los activos por factores ambientales u otros.

Es responsabilidad de cada usuario de un activo bajo su responsabilidad aplicar las medidas de seguridad físicas adoptadas por la organización. Debe tenerse presente que los derechos de acceso a la información se otorgan a título personal y por tanto son intransferibles.

9.7. Gestión de las operaciones

La gestión segura de los sistemas de información que soportan los procesos empresariales hace necesario monitorear, documentar y adoptar controles de diferente índole considerando la dinámica de las amenazas y riesgos empresariales en materia de seguridad de la información y ciberseguridad.

Corresponde a la Dirección de Tecnología Informática y de Comunicaciones (TIC) evaluar el posible impacto operativo de los cambios previstos en la infraestructura crítica, sistemas de información, redes y demás activos, siendo necesario como medida preventiva evaluar la capacidad de estos, realizar copias de respaldo y adoptar los controles requeridos para la seguridad de los datos y servicios conectados a las redes de la organización.

9.8. Controles en las comunicaciones

La gestión segura de las redes, requiere de una cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección, acorde a los objetivos estratégicos de la organización.

Corresponde a la Dirección de Tecnología Informática y de Comunicaciones (TIC) asegurar la protección de la información que se comunica a través de la infraestructrua crítica, sistemas de información y redes. Así mismo, es necesario evaluar e implementar los controles adicionales que se requieran para la protección de la información que se trasmite a través de redes públicas, cumpliendo con la legislación vigente y atendiendo la naturaleza del servicio esencial que presta la organización, estos es la prestación del servicio público de generación de energia.

9.9. Adquisición, desarrollo y mantenimiento de sistemas de información

La seguridad de la información, ciberseguridad y protección de los activos de información, incluidos los datos personales, debe ser un requisito fundamental en los procesos de adquisición, desarrollo y mantenimiento de la infraestructura crítica y de los sistemas de información, en los cuales debe garantizarse la integridad, disponibilidad y confidencialidad de los activos de información durante todo el ciclo de vida de estos; sea que la gestión la realice directamente la organización y/o se contrate con un tercero proveedor.

Corresponderá a la organización, a través de la Dirección de Tecnología Informática y de Comunicaciones (TIC), Dirección de Compras y respectivo o futuro propietario del activo de información, señalar parámetros para establecer en cada caso los requisitos de seguridad de la información, ciberseguridad y protección de datos personales que deben estar presentes en el sistema de información; incorporar mecanismos que validen y verifiquen los datos de entrada, salida y procesamiento completo de las transacciones; adoptar prácticas seguras de desarrollo de sistemas de información; implementar prácticas seguras de control de cambios; definir esquemas de pruebas; definir los mecanismos de monitoreo con el fin que los accesos sean autorizados y/o detectar irregularidades; y diseñar estrategias de salida en producción que no comprometan la operación de los servicios de la organización.

Es responsabilidad de todo líder involucrado en la adquisición, desarrollo y mantenimiento de sistemas de información definir al inicio del proyecto los requisitos que permitan garantizar la seguridad de los activos de información, de operaciones y datos personales tratados en el respectivo sistema de información, considerando el riesgo derivado de la prestación del servicio público de generación de energia y los propios de la infraestructura crítica que soporta a este.

Es indispensable que toda adquisición, desarrollo y/o mantenimiento de un sistema de información incluidas las redes, incorpore como requisito la seguridad de los activos que hacen parte de la infraestructura crítica, activos de información y protección de datos personales en cualquier de los momentos del proyecto, independiente de que este lo ejecute directamente la organización y/o se contrate con un tercero.

No son aceptables sistemas de información que adolezcan de funcionalidades que omitan la seguridad de los activos mencionados, incluidos los datos personales.

9.10. Relaciones con los proveedores

La seguridad de la información, ciberseguridad y protección de datos es un deber que involucra a los terceros proveedores que en razón de las relaciones precontractuales, contractuales o postcontractuales acceden y/o realizan cualquier tratamientos respecto de los activos de información, incluidos los datos personales, que están en poder y/o bajo la custodia de esta organización.

Corresponde a esta TEBSA adoptar directrices en relación con: establecer los criterios a tener presentes en la selección de proveedores que deban acceder y/o tratar activos de información, incluidos los datos personales; fijar las condiciones bajo las cuales los terceros proveedores accederán y tratarán los activos de información que requieran para en el marco de los tres momentos de la contratación antes enunciados; establecer los parámetros; y dar directrices para que los propietarios del activo de información, incluidos los datos personales, verifiquen que los proveedores y/o prestador de servicios gestionan estos de forma segura en razón del acceso y/o tratamiento que realizan de estos en los tres (3) momentos de la relación contractual con estos.

