POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

BRUC

Contenido

1. INTRODUCCIÓN 3
2. ÁMBITO DE APLICACIÓN 3
3. ENFOQUE DE SEGURIDAD 4
4. PRINCIPIOS GENERALES 4
5. COMPROMISO DEL CONSEJO DE ADMINISTRACIÓN 4
6. OBJETIVOS ESTRATÉGICOS 5
7. MARCO DE GESTIÓN DEL RIESGO 5
8. GOBIERNO, ROLES Y RESPONSABILIDADES 5
9. GESTIÓN DE TERCEROS Y CADENA DE SUMINISTRO 6
10. CONCIENCIACIÓN, FORMACIÓN Y DEBER DE COLABORACIÓN 6
11. CUERPO NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN 7
12. SISTEMAS DE GESTIÓN DE SEGURIDAD Y RESILIENCIA 7
13. INCUMPLIMIENTO 8
14. CANAL ÉTICO 8
15. APROBACIÓN Y ENTRADA EN VIGOR 8

1. INTRODUCCIÓN

Bruc Energy, S.L. y las sociedades de su grupo empresarial ("BRUC" o el "Grupo"), conscientes de que la información constituye un activo estratégico esencial para el desarrollo de sus actividades y la prestación segura de sus servicios, promueven un enfoque integral de gestión de la seguridad de la información basado en el análisis y tratamiento de los riesgos, en línea con los principios y requisitos establecidos en normas y marcos de referencia reconocidos, incluyendo la norma ISO/IEC 27001, el Esquema Nacional de Seguridad (ENS) y la Directiva (UE) 2022/2555 (NIS2), así como en cumplimiento del Código de Conducta de BRUC y del resto de normas y políticas corporativas que resulten de aplicación.

Por este motivo, BRUC publica la presente Política General de Seguridad de la Información (en adelante "PGSI" o la "Política"), que establece los principios, criterios, responsabilidades y directrices corporativas que rigen la protección de la información, de los activos que la soportan y de los servicios dependientes de las tecnologías de la información y de operación en BRUC.

La PGSI constituye el marco rector de referencia para definir, implantar, mantener, supervisar y mejorar de forma continua las medidas técnicas, organizativas, físicas y documentales necesarias para proteger la información y los sistemas que la tratan, almacenan, transmiten o procesan, conforme a un enfoque integral y basado en riesgos, a las necesidades del negocio, a los requisitos legales, regulatorios, contractuales y sectoriales aplicables y a las buenas prácticas reconocidas en materia de seguridad de la información, continuidad de negocio y resiliencia operativa.

La presente Política se orienta a garantizar un nivel adecuado y proporcionado de protección de la información y de los servicios esenciales o relevantes para la actividad de BRUC, asegurando la capacidad de prevención, detección, respuesta, recuperación y aprendizaje ante incidentes o situaciones que puedan afectar a la seguridad de la información, a la continuidad operativa o al cumplimiento normativo.

2. ÁMBITO DE APLICACIÓN

La Política es de aplicación a todas las sociedades que integran el Grupo, así como a las sociedades participadas no integradas en el Grupo sobre las que la BRUC tiene un control efectivo, dentro de los límites legalmente establecidos. En aquellas sociedades participadas en las que esta Política no sea de aplicación, BRUC promoverá, a través de sus representantes en sus órganos de administración, el alineamiento de sus políticas propias con ésta. Además, esta Política es aplicable, en lo que proceda, a las joint ventures, uniones temporales de empresas y otras asociaciones equivalentes, cuando BRUC tenga responsabilidad fiscal en su gestión.

La PGSI resulta asimismo de aplicación a todos los trabajadores que mantengan una relación laboral con BRUC (el "Profesional" o los "Profesionales"), así como a los administradores, personal temporal, becarios, colaboradores, proveedores, contratistas, subcontratistas, clientes y cualquier tercero que, con o sin vínculo laboral con BRUC, tenga acceso a información, activos, sistemas o servicios bajo responsabilidad del Grupo, así como a todas las áreas, funciones, procesos, actividades, instalaciones, activos, sistemas, redes, plataformas y servicios bajo titularidad, responsabilidad, gestión, operación o control de BRUC, con independencia de su ubicación geográfica o del modelo de prestación del servicio.

Su alcance comprende, entre otros, los entornos IT, OT, cloud, redes corporativas, infraestructuras de comunicaciones, instalaciones físicas, servicios externalizados, soluciones tecnológicas de terceros y cualquier otro medio o soporte que intervenga en el ciclo de vida de la información.

