POLÍTICA DE PROTECCIÓN

PARA LAS PERSONAS, ACTIVOS Y OPERACIONES TECNOLÓGICAS DE LAS EMPRESAS DEL GRUPO ENERGÍA DE BOGOTÁ

ENERGIA de Bogotá

CASA MATRIZ DEL:

GRUPO ENERGÍA DE BOGOTÁ

POLÍTICA DE PROTECCIÓN
PARA LAS PERSONAS, ACTIVOS Y OPERACIONES TECNOLÓGICAS DE LAS EMPRESAS DEL GRUPO ENERGÍA DE BOGOTÁ

INTRODUCCIÓN

Alineada con la Política Macro de Responsabilidad Corporativa, la Política de protección para las personas, activos y operaciones tecnológicas del Grupo Energía de Bogotá ofrece un marco de referencia con principios que orientan el desarrollo de programas y planes de protección en las empresas del Grupo Energía de Bogotá.

DECLARACIÓN DE COMPROMISO

Es nuestro deber actuar de acuerdo con nuestros valores corporativos donde el Grupo de Energía de Bogotá tenga presencia o impacto.

Con esta motivación, el Grupo de Energía de Bogotá declara su compromiso para promover la protección física de los colaboradores, de las instalaciones e infraestructura, la seguridad de la información, el uso adecuado de las tecnologías de información, la protección de la propiedad intelectual y la seguridad de sus bienes e intereses para las empresas del Grupo Energía de Bogotá y en tal sentido se compromete a:

- Implementar Programas de protección y prevención.
- Analizar los riesgos, estableciendo los controles y medidas, para prevenir, corregir, minimizar, transferir o asumir los riesgos dentro de los programas establecidos.
- Realizar seguimiento a los programas y actualizarlos cuando sea necesario.

MARCO DE ACTUACIÓN

Con el objetivo de cumplir con el compromiso establecido en la Política, las Empresas del Grupo Energía de Bogotá:

- Promueven y establecen una cultura de protección, fundamentada en la promoción del autocuidado en los colaboradores, en su entorno físico y psicológico, que facilite el mejoramiento de la calidad de vida.

- Definen los procesos y protocolos que deben ser tenidos en cuenta para la seguridad de los colaboradores y de la Infraestructura.

- Desarrollan e implementan un Programa de Seguridad Industrial y Salud Ocupacional acorde con las disposiciones legales de cada País y en caso de no existir acorde con las directrices del corporativo; necesario para proteger, prevenir, mitigar y evitar accidentes y enfermedades profesionales de todos sus colaboradores, identificando peligros y evaluación de riesgos en seguridad industrial y salud ocupacional.

- Promueven e incentivan en los colaboradores el deber de cumplir con las normas y políticas de salud ocupacional.

- Adoptan medidas para garantizar que los riesgos a contratistas in-house se cumplan dentro de las normas vigentes de protección.

- Promueven y establecen mecanismos y sistemas de seguridad de los recursos físicos, previniendo los riesgos que vulneren la infraestructura disponible, bienes y/o servicios.

- Mantienen actualizado el esquema de comunicación identificando los organismos de seguridad y los teléfonos de emergencia para los casos de urgencia, así mismo se mantienen al tanto de hechos que afecten la alteración del orden público y pongan en riesgo a las personas, infraestructura o bienes.

- Establecen los protocolos relacionados con la protección de personas, bienes e infraestructura de transmisión de energía y red de gasoductos.

- Implementan procesos de protección de la información como un activo fundamental para el desarrollo de sus actividades, razón por la cual garantizan la calidad e idoneidad de la tecnología disponible, la periodicidad en la conservación, la custodia del archivo, la memoria institucional de todas las compañías y el manejo de información y documentación con la confidencialidad, integridad y disponibilidad requeridas.

- Adoptan medidas para contar con tecnología e información íntegra, confiable, vigente y costo efectiva para apoyar la gestión oportuna y el crecimiento de la organización, tomando acciones apropiadas para asegurar que la información y los sistemas de información estén protegidos de amenazas y riesgos, tales como: fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, "Hackers", interrupción de servicio, accidentes y desastres naturales, así mismo promueven y desarrollan la cultura de protección y uso adecuado de la tecnología de la Información y la propiedad intelectual con todos sus colaboradores.

- Formulan un Plan Estratégico de Tecnología de Información (PETI), alineado con el Plan Estratégico Corporativo (PEC) y los Procesos de la Organización, que sirva de guía para atender las necesidades actuales y futuras, mediante el uso de Tecnología de punta.

- Evalúan riesgos y establecen controles que permitan acceso únicamente a las personas autorizadas, en instalaciones, sistemas de información, telefonía e información.

- Desarrollan planes de continuidad de tecnología de información, para que puedan reanudar sus operaciones básicas, ante un desastre.

- Procuran unificación de las tecnologías de información, para que exista un mismo lenguaje de comunicación entre las empresas del Grupo Energía de Bogotá.

- Protegen legalmente la propiedad intelectual y la información estratégica de cada una de las Empresas del Grupo, cumpliendo con lo consagrado en la Constitución Política, la normatividad y acuerdos regionales e internacionales aplicables.

