RESOLUCIÓN DE 13 DE JULIO DE 2020, DEL PRESIDENTE DEL FROB, POR LA QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los sistemas de información del FROB, esenciales para el ejercicio de las funciones legalmente encomendadas, deben ser administrados con diligencia, adoptando las medidas de seguridad adecuadas para protegerlos frente a daños, accidentales o deliberados, que puedan afectar a su disponibilidad, así como a la integridad y confidencialidad de la información gestionada.

Procede por tanto definir una Política de seguridad de la información del FROB, como marco en el que se articule la gestión de la seguridad de sus sistemas de información desde una perspectiva estratégica, al servicio de los objetivos de esta autoridad.

En consecuencia, en virtud de lo dispuesto en el artículo 55 de la Ley 11/2015, de 18 de junio, de recuperación y resolución de entidades de crédito y empresas de servicios de inversión, el Presidente del FROB, resuelve:

Primero. Aprobación de la política de seguridad de la información del FROB.

Se aprueba la Política de seguridad de la información del FROB que se incorpora como anexo de esta resolución.

La Política de seguridad de la información se aplicará y observará por el FROB en todos sus sistemas de información y por todo su personal, así como por el personal de otros organismos o entidades que en virtud de norma legal, acuerdo o convenio tengan acceso a los sistemas de información del FROB.

Disposición final única. Entrada en vigor.

La presente resolución entrará en vigor el día siguiente al de su publicación en la sede electrónica del FROB.

Jaime Ponce Huerta

Anexo
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL FROB

1 DEFINICIÓN Y ÁMBITO DE APLICACIÓN

La Política de Seguridad de la Información (PSI) identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones.

La PSI es el instrumento en el que se apoya el FROB, autoridad de resolución ejecutiva, para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones y debe entenderse como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en el FROB.

La PSI será de obligado cumplimiento para todo el personal que acceda, tanto a los sistemas de información, como a la propia información gestionada por la entidad, con independencia de cuál sea su destino, adscripción o relación con la misma.

2 MISIÓN DEL FROB

Corresponde al FROB llevar a cabo la resolución de las entidades de crédito y empresas de servicios de inversión que resulten inviables, trabajando por la resolución más eficiente para el interés público, protegiendo la estabilidad del sistema financiero, evitando perturbaciones en la economía real y minimizando el uso de recursos públicos.

3 MARCO NORMATIVO

Junto con la legislación especial del FROB (Ley 11/2015, de 18 de junio, de recuperación y resolución de entidades de crédito y empresas de servicios de inversión), esta PSI se aplicará dentro del marco compuesto por la normativa en materia de protección de datos personales y de Administración electrónica y la Estrategia de Seguridad Nacional y la Estrategia de Ciberseguridad Nacional.

4 PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

4.1 PRINCIPIOS BÁSICOS.

Cualquier actividad relacionada con el uso de los activos de información en el FROB estará sometida a los siguientes principios básicos:

a) Alcance estratégico: la seguridad de la información estará integrada con el resto de los objetivos de la entidad para conformar un todo coherente y eficaz.
b) Proporcionalidad: el establecimiento de medidas de protección, detección y recuperación será proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
c) Mejora continua: las medidas de seguridad se evaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
d) Seguridad por defecto: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad desde su concepción.

4.2 PRINCIPIOS DE ACTUACIÓN.

Los principios básicos se concretan en un conjunto de principios de actuación:

a) Gestión de activos de información: los activos de información de la entidad se encontrarán inventariados y categorizados y estarán asociados a un responsable.
b) Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los activos de información conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
c) Seguridad física: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
d) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las tecnologías de la información y de las comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
e) Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
f) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
g) Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
h) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

i) Gestión de riesgos: debe realizarse de manera continua sobre los sistemas de información y contemplar un análisis de riesgos que evalúe los riesgos residuales y proponga tratamientos adecuados.
j) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por la normativa vigente.
k) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa en materia de seguridad de la información.

5 ORGANIZACIÓN DE LA SEGURIDAD

La seguridad de la información estará gestionada por un Comité de Dirección de Seguridad de la Información, un Comité Técnico de Seguridad de la Información y un Responsable de Seguridad.

5.1 COMITÉ DE DIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Dirección de Seguridad de la Información (CDSI) estará compuesto por los siguientes miembros:

a) Presidente: el Presidente del FROB
b) Vicepresidente: el titular de la Dirección de Administración y Control.
c) Vocales: los titulares del resto de direcciones del FROB
d) Secretaría: el responsable del departamento TIC

El CDSI ejercerá las siguientes funciones:

a) Aprobar las propuestas de modificación de la PSI.
b) Velar e impulsar el cumplimiento de la PSI.
c) Promover la mejora continua en la gestión de la seguridad de la información.
d) Aprobar el plan de auditoría y el plan de formación en materia de seguridad de la información, a propuesta del Responsable de Seguridad.
e) Resolver las cuestiones derivadas del funcionamiento de la PSI, sometidas a su consideración por el Comité Técnico de Seguridad de la Información.
f) Aprobar el informe anual de revisión de la Seguridad de la Información elaborado por el Responsable de Seguridad.
g) Nombrar al Responsable de Seguridad.

5.2 COMITÉ TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN

El Comité Técnico de Seguridad de la Información (CTSI) estará compuesto por los siguientes miembros:

a) Presidencia: el Responsable de la Seguridad de la Información.
b) Vocalías: representantes de cada una de las direcciones a propuesta de su titular.

c) Secretaría: representante del departamento TIC.