Aquellas filiales, sucursales, plantas energéticas, centros operativos o unidades organizativas que, por necesidades locales, operativas, regulatorias o contractuales, desarrollen normativa o procedimientos específicos, deberán estar alineados con la presente Política y con el marco normativo que la desarrolla. En caso de discrepancia, prevalecerá lo dispuesto en la PGSI y la normativa corporativa, salvo que la norma local establezca exigencias más exigentes.

3. ENFOQUE DE SEGURIDAD

La información es un activo esencial para BRUC y debe ser protegida durante todo su ciclo de vida, desde su creación o recepción hasta su destrucción o conservación definitiva, mediante controles adecuados y proporcionales a su criticidad, sensibilidad, valor para el negocio, obligaciones legales y nivel de riesgo asociado.

BRUC adopta un enfoque de seguridad integral, continuo, transversal y basado en riesgos, en virtud del cual la seguridad de la información se integra en los procesos de negocio, en la gestión operativa, en el gobierno corporativo, en la gestión del cambio, en la contratación con terceros y en la toma de decisiones relevantes para el Grupo.

La seguridad de la información es una responsabilidad compartida. Todas las personas sujetas a esta Política deberán conocer, aceptar y cumplir las obligaciones de seguridad que les resulten de aplicación, utilizar de forma diligente los activos y recursos puestos a su disposición y colaborar activamente en la prevención, detección y reporte de riesgos, debilidades e incidentes. BRUC podrá monitorizar, registrar y revisar el uso de sus sistemas, redes y activos de información, así como las actividades de los usuarios, con fines de seguridad, resiliencia operativa, cumplimiento normativo y gestión de incidentes, de conformidad con la legislación y normativa aplicables.

4. PRINCIPIOS GENERALES

BRUC rige su actuación en materia de seguridad de la información conforme a los siguientes principios:

- Confidencialidad: garantía de que la información solo es accesible por personas o sistemas autorizados.
- Integridad: aseguramiento de que la información es completa, exacta y no ha sido alterada de forma no autorizada.
- Disponibilidad: garantía de que la información y los sistemas están accesibles cuando se requieren por los usuarios autorizados.
- Autenticidad: aseguramiento de que las identidades de usuarios, sistemas y datos son veraces y verificables.
- Trazabilidad: capacidad de registrar y rastrear las acciones realizadas sobre la información para su posterior análisis o auditoría.
- Conservación: aseguramiento de que la información se mantiene y protege durante el tiempo necesario, cumpliendo los requisitos legales y operativos.
- Proporcionalidad: aplicación de medidas de seguridad acordes al nivel de riesgo, evitando controles excesivos o insuficientes.
- Gestión del riesgo: identificación, análisis, evaluación y tratamiento de los riesgos que afectan a la información.
- Seguridad desde el diseño y por defecto: integración de la seguridad desde la concepción de sistemas y procesos, aplicando configuraciones seguras por defecto.
- Mejora continua: revisión y actualización permanente de las medidas de seguridad para adaptarse a nuevas amenazas y necesidades.

La interpretación y el desarrollo de dichos principios se realizará en la normativa específica que integra el cuerpo normativo de seguridad de la información de BRUC.

5. COMPROMISO DEL CONSEJO DE ADMINISTRACIÓN

El Consejo de Administración de BRUC asume el compromiso expreso de impulsar, aprobar, apoyar y supervisar la presente Política y el marco normativo que la desarrolla, promoviendo una cultura de seguridad alineada con la estrategia, el modelo de negocio y el perfil de riesgo del Grupo.

Corresponde al Consejo de Administración velar por que la seguridad de la información disponga de una gobernanza adecuada, de recursos suficientes, de responsabilidades claras y de

mecanismos eficaces de seguimiento y control, así como revisar periódicamente su eficacia y promover las acciones de mejora que resulten necesarias.

Para ello, BRUC promoverá la capacitación y concienciación necesaria de los miembros del Consejo de Administración y del personal con responsabilidades relevantes en materia de seguridad, tecnología, continuidad de negocio, operación, control, compras y gestión de terceros.

6. OBJETIVOS ESTRATÉGICOS

La presente Política persigue, como objetivos estratégicos, la protección integral de la información, los activos tecnológicos, los activos operacionales y los servicios de BRUC frente a amenazas internas y externas, deliberadas o accidentales; garantizar la continuidad y resiliencia de los procesos y servicios críticos o relevantes; alinear la seguridad con la estrategia de negocio y tecnológica; y establecer y mantener un marco eficaz de gestión de riesgos de seguridad de la información, ciberseguridad, continuidad y terceros.

