**Circular Externa**

29 de abril del 2022

SGF-0906-2022

A80/0-751

SP-438-2022

**Dirigida a:**

**Supervisados por SUGEF**

* Bancos Comerciales del Estado
* Bancos Creados por Leyes Especiales
* Bancos Privados
* Empresas Financieras no Bancarias
* Otras Entidades Financieras
* Organizaciones Cooperativas de Ahorro y Crédito
* Entidades Autorizadas del Sistema Financiera Nacional para la Vivienda

**Supervisados por SUGEVAL:**

* Puestos de Bolsa
* Sociedades Administradoras de Fondos de Inversión
* Sociedades Titularizadoras
* Sociedades Fiduciarias
* Proveedores de precios
* Bolsas de Valores
* Centrales de Valores

**Regulados por SUPEN**

* Operadoras de Pensiones
* Organizaciones sociales autorizadas para administrar los fondos de capitalización laboral
* Entidades administradoras de regímenes de pensiones sustitutas o complementarias del régimen de invalidez, vejez y muerte (IVM), creados por leyes o convenciones colectivas.

**Asunto:** Cuestionario sobre Ciberseguridad.

**Las Superintendencias Generales**

**Considerando que:**

* 1. En el 2015, Costa Rica puso en marcha la Estrategia Nacional de Ciberseguridad con el fin de mejorar las capacidades de instituciones y retos para posicionar al país en materia de ciberseguridad. El proyecto surgió de los resultados de estudios internacionales y los lineamientos del Plan Nacional de Desarrollo 2014-2018 y el Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021. La estrategia buscó contar con el apoyo y la participación de entidades tanto públicas como privadas, así como de organizaciones no gubernamentales, comunidad técnica, academia y sociedad civil. Uno de los objetivos de la estrategia es la implementación de mejores prácticas y definición de requisitos mínimos de seguridad de la información en el Sector Financiero.
	2. Desde el 2009 el CONASSIF definió el Marco de Gestión de Tecnología de Información (MGTI), siguiendo las buenas prácticas internacionales (COBIT de ISACA). Con esto se implementó un conjunto de procesos destinados a gestionar la Tecnología de Información (TI), que la entidad supervisada debía adoptar como referencia para la gestión integral de sus riesgos tecnológicos, considerando su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y la dependencia tecnológica. Dicho marco reglamentario fue adoptado inicialmente por SUGEF y luego como norma transversal por el resto de las superintendencias (SUGEVAL, SUPEN, SUGESE) en el 2017. El MGTI, junto con la implementación del modelo de Supervisión Basada en Riesgos (SBR), ha permitido una evaluación integral de la actividad de la tecnología de información en las entidades supervisadas y así, evaluar de forma transparente la gobernanza de TI y su gestión de seguridad de la información.
	3. En los últimos días diversas instituciones públicas y empresas privadas costarricenses han visto afectadas sus operaciones habituales por efectos de ciberataques a sus sistemas y herramientas de tecnología de información, lo cual demuestra la dependencia de las tecnologías de información de nuestra sociedad, y la importancia en los diversos sectores y actividades económicas, de crear y mantener sistemas y herramientas tecnológicas que minimicen el impacto del riesgo de ciberataques y establecer medidas de protección y prevención oportunas.
	4. Ante estos eventos, resulta oportuno realizar un estudio horizontal en el sector financiero supervisado, con el objetivo de determinar el estado actual de la gestión de riesgos de ciberseguridad en las entidades supervisadas, que permita identificar los elementos relevantes para mejorar y racionalizar en los próximos meses y años la gestión de los riesgos generados por los ciberataques a los que se enfrentan las entidades financieras, y brinde los insumos necesarios para la valoración y el establecimiento de normas específicas y la coordinación del trabajo de supervisión y comunicación con la industria sobre la Ciberseguridad.

**Dispone:**

1. Remitir un cuestionario sobre ciberseguridad a las entidades supervisadas por SUGEF, SUGEVAL y SUPEN. Para el caso de las entidades supervisadas por la SUGESE, no se requiere que completen la citada encuesta, dado que, durante el 2021 se les remitió una encuesta sobre ciberseguridad.
2. Informar que, la herramienta que se utilizará para recibir las respuestas al cuestionario será mediante *Microsoft FORMS.*
3. Informar que, en un plazo máximo de **diez días hábiles**, contados a partir del día hábil siguiente del recibo de esta comunicación, deberán enviar sus respuestas mediante el siguiente enlace: [Cuestionario sobre Ciberseguridad](https://forms.office.com/Pages/ResponsePage.aspx?id=RQqNYaYlGEafgI9wpDXuUjVO-6c3wNtHrI4oPmQlCShUOUw1VVZDVzBaUDY4S0tPTUk5UDdIWEdVNi4u).
4. Asimismo, el correo electrónico normativaenconsulta@sugef.fi.cr será utilizado **únicamente** como mecanismo de notificación sobre la completitud de dicho formulario.

Atentamente,



|  |  |  |
| --- | --- | --- |
| María del Rocío Aguilar MontoyaSuperintendente General |  | Luis González Aguilar Intendente General a.i. |
| **Superintendencia General de Entidades Financieras (SUGEF)** |  | **Superintendencia General de Valores (SUGEVAL)** |
| **Superintendencia de Pensiones (SUPEN)** |  |  |

**JSC/RSC/APU/GAA/JBA/gvl\***