El CTSI ejercerá las siguientes funciones:

a) Elaborar estudios, análisis previos y propuestas de modificación y actualización de la PSI.
b) Aprobar las normas de desarrollo de la PSI.
c) Examinar el cumplimiento de la PSI y sus normas de desarrollo.
d) Seguimiento de las medidas de seguridad adoptadas resultado del análisis y gestión de riesgos de los activos.
e) Examinar las actividades de concienciación y formación en materia de seguridad, y, en su caso, realizar las propuestas que correspondan.

5.3 RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN

El Responsable de Seguridad de la Información es la persona que detecta las necesidades y toma las decisiones operativas para satisfacer los requisitos de seguridad de la información y de los servicios.

Serán funciones del Responsable de Seguridad de la Información, dentro del ámbito de actuación enunciado con anterioridad, las siguientes:

a) Adoptar las medidas de seguridad resultado del análisis y gestión de riesgos de los activos.
b) Elaborar estudios, análisis previos y propuestas de normativa de seguridad.
c) Seguimiento operativo del cumplimiento de las normas de seguridad.
d) Asegurar que la documentación de seguridad se mantiene organizada y actualizada, y gestionar los mecanismos de acceso a la misma.
e) Implantar la mejora continua en la gestión de la seguridad de la información.
f) Gestionar los incidentes de seguridad de la información que se produzcan.
g) Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.
h) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, que habrán de estar previstas en el plan de auditoría previamente aprobado por el CDSI.
i) Elaborar un Informe anual de revisión de la Seguridad de la Información para su aprobación por el CDSI.
j) Impulsar la formación y concienciación en materia de seguridad de la información.
k) Cualquier otra función precisa para satisfacer los requisitos de seguridad de la información y de los servicios asociados, siempre supeditada al conocimiento y conformidad del CDSI.

6 RESPONSABILIDADES DEL PERSONAL. FORMACIÓN Y CONCIENCIACIÓN

Los datos e informaciones del FROB, cualquiera que sea su soporte, serán de uso exclusivamente reservado para el cumplimiento de los fines que le atribuye el ordenamiento jurídico. Las autoridades, empleados públicos y demás personal que por razón de su cargo o

función tuviesen conocimiento de dichos datos se encontrarán obligados a guardar sigilo riguroso y observar estricto secreto respecto de los mismos de conformidad con lo previsto en el artículo 59 de la Ley 11/2015.

El personal autorizado sólo deberá acceder a aquellos datos e información que deba conocer por razones del servicio, debiendo abstenerse de hacerlo por cualquier otra motivación. Asimismo, será responsable de todos los accesos que se realicen mediante el uso de sus credenciales de identificación lógica de usuario. A tal fin deberá mantener la custodia y secreto de las credenciales, así como vigilar posibles usos ajenos, denunciando cualquier trasgresión. En ningún caso deberá facilitar las credenciales a otra persona, ni deberá acceder a la información utilizando credenciales ajenas, incluso disponiendo del consentimiento del usuario titular.

El acceso a los datos e información del FROB por una persona no autorizada, la realización de transacciones digitales que no estén relacionadas con un objetivo concreto de gestión, la asignación de perfiles de utilización a otras personas para la realización de transacciones no necesarias para la gestión que tengan encomendada, o la revelación o falta de diligencia en la custodia y secreto de sus credenciales podrá dar lugar a la exigencia de las responsabilidades administrativas o de otra naturaleza en que se hubiese podido incurrir y a la supresión de las autorizaciones previamente concedidas por quien las hubiera otorgado en su momento.

Todos los miembros del FROB tienen la obligación de conocer y cumplir esta PSI, así como la normativa de seguridad que la desarrolle y, en consecuencia, deberán ser formados e informados de sus deberes y obligaciones en materia de seguridad. 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 la realización de su trabajo.

7 GESTIÓN DE RIESGOS

La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y su evaluación periódica.

El análisis de riesgos permite conocer el estado actual del riesgo tras el cual, dentro de la etapa de gestión del riesgo, se establecerán los niveles de riesgo máximo aceptados por la organización, procediendo a identificar los controles y salvaguardas necesarios para reducir el riesgo por debajo de dichos niveles.

La selección de las medidas de seguridad a aplicar para minimizar los riesgos localizados será realizada por el Responsable de Seguridad de la Información. Anualmente se procederá a la revisión de su adecuación elevando informe al CDSI.

8 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La PSI regulada en esta resolución se desarrollará mediante las oportunas normas, así como mediante los procedimientos, guías e instrucciones técnicas orientadas a la aplicación e instrumentación de medidas de seguridad en el desarrollo, mantenimiento y explotación de los sistemas de información.

9 PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En lo referente a los datos de carácter personal que sean objeto de tratamiento por parte del FROB, se adoptarán las medidas técnicas y organizativas que corresponda implantar atendiendo a la normativa de protección de datos vigente y a los riesgos derivados del propio tratamiento. Todo ello, de acuerdo con 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 ("Reglamento General de Protección de Datos"), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por su parte, el Delegado de Protección de Datos ejercerá las funciones recogidas en la normativa de protección de datos y supervisará que la normativa de seguridad de la información del FROB se adecúa a la misma.

10 RELACIÓN CON TERCEROS

En los casos en que el FROB utilice servicios de terceros o les ceda información, se les hará partícipes de esta PSI y de la normativa de seguridad que afecte a dichos servicios o información. Los terceros quedarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para cumplirla. Además se establecerán procedimientos específicos de reporte y resolución de incidencias y se garantizará que este personal esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

En los casos en que el FROB preste servicios o gestione información de otros organismos se les hará partícipe de la presente PSI, estableciendo canales para el reporte y coordinación de los respectivos Comités de seguridad y, en su caso, procedimientos de actuación para la reacción ante los ciberincidentes de seguridad.

Cuando algún aspecto de la política no pueda ser abordado según se establece en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos, para el conocimiento y toma de decisión, en su caso, del CDSI.