Asimismo, la Política persigue prevenir, detectar, gestionar, responder y recuperarse eficazmente ante incidentes; cumplir los requisitos legales, regulatorios, contractuales y sectoriales aplicables, reforzar la seguridad en la cadena de suministro y en las relaciones con terceros, integrar la seguridad en los procesos de adquisición, diseño, desarrollo, implantación, mantenimiento y retirada de sistemas, fomentar la cultura de seguridad, garantizar la segregación de funciones y disponer de capacidades de monitorización, supervisión, auditoría y mejora continua.

7. MARCO DE GESTIÓN DEL RIESGO

BRUC establece un marco de gestión del riesgo de seguridad de la información y ciberseguridad que permita identificar, analizar, evaluar, tratar, aceptar, monitorizar, revisar y escalar de forma sistemática los riesgos que puedan afectar a la información, a los activos que la soportan y a la continuidad de los servicios.

Dicho marco abarcará, al menos, los riesgos tecnológicos, operacionales, físicos, ambientales, organizativos, legales, regulatorios, derivados de terceros, de la cadena de suministro, de la externalización de servicios, de los entornos cloud y de los sistemas de operación o industriales que resulten de aplicación en BRUC.

Las metodologías, criterios de evaluación, niveles de aceptación, responsables, periodicidades, herramientas y mecanismos de seguimiento y reporte del riesgo se desarrollarán en la normativa y procedimientos corporativos correspondientes, que formarán parte del cuerpo normativo de seguridad de la información de BRUC.

8. GOBIERNO, ROLES Y RESPONSABILIDADES

La seguridad de la información se articula conforme a un modelo de gobierno que asegura la adecuada segregación de funciones, la coordinación entre áreas, la asignación clara de responsabilidades y la supervisión independiente del marco de control.

Sin perjuicio del detalle que se establezca en la normativa de desarrollo, BRUC adopta un modelo de responsabilidad basado en tres líneas de defensa, bajo la supervisión del Consejo de Administración, como máximo órgano de gobierno y supervisión.

1. La primera línea está constituida por las unidades de negocio y áreas de soporte responsables de operar los procesos, servicios, activos y controles bajo su ámbito de responsabilidad. Estas funciones son responsables de aplicar las medidas de seguridad establecidas, identificar y gestionar los riesgos asociados a su actividad, escalar las desviaciones relevantes y reportar los incidentes, debilidades o incumplimientos que pudieran afectar a la seguridad de la información.

2. La segunda línea está constituida por las funciones corporativas con responsabilidades de definición, supervisión, control, cumplimiento y seguimiento del marco de seguridad de la información y ciberseguridad. Estas funciones actúan con el grado de independencia requerido respecto de la operación diaria, estableciendo criterios, metodologías, requisitos, mecanismos de seguimiento y procesos de validación para verificar la observancia del marco normativo interno y externo, así como para elevar a los órganos competentes las desviaciones, riesgos o deficiencias identificadas.
3. La tercera línea corresponde a Control Interno o la función independiente que BRUC determine, siempre que actúe con independencia suficiente respecto de las funciones de gestión y supervisión ordinaria. Esta tercera línea proporciona una revisión independiente y objetiva de la eficacia del modelo de gobierno, del sistema de gestión, del control interno y de la gestión de riesgos en materia de seguridad de la información y ciberseguridad.

El Consejo de Administración, como máximo órgano de gobierno y supervisión, ostenta la responsabilidad última en materia de seguridad de la información y ciberseguridad. En este sentido, es el encargado de definir y/o aprobar, según corresponda, el marco estratégico, los principios generales de seguridad y el apetito de riesgo del Grupo, asegurando la existencia de políticas, controles, capacidades y recursos adecuados. Asimismo, supervisa la correcta gestión de los riesgos relevantes y vela por que la Alta Dirección impulse medidas eficaces para prevenir, detectar, responder y recuperarse frente a incidentes de seguridad.

Adicionalmente, BRUC dispone de un Comité de Seguridad, entendido como el órgano interno responsable de la coordinación, seguimiento, priorización, reporte y escalado de las cuestiones relevantes en materia de seguridad de la información y ciberseguridad. Este Comité actúa de acuerdo con lo establecido en su reglamento de funcionamiento, donde se regulan, entre otros aspectos, su composición, periodicidad de reuniones, responsabilidades, mecanismos de decisión y canales de escalado.

