EEC.13 Seguridad de la información

Política – Procedimiento Seguridad de la Información - ENS

Índice

Control del Documento

Identificación del documento

Nombre del fichero	Título
EEC.P02-02 Política Procedimiento Seguridad de la Información - ENS	Procedimientos

Autor/es del documento

Persona	Entidad

Resumen de cambios

Versión	Fecha	Resumen de los cambios
1	11/2021	Documento base
2	01/2024	Actualización RD 311/2022

Aprobaciones del documento

Persona	Entidad
Juan Enrique Núñez	Epresa
Emilio Fernández	Epresa
David Muñoz	Epresa

Distribución del documento

Persona	Entidad
Personal	Epresa

Documentos relacionados

Fichero

1. Aprobación y entrada en vigor

Texto aprobado el día 09 de enero de 2024 por EPRESA.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política. Fases de un plan de continuidad

2. Introducción

EPRESA ENERGIA S.A. depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, trazabilidad, autenticidad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo legislación RD 311/2022.

Desde su constitución, el objetivo de EPRESA ENERGÍA, S.A., es prestar servicio a sus clientes cumpliendo los requisitos establecidos, de forma que obtengan la máxima satisfacción con nuestros servicios y garantice la máxima privacidad y seguridad de la información. Dicho objetivo de satisfacción de nuestros clientes y confidencialidad de la información es la piedra angular de nuestra política, entendiendo la satisfacción como el cumplimiento de los compromisos contraídos de la forma más eficiente posible, a la vez que se procura cumplir con las expectativas no contractuales derivadas de las necesidades descubiertas en la ejecución del servicio y relacionadas con el mismo, que el propio cliente nos comunica. Mediante la aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en los requisitos del Esquema Nacional de

Seguridad conforme al RD 311/2022 , se persigue una mejora continua en la calidad de los servicios que desarrolla nuestra organización, así como un compromiso de mejora técnica de nuestros activos, sistemas y procesos y los de nuestros proveedores, para garantizar una adaptación, de forma continuada, a las necesidades tecnológicas de nuestros clientes. Para ello, EPRESA ENERGÍA, S.A, recoge en esta Política, los pilares básicos de la Organización para alcanzar la mejora continua de la eficacia de dicho sistema de Gestión, que servirán de base al establecimiento de nuestros objetivos anuales:

- Asegurar la satisfacción de sus clientes basándose en un trato siempre correcto y en un esfuerzo continuo en la prestación del servicio en base a sus requisitos y a nuestros compromisos de actualizaciones y mejoras.
- Cumplir con los requisitos de los clientes y de sus grupos de interés, así como con los requisitos legales y reglamentarios que afecten a la realización y prestación de los servicios prestados.
- Cumplir con los requisitos legales que le son de aplicación, así como con aquellos requisitos que la organización suscriba evaluando continuamente dicho cumplimiento, en todas sus áreas de actividad.
- Evaluar los riesgos de la organización, de todos los procesos realizados y de los activos de información, previendo y evitando así desviaciones y tomando las oportunas decisiones para minimizar posibles no conformidades.
- Establecer procesos operacionales que salvaguarden a las personas, la propiedad, la información, los datos y las aplicaciones o sistemas de uso para las instancias establecidas por la Organización.
- Velar por una continua y permanente actualización de nuestros recursos, tanto tecnológicos como humanos, fomentando políticas de información y formación continua profesional que les permita avanzar en sus conocimientos al ritmo que lo hace nuestro sector, fomentando la concienciación de la seguridad de la información.
- Establecer y revisar regularmente los Objetivos, acordes con los compromisos que se asumen en esta declaración, fortaleciendo el compromiso y participación de todo el personal en el desarrollo y consecución de los mismos.
- Garantizar la mejora continua del Sistema, para constatar el compromiso asumido con los clientes, buscando una mejor organización interna del trabajo y cómo tratamos la información de nuestros clientes.
- Lograr que la seguridad de la información y el respeto a los datos personales sean una constante:
    - Preservando la confidencialidad de la información y evitando su divulgación y el acceso por personas no autorizadas.
    - Manteniendo la integridad de la información procurando su exactitud y evitando su deterioro.

    - Asegurando la disponibilidad de la información en todos los soportes y siempre que sea necesaria.
- La Dirección, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos la valoración de la disponibilidad, confidencialidad e integridad de su información y aún más de la de sus clientes.

2.1 Prevención

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Autorizar los sistemas antes de entrar en operación.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3 Respuesta

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias.

2.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. Alcance

La Organización establece para el ENS RD 311/2022 esta política que se aplica a Los sistemas de información que dan soporte a las actividades de:

- Comercialización de energía eléctrica en el mercado libre, diseño e instalación de redes de telecomunicaciones.
- Proveedor de acceso a internet + voz IP y telefonía.

