PROTOCOLO SOBRE MEDIDAS DE SEGURIDAD RECURSOS TIC

OBJETO.-

El presente protocolo tiene por objeto definir y regular la política de seguridad de la información y comunicaciones del Grupo hc energía para su aplicación en el tratamiento de los activos de tecnologías de la información y comunicaciones (activos TIC) de su titularidad o cuya gestión tenga encomendada. La Política TIC que se recoge en este documento es el marco general sobre el tratamiento de la seguridad de la información en el ámbito de la Compañía que habrá de desarrollarse posteriormente en protocolos específicos con las recomendaciones oportunas sobre el uso correcto de los sistemas de información, así como para el desarrollo de las buenas prácticas necesarias para la prevención, detección, respuesta y recuperación de la información ante incidentes de seguridad.

PRINCIPIOS DE SEGURIDAD TIC.-

La política de seguridad TIC del Grupo hc energía se desarrollará, con carácter general, de acuerdo a los siguientes principios:

a) **Principio de confidencialidad**: los activos TIC deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

b) **Principio de integridad y calidad**: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos

de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

c) **Principio de disponibilidad y continuidad**: se garantizará un alto nivel de disponibilidad en los activos TIC y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

d) **Principio de gestión del riesgo**: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC.

e) **Principio de proporcionalidad en coste**: la implantación de medidas que mitiguen los riesgos de seguridad de los activos TIC deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

f) **Principio de concienciación y formación**: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

g) **Principio de prevención**: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

h) **Principio de mejora continua**: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico del Grupo hc energía.

i) **Principio de seguridad TIC en el ciclo de vida de los activos TIC**: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

j) **Principio de función diferenciada**: la responsabilidad de la seguridad de los sistemas de tecnologías de la información y

comunicaciones estará diferenciada de la responsabilidad sobre la prestación de los servicios.

NORMAS DE USO ACTIVOS TIC.-

- Los sistemas de información y recursos TIC de hc energía puestos a disposición de los colaboradores y usuarios en general, en especial equipos, correo electrónico y acceso a redes, son para uso exclusivo de los procesos y tratamientos de las empresas del grupo por parte de los usuarios autorizados, con finalidades de gestión y administración, y no pueden usarse con otras finalidades comerciales o particulares que no estén expresamente autorizadas.

- Cada usuario es responsable del uso que haga de los recursos TIC, así como de las contraseñas o posibilidades de acceso que reciba, no pudiendo sin autorización copiar, difundir, modificar o destruir información de las empresas de hc energía, ni mantener desprotegidos equipos, soportes digitales o documentos en papel.

- El Departamento de Sistemas y Tecnología de la Información es el responsable de la administración y gestión de los recursos TIC, debiéndose autorizar por él cualquier instalación, conexión o desconexión de elementos, periféricos, aplicaciones, o herramientas informáticas del tipo que sea en el ámbito de actuación y/o de responsabilidad de hc energía. A las finalidades indicadas, se comunicarán las instrucciones de uso oportunas.

- El incumplimiento del contenido de esta norma o de las normas y procedimientos que la desarrollen puede suponer el bloqueo o suspensión de derechos de acceso del usuario, que podrá ser sancionado de acuerdo con la legislación aplicable o del régimen disciplinario interno, sin perjuicio de las posibles acciones administrativas,

civiles o penales que en su caso correspondan en función de los hechos, su tipificación y gravedad.

- Se fomentará la difusión de información y la concienciación de los usuarios, para crear una cultura de la seguridad y de la protección de la información.

- Esta norma se desarrollará en lo que fuera necesario por otras normas, procedimientos e instrucciones técnicas más detalladas. En lo que se refiere a datos personales aquellos procedimientos estarán recogidos o referenciados en el Documento de Seguridad.

- Será objeto de mejora continua el Sistema de Gestión de la Seguridad de la Información (SGSI), siguiendo la filosofía de estándares aplicables ISO / UNE, y se evaluarán periódicamente los riesgos, partiendo de la identificación de los activos relacionados, las amenazas que puedan afectar y las posibles salvaguardas a establecer, a fin de eliminar o disminuir dichos riesgos, o gestionarlos de forma adecuada.

- En cuanto a la autenticación de usuarios se usarán mecanismos fiables que exijan la identificación inequívoca y personalizada, como contraseñas robustas, certificados digitales, datos biométricos o dispositivos físicos, y los usuarios no suplantarán la identidad de otro. En todos los casos, sobre todo si la autenticación es mediante contraseñas, los datos de autenticación estarán protegidos tanto en los sistemas como cuando se transmitan y por parte del propio usuario.

- Cada usuario podrá acceder solamente a los datos y recursos de información a los que esté autorizado por quien tenga competencia para ello, para el desarrollo de sus funciones y según el principio de mínimo privilegio. Los usuarios con perfiles más amplios necesitarán autorización especial, y se revisará periódicamente por si fuera preciso actualizar su perfil.