9. GESTIÓN DE TERCEROS Y CADENA DE SUMINISTRO

BRUC exige a los terceros con los que se relaciona, cuando implique acceso a información, sistemas, activos, instalaciones, redes o servicios bajo su responsabilidad, medidas de seguridad adecuadas y proporcionales al nivel de riesgo, formalizadas mediante requisitos contractuales, controles de homologación, procesos de evaluación, mecanismos de seguimiento y cuando proceda, derechos de verificación o auditoría.

La gestión de los riesgos de terceros y de la cadena de suministro contemplará, entre otros aspectos, la clasificación de los servicios, la criticidad del proveedor, el grado de dependencia operativa, el tratamiento de la información, los procesos de subcontratación, las obligaciones de notificación de incidentes, la continuidad del servicio, la reversibilidad o salida ordenada y la protección de los activos de BRUC durante toda la vigencia de la relación contractual.

10. CONCIENCIACIÓN, FORMACIÓN Y DEBER DE COLABORACIÓN

BRUC promueve una cultura corporativa de seguridad mediante programas continuados de concienciación, capacitación y formación adaptados al perfil de riesgo, al nivel de responsabilidad y a las funciones desempeñadas por los distintos colectivos sujetos a esta Política.

En este sentido, BRUC establece y mantiene actividades de concienciación, capacitación y formación en materia de seguridad de la información, ciberseguridad y gestión de riesgos, dirigidas a sus profesionales, administradores y demás colectivos incluidos en el ámbito de aplicación de esta Política, de forma proporcional a sus funciones, responsabilidades y exposición al riesgo. Estas actividades tienen por objeto asegurar un nivel adecuado de conocimiento de las obligaciones aplicables, promover comportamientos seguros y reforzar la adopción de buenas prácticas en el uso, tratamiento y protección de la información y de los activos asociados

Toda persona incluida en el ámbito de aplicación de la PGSI tiene el deber de actuar diligentemente, proteger los activos de BRUC a los que tenga acceso, observar las normas e

instrucciones vigentes, comunicar sin demora cualquier debilidad, incumplimiento o incidente de seguridad del que tenga conocimiento y colaborar en las investigaciones, verificaciones y medidas de respuesta que resulten necesarias.

11. CUERPO NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN

La presente PGSI se desarrolla mediante un cuerpo normativo corporativo de seguridad de la información estructurado jerárquicamente, que permitirá trasladar los principios y mandatos de esta Política a disposiciones de mayor detalle, control y operatividad. Este marco estará alineado con el ENS y con cualquier otro requisito normativo aplicable. En particular, los documentos que conforman los niveles 2 a 4 desarrollarán e implementarán las medidas de seguridad y los controles mínimos aplicables a BRUC, incluyendo los establecidos en el Anexo II del ENS, teniendo en cuenta la categorización de los sistemas de información en función de su impacto sobre la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Dicho cuerpo normativo se organiza en distintos niveles, definidos en función de su alcance, propósito y grado de especificidad:

Nivel 1 - Política General de la Seguridad de la Información (PGSI): constituye el marco superior del cuerpo normativo de seguridad de la información, del cual dependen la totalidad de los documentos que lo integran. Se trata de un documento de carácter estratégico que formaliza y presenta, a alto nivel, los principios, directrices y compromisos en materia de seguridad de la información.

Nivel 2 - Políticas Generales (PG): desarrollan los principios establecidos en la PGSI, estableciendo las bases de los distintos dominios de seguridad. Estas políticas definen el marco de actuación y orientan la elaboración de las Normas del nivel inferior, agrupando y estructurando los diferentes ámbitos de seguridad.

Nivel 3 - Normas: establecen de forma específica los controles, requisitos y directrices que deben aplicarse para garantizar la adecuada protección de los activos de información. Cada norma se encuentra alineada con una Política General y se define considerando los dominios de seguridad y las regulaciones aplicables.

Nivel 4 - Procedimientos y documentación de soporte: incluye procedimientos, instrucciones técnicas, guías, directivas, anexos y demás documentos operativos, cuyo objetivo es detallar la implementación práctica de los controles y directrices definidos en los niveles superiores, así como generar los registros y evidencias correspondientes.