- Establecen programas de seguros que garanticen que todos sus activos, operaciones, personas e intereses están protegidos de manera oportuna y adecuada en consonancia con los lineamientos definidos por la EEB como Casa Matriz.

- Realizan una gestión de seguimiento y monitoreo a los programas y las acciones establecidas a fin de que se cumplan; así mismo se comprometen a mantenerlos actualizado de conformidad con las necesidades que surjan dentro de su entorno o ámbito de país.

RESPONSABLES DE LA POLÍTICA

La administración y seguimiento de la política está a cargo de la Vicepresidencia Administrativa, quien velará por el cumplimiento de la misma en el Centro Corporativo, filiales y en la Fundación del Grupo a quienes corresponde implementar y cumplir la presente política.

MEJORES PRÁCTICAS

Las Empresas del Grupo, conforme con las mejores prácticas aplica normas estándares, para desarrollar técnicas y lograr la continuidad del negocio, para responder a eventos severos de interrupción y evitar impactos significativos; contando con respuestas a emergencias, gestión de crisis, comunicación en crisis, recuperación de áreas de Negocio y Apoyo (BCP) y recuperación ante desastres (DRP). Tener una visión integral de la continuidad del negocio, se deben incluir áreas de apoyo.

Así mismo y dentro de esas mejores prácticas desarrolla un plan estratégico en continuidad del negocio, incluyendo indicadores de cumplimiento cuyos objetivos sean negociados por el Gestor de Continuidad y realizar un diagnóstico de la Gestión de Continuidad de Negocio en EEB, tomando como referencia las mejores prácticas internacionales (DRII, BCI y BS 25999).

ANEXO 1

CONCEPTOS APLICABLES A LA POLITICA DE PROTECCIÓN PARA LAS PERSONAS, ACTIVOS Y OPERACIONES

A continuación se enuncian las definiciones aplicables:

CALIDAD DE VIDA: Compromiso con la calidad de vida de sus colaboradores a través del código de conducta, en el cual se expresan valores como el respeto profesional y personal, la colaboración y ayuda mutua, la igualdad de oportunidades para el desarrollo profesional y el compromiso y dedicación en las labores que propenden por el logro de los objetivos del Ámbito Corporativo y de la Seguridad Industrial que se basa en la prevención.

CONFIDENCIALIDAD: Seguridad de que la información es accesible solamente a personal autorizado para ello; haciendo un manejo prudente y una utilización estricta relacionada únicamente con las responsabilidades del cargo.

CONTROL: Medida que modifica el riesgo.

GESTIÓN DEL RIESGO: Involucra los siguientes procesos:

1. Identificar y analizar el riesgo.

2. Examinar la factibilidad de alternativas o técnicas para su mitigación.

3. Seleccionar las mejores técnicas disponibles y factibles.

4. Implementar las técnicas escogidas.

5. Dar el seguimiento al programa o acciones implementadas.

INFORMACIÓN: Recurso y activo intangible de una empresa que permite a la Alta Gerencia la toma de decisiones correctas. Así como el conocimiento de la Empresa que cada colaborador adquiera en virtud de sus funciones.

LICENCIAS O AUTORIZACIONES DE USO: Autorización o permiso que concede el propietario patrimonial de una aplicación (software), una obra literaria, musical, etc., para que las compañías puedan desarrollar determinadas actividades.

POLÍTICA DE PROTECCIÓN PARA LAS PERSONAS, ACTIVOS, OPERACIONES Y TECNOLOGÍA DE LA INFORMACIÓN: Propósitos y dirección generales de la organización relacionados con el manejo de seguridad, manejando el riesgo que pueda ocasionarse en cualquier ámbito.

PREVENCIÓN: Preparar con anticipación lo necesario para un fin, anticiparse a una dificultad, prever un daño. La prevención, por la tanto, es la disposición que se hace de forma anticipada para minimizar un riesgo. El objetivo de prevenir es lograr que un perjuicio eventual no se concrete.

PROGRAMA: Un conjunto de instrucciones u órdenes para resolver un problema o una función específica. Es la relación ordenada de actividades, con una secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.

PROTECCIÓN AMBIENTAL: Toma de acciones preventivas, reactivas y correctivas sobre los impactos en el entorno en el cual el Grupo de Energía opera, incluidos el aire, el agua, el suelo, los recursos naturales, la flora, la fauna, los seres humanos y sus interrelaciones.

PROTECCIÓN DE LA VIDA: Toma de acciones preventivas, reactivas y correctivas sobre las condiciones y factores que afectan, o podrían afectar a la salud y la seguridad de las personas en el lugar de trabajo.

RIESGO: Es el efecto de la incertidumbre sobre los objetivos. Cualquier, evento, amenaza, acto u omisión que en algún momento pueda impedir el logro de los objetivos de la organización. No está limitado a acontecimientos negativos o eventos inesperados, incluye también la ausencia desaprovechamiento de oportunidades.

RIESGO INFORMÁTICO: Evento potencial generado por uso inadecuado de tecnología de información.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

TECNOLOGÍA DE INFORMACIÓN: Adelantos científicos que permiten la optimización en el manejo de grandes volúmenes de información, así como su adecuada organización, su disponibilidad y protección.