Esta política se aplica a todos los sistemas TIC de EPRESA ENERGIA S.A., y a todos los miembros de la organización, sin excepciones.

4. Misión

EPRESA ENERGIA S.A., para la gestión de sus intereses, y en el ámbito de sus competencias y como empresa que presta servicios tanto a empresas privadas como a la Administración pública, sirve con objetividad los intereses generales y actúa de acuerdo a los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios que contribuyen a satisfacer las necesidades y aspiraciones de su personal y de sus clientes.

La presente Política de Seguridad aplica a las diferentes actividades en las que participa EPRESA ENERGÍA S.A.

5. Marco Normativo

El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

Atendiendo al ámbito datos personales:

- Real Decreto 1720/2007 de 21 de Diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018 de 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales
- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).

En el marco de certificaciones:

- ISO 9001:2015, Sistemas de Gestión de la Calidad
- ISO 14001:2015, Sistemas de Gestión Ambiental
- ISO 45001:2018, Sistemas de Gestión de seguridad y salud en el trabajo.
- Norma UNE-EN ISO/IEC 27001:2017 - Sistemas de Gestión de Seguridad de la Información (SGSI)
- ISO 50001:2018 Sistema de Gestión de la Energía.

Área ENS:

- Real Decreto 311/2022 de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad
- Guías de la serie 800 CCN-STIC como guías de estructuración documental.
- Ley 39/2015 de 1 de Octubre, Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015 de 1 de Octubre, Régimen Jurídico del Sector Público
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y de su Reglamento de Desarrollo.

Área de Contratación Pública:

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014
- Ley Foral 2/2018, de 13 de abril, ce contratos Públicos. Área de actividades comerciales Ley 34/2002 de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico

En cualquier caso, EPRESA ENERGÍA, S.A, cumple con el marco normativo vigente que regula su actividad y dispone de un procedimiento y registro para identificación y evaluación de requisitos legales.

6. Roles: Funciones y responsabilidades

La estructura organizativa de seguridad, y jerarquía en el proceso de decisiones la componen:

Funciones de la Dirección:

- Designar los diferentes roles encargados de la gestión de la seguridad.
- Dirigir, coordinar y controlar las acciones de los órganos ejecutivos y operativos de la empresa.
- Ejecutar las disposiciones para el logro, competitividad y rentabilidad empresarial en un marco de mejora continua.

- Es el área de mayor jerarquía de la empresa y le corresponde la representación de la Sociedad ante toda clase de autoridades, gozando de las facultades necesarias para ejercer esta representación.

Aprobar:

- Aprobar el Plan de Adecuación al ENS.
- Aprobar la Política de Seguridad así como las revisiones de la misma.
- Aprobar, tras cada proceso de Apreciación del Riesgo que se realice, del Plan de Tratamiento del Riesgo que se elabore, que puede incluir la aplicación de controles, la transferencia a terceros, evitar riesgos, o bien la asunción de determinados riesgos.

Recursos

- Proporcionar los recursos necesarios para el aseguramiento del cumplimiento de estos objetivos y para la operación del Sistema Integrado de Gestión.

Funciones del Comité de Seguridad de la Información y la Privacidad y Privacidad:

Responsables que toman decisiones que concretan cómo alcanzar los objetivos de seguridad y protección de la privacidad marcada por la Dirección.

Funciones del Responsable de la Información:

- Determina los requisitos de seguridad de la información tratada, según los parámetros del Anexo I del ENS.
- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Aprobación de los niveles de seguridad de la información.

- Proteger los activos.
- Cumplimiento de sus obligaciones de servicio, el respecto de la legalidad y los derechos.

Funciones del Responsable de Servicio:

- Determina los requisitos de seguridad de los servicios prestados, según los parámetros del Anexo I del ENS.
- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Aprobación de los niveles de seguridad de los servicios.
- Proteger los activos.
- Cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos.

Funciones del Responsable de Seguridad:

- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por el responsable de la información y de los servicios.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la Organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.
- Elaborar y proponer para aprobación por la organización, las medidas técnicas y organizativas, adecuadas y proporcionales, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y minimizar así los efectos.
- Desarrollar, supervisar y auditar las medidas técnicas y organizativas aprobadas.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como mentor de buenas prácticas en seguridad de las redes y sistemas de información.
- Ser punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y de su Reglamento de Desarrollo.
- Ser el punto de contacto para la coordinación con el CSIRT (Computer Security Incident Response Team – Equipo de Respuesta ante Emergencias Informáticas) de referencia (CCN-Cert, INCIBE.).

- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

Funciones del Responsable del Sistema:

- Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.
- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Elaborar procedimientos operativos de seguridad.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.