12. SISTEMAS DE GESTIÓN DE SEGURIDAD Y RESILIENCIA

Con el fin de dar soporte al cumplimiento de la presente Política y asegurar un enfoque sistemático, trazable y basado en riesgos, BRUC establecerá, mantendrá y mejorará los sistemas de gestión que resulten necesarios o adecuados en función de su contexto, modelo operativo, obligaciones regulatorias, compromisos contractuales y exposición al riesgo. Dichos sistemas de gestión se alinearán con estándares y marcos reconocidos internacionalmente en materia de seguridad de la información, continuidad de negocio, ciberseguridad, gestión de riesgos, seguridad de servicios cloud u otros ámbitos relacionados.

En particular, BRUC articulará su modelo de seguridad mediante un sistema de gestión de la seguridad de la información (SGSI), orientado a establecer el marco de gobierno, gestión de riesgos, definición de controles, seguimiento, medición, auditoría, revisión y mejora continua de la seguridad de la información. Asimismo, cuando resulte aplicable, BRUC podrá apoyarse en un sistema de gestión de continuidad de negocio (SGCN), así como en otros sistemas, marcos o metodologías complementarias que permitan reforzar la resiliencia operativa, la protección de los activos, la seguridad de los servicios externalizados y el cumplimiento de los requisitos legales, regulatorios, normativos y contractuales aplicables.

La implantación y mantenimiento de estos sistemas de gestión no sustituye el cumplimiento de la presente Política ni de la normativa que la desarrolla, sino que constituye un mecanismo estructurado para su ejecución, seguimiento, evaluación y mejora continua.

Cada sistema de gestión deberá contar, en la medida que resulte aplicable, con un alcance definido, responsabilidades asignadas, procesos documentados, indicadores, mecanismos de revisión, gestión de riesgos, tratamiento de desviaciones y evidencias suficientes para demostrar su funcionamiento efectivo.

13. INCUMPLIMIENTO

El incumplimiento de la presente Política o de la normativa que la desarrolla podrá dar lugar a la adopción de medidas correctivas, disciplinarias, contractuales, organizativas o legales, de conformidad con la normativa interna de BRUC, la legislación aplicable y las obligaciones contractuales correspondientes.

La respuesta frente al incumplimiento será proporcional a la naturaleza de los hechos, a su gravedad, intencionalidad, recurrencia, impacto efectivo o potencial, criticidad de los activos afectados y riesgo residual generado para BRUC, sus partes interesadas o sus obligaciones legales y regulatorias.

Sin perjuicio de las medidas que correspondan, todo incumplimiento relevante deberá ser analizado para identificar sus causas, valorar su impacto, definir las acciones correctoras necesarias y evitar su repetición.

14. CANAL ÉTICO

En el supuesto de que se tengan indicios razonables de la vulneración de lo dispuesto en esta Política o de que se haya producido cualquier acto contrario a la ley o a la ética empresarial que pueda afectar a BRUC, se debe comunicar dicha sospecha a BRUC a través de los canales establecidos.

A tal fin, el Grupo ha establecido el Canal Ético, un sistema de información interno a través del cual los Profesionales de BRUC, administradores, proveedores o cualquier tercero deben denunciar posibles infracciones penales o administrativas o cualquier conducta ilícita o contraria a la ética, al presente Código o a la legislación aplicable cometidas en el contexto de la actividad del Grupo.

El acceso al Canal Ético se puede realizar a través de la siguiente ruta: https://brucenergy.integrityline.com/frontpage.

Las comunicaciones efectuadas a través del Canal Ético se tramitarán de acuerdo con lo dispuesto en la Política del Canal Ético de BRUC y con las garantías reconocidas en el mismo. BRUC admite comunicaciones anónimas.

Las comunicaciones serán tratadas de forma estrictamente confidencial y no habrá ningún tipo de represalia contra el informante por el hecho de realizar la denuncia, salvo que la misma se haya realizado de mala fe, en cuyo caso BRUC podrá adoptar las medidas que considere oportunas.

15. APROBACIÓN Y ENTRADA EN VIGOR

La Política ha sido aprobada por el Consejo de Administración de BRUC el día 23 de junio de 2026, entrando en vigor el día siguiente de su aprobación y está disponible para todos los Profesionales y administradores, así como para todos los grupos de interés del Grupo a través de su página web corporativa (https://brucenergy.com/).

La presente PGSI será revisada, al menos, con periodicidad anual y adicionalmente, siempre que se produzcan cambios relevantes en el contexto de riesgo, en la estrategia del negocio, en el

Grupo, en la arquitectura tecnológica, en la normativa aplicable, en las obligaciones contractuales o en el entorno de amenazas que puedan afectar a su adecuación o eficacia.