9.11. Gestión de incidentes de seguridad de la información

La seguridad de la información y de los datos personales imponen a la organización la obligación de gestionar de forma adecuada los incidentes de seguridad que comprometan algún activo que haga parte de la infraestructura crítica, activos de información; siendo obligación reportar ante las autoridades competentes en Colombia tales como el Centro Cibernético de la Policia Nacional, Csirt, Colcert, la SIC[4] aquellos que hayan comprometido cualquier tipo de dato personal, entre otros conforme la regulación existente en el momento del incidentes.

Corresponde a la Dirección de Tecnología Informática y de Comunicaciones (TIC) en relación con la gestión de los incidentes de seguridad de la información adoptar el procedimiento para la gestión de estos y consecuente respuesta, así como desplegar un plan de acción que de forma periódica evalúe las debilidades de la seguridad de la información y ciberseguridad a nivel físico e informático; clasificar y analizar los eventos de seguridad para definir si han alcanzado el nivel de incidentes; gestionar el conocimiento a partir de los incidentes para adoptar controles que mejoren la seguridad de la información y fortalezcan las competencias para responder a los incidentes de seguridad de la información y/o ciberseguridad, sea que incluyan datos personales o no.

Es responsabilidad de la Dirección de Tecnología Informática y de Comunicaciones (TIC) y/o de la Dependencia responsable de la Protección de Datos Personales según el caso, gestionar de forma adecuada todo incidente de seguridad de la información que comprometa un activo que haga parte de la infraestructura crítica, un activo de información y/o datos personales. El Informe del incidente de seguridad, realizado a partir del procedimiento de atención a este, será presentado a la Alta Dirección con el fin de informar sobre la situación, previo el reporte que debe realizarse a las autoridades competentes según el caso en los términos establecidos en la ley.

La gestión del incidente de seguridad de respecto de la infraestructura crítica, activos de información y/o datos personales debe ser pactado como obligación de los proveedores involucrados de forma directa o indirecta en el incidente de seguridad; tal como lo exige el principio de seguridad incorporado en el régimen de Protección de Datos vigente en Colombia

Es obligación de todo destinatario de esta norma informar sobre la sospecha de una situación que pueda comprometer la seguridad de la infraestructura crítica, un activo de información, incluido los datos personales. Reporte que se realizará a la Dirección de Tecnología Informática y de Comunicaciones (TIC) conforme el procedimiento adoptado para este fin.

9.12. Gestión de la continuidad tecnológica

Preservar la seguridad de la información durante las fases de activación, desarrollo de procesos, procedimientos y planes para la continuidad de negocio y retorno a la normalidad, implica integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información, ciberseguridad y datos personales con atención especial a la

[4] Congreso de Colombia. (17 de octubre de 2012). Artículos 17 y 18 [Título VI]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

legislación, la prestación del servicio público de generación de energía, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

Corresponde a la Dirección de Tecnología Informática y de Comunicaciones (TIC) desarrollar e implementar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información y ciberseguridad utilizada en los planes de continuidad y función de los resultados del análisis de riesgos, minimizando los efectos de las posibles interrupciones de las actividades normales de la organización asociadas a desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos, protegiendo los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

9.13. Cumplimiento de los requisitos legales

Es deber de la organización en materia de seguridad de la información, ciberseguridad, protección de datos personales, propiedad intelectual entre otros, monitorear y evaluar de forma periódica en cumplimiento de la normatividad legales, así como el cumplimiento de las obligaciones contractuales con terceros proveedores que participen en la prestación del servicio público de generación de energia y/o mantenimiento y/o soporte a la infraestructura crítica que gestiona esta organización.

En este sentido, los requisitos normativos y contractuales pertinentes a cada sistema de información impacatdo en materia de seguridad de la información, ciberseguridad y protección de datos personales deberían estar debidamente definidos y documentados.

10. Desarrollo de la Política

El cumplimiento de esta política se realizará en armonía con la Política de Privacidad (Protección de Datos Personales) adoptada por esta organización y demás instrumentos normativos que la desarrollan. Lo anterior, sin perjuicio de la necesaria y armónica interpretación que debe realizarse con las normas legales que apliquen a la organización.

11. Control

El responsable de este documento es la Dirección de Tecnología Informática y de Comunicaciones (TIC) a quien corresponde revisarlo al menos una vez al año y realizar una actualización si lo considera necesario o realizar esta cuando surja un cambio importante; caso en el cual deberá ser aprobado por la Alta Dirección y comunicarlo a los destinatarios y/o partes interesadas de este documento.

12. Aprobación

Esta Política de Seguridad de la Información y Ciberseguridad ha sido aprobada 18/12/2019 por la Presidencia de TERMOBARRANQUILLA S.A. ESP.

LUIS MIGUEL FERNANDEZ ZAHER
PRESIDENTE

Soledad, Diciembre 18 de 2019.