Certificación de Seguridad de la Información y Ciberseguridad

La Sociedad SET-ICAP SECURITIES, en adelante La Sociedad,

Certifica que:

En su calidad de proveedor de infraestructura y entidad financiera con licencia de la Superintendencia Financiera de Colombia cumple con lo establecido en la Circular Externa 007 de junio 2018 en la que se establecen los requisitos mínimos para la gestión de los riesgos de ciberseguridad y seguridad de la información. Al respecto, el representante legal de Set Icap certifica que:

- SET-ICAP S.A. cuenta con un sistema de gestión de ciberseguridad y seguridad de la información.
- SET-ICAP S.A. cuenta con políticas y procedimientos para la seguridad de la información, aprobados por la dirección, publicadas y comunicadas a los empleados y a las partes interesadas.
- Tiene definida la estructura organizacional de seguridad de la información, que incluye entre otros, los roles y responsabilidades para la seguridad de la información.
- Se tiene identificadas las amenazas que puedan materializar algún riesgo para la sociedad.
- Existe segregación de funciones en la sociedad en materia de Seguridad de la información y ciberseguridad.
- Cuenta con un modelo para integrar la seguridad de la información dentro del proceso de gestión de proyectos.
- Existe un procedimiento para la selección y contratación de recurso humano.
- Se cuenta con una política de confidencialidad de la información la cual se da a conocer al momento de la contratación de un funcionario o de un proveedor externo.
- Cuenta con programas de educación y formación para los empleados y terceros, relacionados con la cultura de seguridad.
- Tiene implementado y comunicado un proceso formal para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información
- Tiene un proceso de planeación y ejecución de auditorías a procesos, infraestructura tecnológica, ciberseguridad y seguridad de la información.
- Sobre los hallazgos encontrados por las auditorias, se aplican planes de acción y son tramitados en su totalidad.
- Cuenta con procesos implementados para inventariar y clasificar la información que es gestionada dentro de la sociedad de acuerdo con su criticidad.

- Sobre los activos de información se tienen identificados los riesgos y se establecen controles para mitigarlos.
- Garantiza que los empleados y terceros devuelvan todos los activos asignados, al terminar su empleo, contrato o acuerdo.
- Tiene identificados y clasificados los activos de información de la sociedad.
- Tiene un procedimiento de borrado seguro.
- Tiene un procedimiento de control de acceso lógico y físico que protege el hardware y software que contienen información del servicio contratado
- El acceso de los usuarios a la red y a los sistemas está restringido exclusivamente a los que han sido autorizados específicamente.
- Tiene implementado un proceso formal de creación, revocación y cancelación de usuarios.
- Cuenta con un proceso para retirar los derechos de acceso de todos los empleados y terceros a la información y a las instalaciones de procesamiento de información al terminar su empleo, contrato o acuerdo.
- Tiene controles de seguridad física para proteger áreas o instalaciones donde se maneje información confidencial.
- Aplica controles de seguridad sobre los medios de almacenamiento antes de su destrucción o reúso para garantizar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito.
- Cuenta con una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de escritorio limpio en las instalaciones de procesamiento de información.
- Tiene separados los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso o cambios no autorizados.
- Tiene implementados y revisa regularmente los registros de actividades de los usuarios, excepciones, fallas y eventos de seguridad.
- Cuenta con procedimientos para controlar la instalación de software en sistemas operativos.
- Tiene controles de seguridad en la red de datos que utiliza para proteger la información.
- Posee protocolos de seguridad implementados para la transferencia segura de información.
- Cuenta con un procedimiento de mantenimiento preventivo a la infraestructura tecnológica.
- Cuenta con estándares para el desarrollo seguro de software.
- Realiza pruebas de seguridad sobre los sistemas antes de la puesta en producción.
- Establece requisitos de seguridad de la información para proveedores que puedan tener acceso, procesen, almacenen, o suministren componentes de TI para la sociedad.
- Realiza seguimiento, revisa y audita con regularidad la prestación de servicios de sus proveedores.

- Posee un procedimiento para asegurar la respuesta eficaz a incidentes de ciberseguridad y seguridad de la información.
- Posee un procedimiento de reporte de incidentes o ataques cibernéticos.
- Realiza actividades de prevención y mejoras en ciberseguridad.
- Realiza Análisis y gestión de vulnerabilidades a plataformas críticas.
- Cuenta con procedimientos para la adquisición desarrollo y mantenimiento de sistemas.
- Cuenta con procedimientos de destrucción segura de información y conservación de evidencia digital.
- Cuenta con políticas de privacidad y protección de datos personales.
- Cumple con requisitos de seguridad exigidos por la normatividad y las regulaciones nacionales e internacionales del sector financiero, dentro del servicio contratado.

.

La presente certificación se expide en Bogotá, el 22 de marzo de 2024.

Cordialmente,

FRANZ CHAMORRO ALVAREZ
Gerente de Tecnología