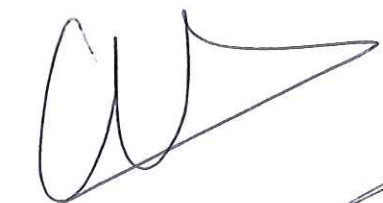
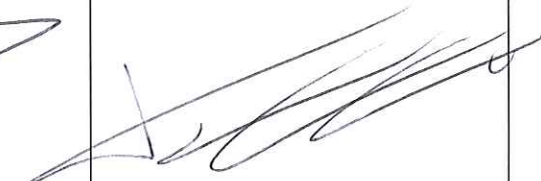


Política

SSII.SEG.01 – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistemas de Información y Procesos

REALIZADO	APROBACIÓN	APROBACIÓN
Susana Lorenzo de la Orden	Cristina Ávila García	Fernando Bergasa Cáceres
Firma: 	Firma: 	Firma: 
Fecha: 20/02/2020	Fecha:	Fecha:
Cargo:	Cargo:	Cargo:
Directora de Recursos	Consejera Directora General	Presidente Ejecutivo

Control de Versiones y Cambios del Documento						
Versiones	ELABORACIÓN	Fecha	REVISIÓN	Fecha	APROBACIÓN	Fecha
1.0	Nerea de Andrés	24/09/19		DD/MM/AA	Susana Lorenzo	20/02/20

ÍNDICE

1	APROBACIÓN Y ENTRADA EN VIGOR	4
2	INTRODUCCIÓN.....	5
2.1	PREVENCIÓN.....	5
2.2	DETECCIÓN	6
2.3	RESPUESTA.....	6
2.4	RECUPERACIÓN.....	6
3	ALCANCE	7
4	MISIÓN Y OBJETIVOS DE LA ORGANIZACIÓN.....	8
5	ORGANIZACIÓN DE LA SEGURIDAD	9
5.1	COMITÉS: FUNCIONES Y RESPONSABILIDADES	9
5.2	ROLES: FUNCIONES Y RESPONSABILIDADES	10
5.2.1	Responsable de Seguridad de la Información	10
5.2.2	Responsables de sistemas de información.....	11
5.2.3	Seguridad física	12
5.2.4	Administrador de seguridad	12
5.3	PROCEDIMIENTO DE DESIGNACIÓN	12
5.4	REVISIÓN POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	12
6	DATOS DE CARÁCTER PERSONAL.....	14
7	GESTIÓN DE RIESGOS.....	15
8	DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	16
9	OBLIGACIONES DEL PERSONAL.....	17
10	CONCIENCIACIÓN Y FORMACIÓN	18
11	TERCERAS PARTES.....	19

1 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado según tabla de aprobación en la portada del documento.

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

2 INTRODUCCIÓN

Las empresas del grupo Redexis Gas dependen 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 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, 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 las empresas del grupo deben aplicar las medidas mínimas de seguridad exigidas por el Departamento de Sistemas y Procesos, 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 departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes por ello 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.

Este documento está elaborado en base los principios básicos de seguridad, el cual establece el marco para el resto de los desarrollos normativos.

- La seguridad como un proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, reacción y recuperación.
- Líneas de defensa.
- Reevaluación periódica.
- La seguridad como función diferenciada.

2.1 PREVENCIÓN

Las empresas del grupo deben prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello las Áreas de Negocio deben implementar las medidas mínimas de seguridad determinadas por el Comité de Seguridad de la Información, 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, las empresas del grupo deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- 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, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido por el Departamento de Sistemas y Procesos de Redexis. La monitorización es especialmente relevante cuando se establecen líneas de defensa.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente, así como cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3 RESPUESTA

Redexis en todas sus sociedades y todas sus áreas debe:

- 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.

2.4 RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, Redexis en todas sus sociedades y todas sus áreas debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

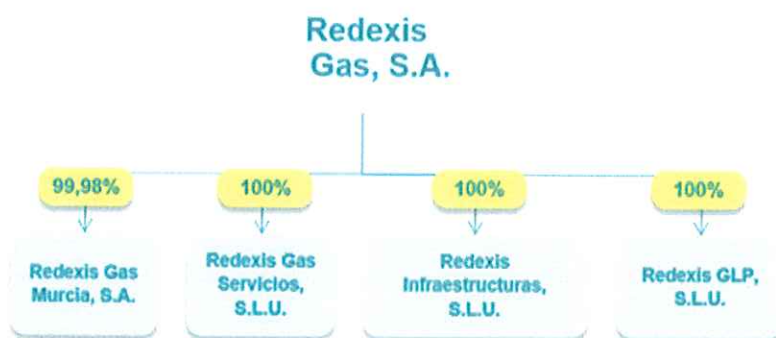
3 ALCANCE

Esta política aplica a todos los sistemas TIC de las empresas del grupo Redexis Gas y a todos los miembros de la organización en su totalidad sin ninguna excepción.

4 MISIÓN Y OBJETIVOS DE LA ORGANIZACIÓN

El grupo Redexis Gas, S.A. con sede social en Madrid, es la sociedad matriz compuesta por un conjunto de sociedades:

- Redexis Gas Murcia, S.A.
- Redexis Gas Servicios, S.L.U.
- Redexis Infraestructuras S.L.U.
- Redexis GLP S.L.U



Redexis tiene como misión ser una compañía integral de infraestructuras energéticas, maximizando el crecimiento y la eficiencia, y contribuyendo decisivamente al desarrollo sostenible y a la generación de valor para clientes, empleados y accionistas.

El grupo está dedicado al desarrollo y operación de redes de transporte y distribución de gas natural, a la distribución y comercialización de gas licuado del petróleo y a la promoción del gas natural vehicular y de aplicaciones renovables del gas natural y del hidrógeno.