- Comunicar tan pronto como se tenga constancia de la misma al Responsable de Seguridad las violaciones de seguridad que afecten a datos personales.

Funciones de Administradores de seguridad.

- Son las personas encargadas de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Comunicar tan pronto como se tenga constancia de la misma al Responsable de Seguridad las violaciones de seguridad que afecten a datos personales.

Funciones del Delegado de Protección de Datos

Si fuera obligatorios, es el encargado de asesorar y supervisar todos los aspectos relacionados con el tratamiento de datos de carácter personal, incluidos los aspectos de seguridad (integridad, confidencialidad y disponibilidad) y violación de datos personales. Su nombramiento se produce por otra vía ya que sus cometidos no se ciñen únicamente a aspectos de seguridad.

Comité de Seguridad de la Información y la Privacidad.

El Comité de Seguridad de la Información y la Privacidad coordina la seguridad de la información a nivel de Organización.

Composición. Se ha creado el Comité de Seguridad de la Información y la Privacidad que estará compuesto por los siguientes miembros:

a. Dirección y Responsable de la información: Juan Enrique Nuñez.
b. Responsable de Dpto. de Sistemas y Responsable del Sistema: Emilio Fernández González
c. Adjunto a Dirección y Responsable del Servicio: Emilio Fernández González
d. Técnico de Dpto. de Sistemas y Responsable de Seguridad: Antolín Soria

Funciones del Comité de Seguridad de la Información y la Privacidad:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos/áreas.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de EPRESA ENERGÍA S.A.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Elaborar la estrategia de evolución de EPRESA ENERGÍA S.A. en lo que respecta a la seguridad de la información.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y cualificación de los trabajadores desde el punto de vista de seguridad de la información
- Aprobar planes de mejora de la seguridad de la información de EPRESA ENERGÍA S.A. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Monitorizar los principales riesgos residuales asumidos por EPRESA ENERGÍA S.A. y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Velar para que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- Decidir si una violación de seguridad de datos personales debe ser notificada a la Agencia Española de Protección de Datos y/o a los propios interesados.
- Emitir su opinión y participar en los aspectos de seguridad de las Evaluaciones de impacto en protección de datos.

6.1. Jerarquía en el proceso de decisiones y mecanismos de coordinación

Los diferentes roles de seguridad de la información se limitan a una jerarquía simple: el Comité de Seguridad de la Información y la Privacidad da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para EPRESA ENERGÍSA S.A.

El Responsable del Sistema:

- Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
- Informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
- Da cuenta al Responsable de la Seguridad:
    - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
    - Resumen consolidado de los incidentes de seguridad.
    - Medidas de la eficacia de las medidas de protección que se deben implantar.

El Responsable de la Seguridad:

- Informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Da cuenta al Comité de Seguridad de la Información y la Privacidad, como secretario:
    - Resumen consolidado de actuaciones en materia de seguridad.
    - Resumen consolidado de incidentes relativos a la seguridad de la información.
    - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.
- Da cuenta al Consejo de Dirección, según lo acordado en el Comité de Seguridad de la Información y la Privacidad.

- Resumen consolidado de actuaciones en materia de seguridad.
- Resumen consolidado de incidentes relativos a la seguridad de la información.
- Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

- Da cuenta al Delegado de Protección de Datos, si lo hubiera, sobre los aspectos que afecten a la seguridad de los datos personales.

  - Violaciones de seguridad de los datos personales que afecten a la confidencialidad, disponibilidad e integridad de los datos personales.
  - Riesgos detectados y medidas correctoras oportunas relacionados con la seguridad de los tratamientos de datos personales.
  - Pedirá asesoramiento ante nuevas arquitecturas de seguridad, políticas y procedimientos que afecten al tratamiento de datos personales.

7. Datos de Carácter Personal

EPRESA ENERGÍA S.A. trata los datos de carácter personal, por lo que mantiene un “registro de actividades de tratamiento”, al que tendrán acceso sólo las personas autorizadas, en le que se recogen los datos afectados y los responsables del tratamiento. Todos los sistemas de información de EPRESA ENERGÍA S.A se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado registro.

8. Obligaciones del personal

Todos los miembros de EPRESA ENERGÍA S.A., tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender al Personal de EPRESA ENERGÍA S.A., en particular al de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

9. Terceras Partes

Las terceras partes relacionadas con EPRESA ENERGÍA S.A., dentro del alcance, firman con la empresa un acuerdo que protege la información intercambiada.

Cuando EPRESA ENERGÍA S.A., utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte, quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Esta Política será revisada para su continua adecuación anualmente por la Dirección, así como los objetivos y metas de la empresa, y comunicada a todo el personal de la organización encontrándose a disposición del público bajo solicitud de cualquier parte interesada.

Puerto Real a 9 de enero de 2024.

Gerente

Juan Enrique Núñez García