- Solo se utilizarán, siguiendo las instrucciones y/o procedimientos autorizados por el Departamento de Tecnologías de la Información los sistemas, productos, aplicaciones, paquetes y dispositivos que permitan una seguridad adecuada, así como los cambios posteriores que se incorporen. Para el cifrado de datos se emplearán algoritmos de cifrado robustos y fiables, protegiéndose las claves de forma efectiva.

- Solamente se grabarán datos de hc energía en soportes informáticos (CDs, DVDs, tarjetas tipo SD, conectables a puertos USB...) en los casos autorizados, y los soportes no podrán sacarse de las instalaciones si no es con autorización expresa. Han de estar protegidos, reflejados en un inventario si son varios, y en un registro de salida cuando proceda, y destruyéndolo cuando no sea necesario, según la normativa de datos personales.

- Para garantizar la disponibilidad, y bajo la responsabilidad del departamento de Sistemas y Tecnologías de la información, los sistemas y conexiones serán fiables, se obtendrán copias protegidas de la información, que se almacenarán en lugares no afectados por las mismas amenazas que los sistemas primarios, y en los casos más críticos existirán sistemas alternativos de proceso, propios o ajenos, que junto con los planes y procedimientos correspondientes, puedan permitir la continuidad de las operaciones, según la criticidad de los procesos y las circunstancias surgidas.

- La red de comunicaciones estará protegida mediante cortafuegos y otros sistemas aplicables para evitar accesos no autorizados, especialmente desde el exterior de la red.

- Se podrá registrar la actividad de los usuarios, siempre de acuerdo con la normativa sobre protección de datos personales, a fin de poder monitorizar y revisar las actividades realizadas y los posibles cambios introducidos en los sistemas o referidos a los datos.

- Cuando se produzca la baja de un usuario se bloqueará o inhabilitará su cuenta de usuario, y devolverá todas las llaves e identificadores, tarjetas, y los recursos y documentos que sean de hc energía.

- Se considerará un mal uso o uso inaceptable aquella actuación del usuario que pueda afectar a la disponibilidad de un servicio, al trabajo del resto de los usuarios, a la confidencialidad y seguridad de la información o que, en general, ponga en riesgo cualquiera de las cinco dimensiones de la seguridad (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) de la información y/o de los servicios relacionados con ella. A continuación se recogen algunos ejemplos de lo que se consideran "malos usos":

    - El uso de una cuenta de usuario para lo que no se tiene autorización o bien la apropiación indebida de las credenciales (usuario y contraseña) de otro.
    - Uso de la red de hc energía para conseguir un acceso no autorizado a cualquier ordenador, servidor o aplicación.
    - Realizar alguna actuación de forma intencionada que interfiera en el funcionamiento normal de otros ordenadores, impresoras, dispositivos o redes.
    - Instalar y ejecutar de forma intencionada en cualquier ordenador o subred cualquier tipo de software que provoque el mal funcionamiento o la sobrecarga de dicho equipo o subred (malware).
    - El abuso deliberado de los recursos puestos a disposición del usuario.
    - Los intentos de saltarse medidas de protección de la información o de explotar posibles fallos de seguridad en los sistemas.
    - El no cumplimiento intencionado de las condiciones de las licencias de software o de sus derechos de autor.

- El envío de mensajes de correo con contenido faudulento, ofensivo, obsceno o amenazante.
- Ocultar o falsificar la identidad de una cuenta de usuario o de una maquina.
- El uso de los servicios de difusión de información para fines que no tengan relación con las propias del desempeño laboral o que no sean de interés para hc energía.
- Los intentos de monitorización y/o rastreo de las comunicaciones de los usuarios.
- La lectura, copia, modificación o borrado de los ficheros de otros usuarios sin la autorización expresa del propietario.

➢ Los usuarios, cuando se les solicite, deben colaborar con los administradores de sistemas, en la medida de sus posibilidades, en cualquier investigación que se haga sobre mal uso de los recursos, aportando la información que tengan y se les requiera.

➢ hc energía colaborará en la persecución de los delitos informáticos que tengan origen o destino en su infraestructura o usuarios, dando prioridad a los requerimientos que se reciban por parte de las autoridades competentes, aportando toda la información que sea posible para el esclarecimiento del incidente y todo ello dentro del marco de la legalidad vigente.

ORGANIZACIÓN Y GESTIÓN DE LA SEGURIDAD TIC.-

Siendo la Seguridad TIC un aspecto esencial en la Seguridad de la Información, entendida esta como un activo de la organización y un componente fundamental estratégico del negocio, se encomienda la labor de seguimiento, vigilancia y coordinación de las medidas aplicables en este ámbito al Comité

de Seguridad de la Información, cuyas funciones en este ámbito de actuación se concretan en:

- Definición y propuesta de objetivos, iniciativas y planes estratégicos en seguridad TIC.
- Elevación de propuestas en relación con:
    a) Disponibilidad de los recursos necesarios.
    b) Revisión de normas en materia de seguridad TIC.
- Supervisión del cumplimiento de la normativa de seguridad TIC.
- Supervisión, seguimiento e informe acerca de incidentes en elementos TIC que afecten a la seguridad de la información.