5 ORGANIZACIÓN DE LA SEGURIDAD

La Organización de la Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) está constituida por las Autoridades responsables del establecimiento y aplicación de los procedimientos y normas STIC en los sistemas.

Dentro del Grupo Redexis se establecen dos tipos de estructuras STIC:

- Estructura de Supervisión: Responsable de establecer y aprobar los requisitos de seguridad para el sistema además de verificar y supervisar la correcta implementación y mantenimiento de los mismos.
- Estructura de Operación: Responsable de la implementación y mantenimiento de los requisitos de seguridad aprobados para el Sistema por el Comité de Dirección.

La estructura de Operación STIC está formada por:

- o Administradores STIC, encargados de la instalación y configuración.
- o Operadores STIC, encargados de la operación diaria.
- o Usuarios de los Sistemas

5.1 COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad TIC estará formado por representantes de la Dirección de Sistemas, entre ellos el Responsable de Seguridad de la información y por representantes de otras áreas de la organización afectadas, según se indica a continuación:

- Director de Sistemas de Información
- Responsable de Seguridad de la Información
- Otros Responsables de Alta Dirección

El Responsable de la Seguridad de la Información, ejercerá de Secretario del Comité de Seguridad TIC y tendrá como funciones:

- Convocar las reuniones del Comité STIC.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El Comité de Seguridad TIC reportará al Comité de dirección/Alta Dirección.

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.

- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- 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 tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las sociedades del grupo Redexis en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Puesto que no se trata de un comité técnico, se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas:
 - o Grupos de trabajo especializados internos, externos o mixtos.
 - o Asesoría externa.
 - o Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

5.2 ROLES: FUNCIONES Y RESPONSABILIDADES

5.2.1 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

El responsable de la Seguridad de la información es la persona designada por la Dirección de Redexis Gas, según este procedimiento. Sus funciones son:

1. Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
2. Además de ello, en caso de servicios externalizados, la responsabilidad última la tiene siempre la Organización, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, etc.) a la organización prestataria del servicio.
3. Las dos funciones principales del Responsable de la Seguridad son:

- 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.
4. Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
 5. Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
 6. Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

Redexis exigirá, de manera objetiva y no discriminatoria, que las compañías que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de la Seguridad.

Las medidas necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o de la decisión del Responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable de Sistemas de la Información que corresponda en cada caso para que adopte las medidas correctoras adecuadas.

5.2.2 RESPONSABLES DE SISTEMAS DE INFORMACIÓN

Tiene las siguientes funciones:

1. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
2. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
3. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
4. El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran al cumplimiento de los requisitos establecidos. La decisión final, que será tomada por la dirección de Redexis, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.

5.2.3 SEGURIDAD FÍSICA

1. Las medidas de protección de las instalaciones físicas pueden clasificarse en: obstáculos físicos (accesos físicos, torniquetes, puertas, candados, etc.); técnicas de vigilancia (sistemas de alarma, técnicas de vigilancia y monitorización); sistemas de inteligencia (herramientas de análisis y simulación de información basados en los datos extraídos de la monitorización); vigilantes y personal de seguridad.
2. El responsable de la Seguridad Física adoptará las medidas de seguridad que le competan, dentro de las determinadas por el Responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

5.2.4 ADMINISTRADOR DE SEGURIDAD

Sus funciones más significativas serían las siguientes:

1. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
2. 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.
3. La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
4. La aplicación de los Procedimientos Operativos de Seguridad.
5. Asegurar que los controles de seguridad establecidos son adecuadamente observados.
6. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
7. 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.
8. 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.
9. Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
10. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

5.3 PROCEDIMIENTO DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por la Alta Dirección. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

5.4 REVISIÓN POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Alta Dirección y difundida para que la conozcan todas las partes afectadas, así mismo también debe ser revisada periódicamente por Auditoría Interna y el responsable de Seguridad de la información para garantizar el cumplimiento de las normativas, la gobernanza adecuada y la alineación con las necesidades legislativas de REDEXIS y/ o cuando haya un incidente de seguridad importante o un cambio en la infraestructura organizativa o técnica.

Lo siguiente debe ser revisado y evaluado:

1. La efectividad de la política, demostrada por la naturaleza, el número y el impacto de los incidentes de seguridad registrados.
2. Costo e impacto de los controles sobre la eficiencia del negocio.
3. Efectos de los cambios en la tecnología y los impactos resultantes en el negocio.
4. Cobertura de obligaciones legales y reglamentarias.
5. Alcance sobre todos los empleados del grupo Redexis, o terceros, privacidad y prácticas regulatorias.

6 DATOS DE CARÁCTER PERSONAL

Las empresas del grupo Redexis Gas tratan datos de carácter personal. El documento con el Registro de tratamientos de todas las sociedades del grupo Redexis Gas, S.A, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información del grupo Redexis Gas 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 Documento de Seguridad realizado y actualizado por el Departamento de Jurídico.

7 GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La normativa de seguridad vigente según el documento SSII.SEG.02 – Normativa de Seguridad de la información, estará disponible en la intranet.

9 OBLIGACIONES DEL PERSONAL

Todos los empleados del grupo Redexis Gas 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 TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los empleados del grupo Redexis Gas atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los empleados del grupo Redexis Gas, en particular a los de nueva incorporación.

10 CONCIENCIACIÓN Y FORMACIÓN

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.

11 TERCERAS PARTES

Cuando las sociedades de Redexis presten servicios a otras empresas o manejen información de otras empresas, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Redexis utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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 Directores de Sistemas de la Información y los servicios afectados antes de seguir adelante.

