PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EMPRESA DE SERVICIOS PÚBLICOS DE CAJICÁ SA ESP

VIGENCIA

Actualizado FEBRERO 2024

RAFAEL PACHÓN CALDERON
Profesional Universitario Sistemas

Contenido

1. OBJETIVO

Definir y aplicar los lineamientos para tratar de una manera integral los riesgos de Seguridad y Privacidad de la información, seguridad digital y permitiendo la estabilidad de los servicios (riesgos de interrupción) a los que la Empresa de Servicios Públicos de Cajicá S.A. E.S.P, pueda estar expuesta, y de acuerdo a esta manera lograr los objetivos, la Misión y Visión institucional, protegiendo la integridad, la confianza, la privacidad y la autenticidad de la información.

Establecer un plan de acción que permita enfrentar los riesgos en ciberseguridad, sobre la infraestructura tecnológica de la EPC, los servicios informáticos y la información. Para garantizar la prestación de los servicios públicos.

2. ALCANCE DEL PLAN

El plan Tratamiento De Riesgo De Seguridad Y Privacidad de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P.,

El plan de seguridad y privacidad de la información (PSPI) de la EPC, abarca toda la infraestructura tecnológica de la empresa, los servicios que allí se prestan la información procesada y almacenada y todas las personas o entidades que tenga relación con la prestación de los servicios de la EPC.

3. CONCEPTOS

Conforme la Comisión de Regulación de Comunicaciones y su normativa aplicable se tienen en cuenta los siguientes términos:

Autenticación: Proceso destinado a permitir al sistema asegurar la identificación de una parte.
Autorización: Proceso de atribución de derechos o concesión de permisos para realizar determinadas actividades y su relación con determinados procesos, entidades, personas jurídicas o naturales.
Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.
Ciberseguridad: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.
Confidencialidad de datos: Impedir que los datos sean divulgados sin autorización.

Disponibilidad: Acceso por parte de una entidad autorizada a la información y sistemas informáticos, cuando esta entidad lo requiera.
Entidad: Persona natural o jurídica, organización, elemento perteneciente a un equipo o a un programa informático.
Infraestructura crítica: Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una Nación.
Integridad de datos: Propiedad o característica de mantener la exactitud y completitud de la información.
Interceptación: Es la adquisición, visualización, captura o copia de contenido, datos o parte de contenido de una comunicación transmitida por medio alámbrico, electrónico, óptico, magnético u otras formas, realizada durante la transmisión, utilizando medios electrónicos, mecánicos, ópticos o electromagnéticos.
Interferencia: Es la acción de bloquear, ocultar, impedir o interrumpir la confidencialidad, la integridad de programas computacionales, sistemas computacionales, datos o información, mediante la transmisión, daño, borrado, destrucción, alteración o supresión de datos, de programas de computación o tráfico de datos.
Interrupción: Es el evento causado por un programa computacional, una red de telecomunicaciones o sistema computacional que interfiere o destruye un programa computacional, una red de telecomunicaciones, datos e información que esta contenga.
No repudio: Servicio que tiene como objetivo garantizar la disponibilidad de pruebas que pueden presentarse a terceros y utilizarse para demostrar que un determinado evento o acción ha tenido lugar, con el propósito de evitar que una persona o una entidad niegue haber realizado una acción de tratamiento de datos, proporcionando prueba de dichas acciones en la red.
Pharming: Es la acción de modificar el servidor (DNS) Domain Name System, cambiando la dirección IP correcta por otra, de tal manera que haga entrar al usuario a una IP diferente con la creencia de que accede a un sitio personal, comercial o de confianza.
Phishing: Acto de enviar un correo electrónico cuyo objeto es engañar al usuario dirigiéndolo a una página web falsa y por este medio, obtener de este, información privada que será utilizada para fines no autorizados o ilícitos como el robo de identidad y de contraseñas.
Software Malicioso (Malware): Es un programa computacional que es insertado en un computador o sistema computacional sin autorización, con el objeto de comprometer la confidencialidad e integridad del sistema computacional, de la red de telecomunicaciones, datos y del tráfico de datos. Esta clase de programa se presenta en forma de virus, gusanos, y troyanos electrónicos y demás, que se pueden distribuir a través de email, web site, shareware o freeware.
Vulnerabilidad: Cualquier debilidad que pudiera explotarse con el fin de violar un sistema o de la información que contiene".

4. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan es una guía complementaria a los procesos y procedimientos del *proceso de gestión de tecnología e infraestructura*, de la EPC, así como al documento PETI, y los demás documentos que soportan la infraestructura tecnológica de la EPC.

El Ministerio de las Tecnologías de la Información y las Comunicaciones MinTIC, ha establecido a través del Modelo de Seguridad y Privacidad de la Información que su adopción permitirá a las entidades garantizar los tres pilares de la seguridad de la información: Confidencialidad, integridad y disponibilidad, por tal razón la EPC ha desarrollado un plan conforme a los recursos existentes en la empresa.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EPC			
COMPONENTE	**DESCRIPCIÓN DE LAS ACTIVIDADES**	**RESPONSABLE**	**FECHA LIMITE**
Seguridad de hardware y elementos de red	* Revisar equipos y su configuración * Adquirir e instalar equipos UPS, para garantizar su funcionamiento ininterrumpido.	* Profesional universitario Sistemas * Apoyo sistemas	15 junio de 2024
Seguridad de software	* Adquisición de antivirus * Instalación y actualización de antivirus instalados * Adquisición de software legal	* Profesional universitario Sistemas * Apoyo sistemas	30 octubre de 2024
Seguridad de la información	* Revisión al software de automatización de copias de seguridad * Revisión de copias e integridad de datos	* Apoyo Sistemas	Constante
Riesgos	* Construcción y análisis de matriz de riesgos en ciberseguridad	* Profesional universitario Sistemas * Apoyo sistemas	30 marzo de 2024
Infraestructura tecnológica	* Actualización de inventario y hoja de vida de equipos de computo	* Apoyo Sistemas	30 mayo de 2024
Infraestructura tecnológica	* Instalación y mejoramiento de las adecuaciones de redes	* Profesional universitario Sistemas * Apoyo sistemas	30 noviembre de 2024

Capacitación	* Capacitación en ciberseguridad a los funcionarios administrativos de la EPC	* Profesional universitario Sistemas * Apoyo sistemas	30 agosto de 2024

5. PLAN DE CONTINGENCIA

La EPC, cuenta con un plan de contingencia descrito en el documento denominado *PLAN DE CONTIGENCIA EPC*, en este se definen los posibles riesgos y su materialización, actividades posteriores a la detección de los mismos y su completa mitigación.

El plan de contingencia contempla la restauración de los servicios informáticos locales, bases de datos, información de gestión disponible, recursos de internet (si existe ISP), recursos de impresión y el restablecimiento de la seguridad informática.

Matriz de riesgos en tecnología

I. IDENTIFICACIÓN DEL RIESGO										
ID Riesgo	**Sistema Asociado al Riesgo**						**Tipo de Riesgo**	**Descripción del Riesgo**	**¿El riesgo ya se ha materializado?**	**Parte Interesada Asociada**
	Calidad	**Ambiental**	**SST**	**Seguridad de la**	**Anticorrupción**	**MIPG**				
R-GTI-001	Si	No	No	Si	No	Si	Tecnológico	Insuficiencia e inadecuada infraestructura tecnológica	No	* Entes de Control y Vigilancia * Colaboradores * Proveedores y/o Contratistas

R-GTI-002	Si	No	No	Si	No	Si	Tecnológico	Accesos no autorizados al area fisica de la empresa	No	* Entes de Control y Vigilancia * Colaboradores * Proveedores y/o Contratistas
R-GTI-003	Si	No	No	Si	No	Si	Tecnológico	Incumplimiento o inconsistencias en el Backup institucional	No	* Entes de Control y Vigilancia * Colaboradores * Proveedores y/o Contratistas
R-GTI-004	Si	No	No	Si	No	Si	Tecnológico	Acceso no autorizado al sistema de información de la EPC	No	* Colaboradores * Proveedores y/o Contratistas
R-GTI-005	Si	No	No	Si	No	Si	Tecnológico	Instalación de malware en los equipos de computo	No	* Colaboradores * Proveedores y/o Contratistas
R-GTI-006	Si	No	No	Si	No	Si	Tecnológico	Acceso no autorizado a los equipos de computo	No	* Colaboradores * Proveedores y/o Contratistas

Ver matriz de riesgos del proceso de Gestión de Tecnología e infraestructura