AGCE FINANCIAL GROUP
Servicios Financieros

POLÍTICA

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Año: 2023

EDICIÓN

AGCE FINANCIAL GROUP SPA

AGCE FINANCIAL GROUP
Servicios Financieros

Contenido

AGCE Financial Group SpA
13 norte #853, Oficina 803, Viña del Mar, V Región, Chile
https://www.agcegroup.cl/

1. INTRODUCCIÓN

La Seguridad de la Información es parte de la gestión del Riesgo Operacional de AGCE Financial Group SpA y se refiere a la gestión preventiva y reactiva de aquellos riesgos y eventos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información manejada por AGCE y que potencialmente pueda derivar en pérdidas económicas para la empresa o sus clientes.

Se entiende por Ciberseguridad todas aquellas acciones para la protección de los activos de información presentes en el ciberespacio y en los diversos medios digitales, así como de la infraestructura que los soporta; que tiene por objeto evitar, mitigar, controlar o transferir los efectos adversos de sus riesgos, amenazas y vulnerabilidades que puedan exponer a AGCE.

1.1 OBJETIVO

Definir el marco global para la gestión de la Seguridad de la Información y Ciberseguridad en AGCE, estableciendo los lineamientos para la protección y preservación de la confidencialidad, integridad y disponibilidad de la información de AGCE y de sus clientes en forma consistente con las estrategias de la Empresa.

1.2 ALCANCE

Esta política aplica a AGCE Financial Group SpA. La empresa deberá desarrollar e implementar su política interna, homologable a la presente, ajustada a sus particularidades y aprobada por su gerencia. AGCE instará para dicho desarrollo e implementación.

En adelante, esta política se referirá a AGCE.

El cumplimiento de esta Política es parte de las responsabilidades de todo el personal con independencia de su relación laboral tanto para colaboradores de AGCE como para terceros que tengan acceso a los activos de información del AGCE y/o a la infraestructura que los soporta.

1.3 PROPIETARIOS

Esta política forma parte del conjunto de políticas que pertenecen a la Gerencia de Riesgo Tecnológico.

La coordinación necesaria para la actualización de esta Política, así como el velar por el cumplimiento de la misma, es parte de las responsabilidades y funciones del área de riesgo tecnológico de AGCE.

1.4 VIGENCIA Y REVISIÓN

La presente política se revisará anualmente. No obstante lo anterior, si algún evento interno o externo afectara a los procedimientos, estructuras o los lineamientos previamente establecidos, se deberá realizar su revisión y cualquier modificación que se estime conveniente introducir, deberá contar con la aprobación previa del área de Riesgo Operacional y la posterior ratificación de gerencia de AGCE.

1.5 TERMINOLOGÍA Y DEFINICIONES

Activo: Aquello que tiene valor para la organización y por lo tanto debe protegerse. (Ej. Aplicativos, documentos, bases de datos, redes, entre otros).

Activo de información: Corresponde a los activos del tipo aplicaciones locales (no administrados por tecnología e infraestructura), documentos (físicos y electrónicos), medios de almacenamiento portátiles.

Activo tecnológico: Corresponde a los activos del tipo aplicaciones, servidores, middleware, bases de datos, redes, infraestructura de seguridad, entre otros activos.

Seguridad de la información: La Seguridad de la Información es parte de la naturaleza del riesgo operacional de AGCE, la cual se refiere a la gestión preventiva y reactiva de aquellos riesgos y eventos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información manejada por AGCE y que potencialmente pueda derivar en pérdidas económicas para la Empresa o sus clientes.

Ciberseguridad: Es la práctica de proteger redes, dispositivos y activos de información de accesos no autorizados y uso criminal, asegurando la confidencialidad, integridad y disponibilidad de la información.

2. ROLES Y RESPONSABILIDADES

AGCE mantendrá una estructura adecuada para dar cumplimiento a la Política de Seguridad de la Información y Ciberseguridad para realizar una gestión eficaz de los riesgos en esta materia. Dicha estructura incluye al área de Riesgo Operacional.

2.1 ESTRUCTURA Y ÁREAS FUNCIONALES

Las principales responsabilidades de la Gerencia en materia de Ciberseguridad, son:

- Ratificar estrategias, objetivos, políticas, estructura funcional, procedimientos y modelo de Ciberseguridad.
- Ratificar, por lo menos una vez al año, el nivel de tolerancia y apetito al riesgo de Ciberseguridad que el AGCE está dispuesto a asumir, siendo consistente con el volumen y la complejidad del negocio.
- Garantizar una adecuada implantación del modelo de gestión de riesgo de Ciberseguridad en AGCE y un adecuado entendimiento por toda la organización.
- Tomar conocimiento sobre los principales riesgos de Ciberseguridad de AGCE y monitorear el grado de avance de los planes de acción.

Gerencia de Riesgo Tecnológico

- Centralizar, procesar y realizar gestión sobre la información generada a través de la gestión de riesgo de seguridad de la información.
- Mantener informado a las autoridades responsables de supervisar los niveles de riesgo de seguridad de la información y tecnología.
- Coordinar con las diferentes áreas del AGCE el proceso de planeación, implementación, monitoreo, chequeo, revisión, mantención, difusión y mejora continua de la gestión de riesgo de seguridad de la información.
- Apoyar y realizar seguimiento al cumplimiento de las políticas y normas de seguridad de la información.
- Representar las responsabilidades y funciones del área de Seguridad de la Información.

AGCE Financial Group SpA
13 norte #853, Oficina 803, Viña del Mar, V Región, Chile
https://www.agcegroup.cl/

Área de Seguridad de la Información

- Generar y proponer el plan de seguridad de la información del AGCE, en conjunto con la División de Ciberseguridad.
- Impulsar las políticas, normas y procedimientos de seguridad de la información basado en las leyes y regulaciones locales vigentes, mejores prácticas de mercado y necesidades del negocio.
- Proponer, organizar y supervisar el plan de capacitación y sensibilización de seguridad de la información para los colaboradores de AGCE.
- Realizar seguimiento al plan de seguridad de la información a través de la matriz de seguridad y generar nuevas iniciativas de seguridad de la información
- Comunicar e involucrar a la organización en las iniciativas de seguridad la Información a fin de asegurar su efectiva implementación a nivel del AGCE.
- Analizar el riesgo asociado a la implementación de los distintos proyectos, productos y servicios y entregar las recomendaciones para el tratamiento de riesgos y vulnerabilidades.
- Apoyar en la definición, desarrollo e implementación de planes de mejoras en el ámbito de seguridad de la información para los distintos procesos, productos y servicios en la organización.
- Mantener informado a las gerencias y comités responsables de supervisar los niveles de riesgo de seguridad de la información y tecnología.
- Manejar una visión integral de la seguridad de la información de AGCE, teniendo roles y responsabilidades en otras políticas relacionadas a seguridad de la información.
- Controlar la Seguridad de la Información de AGCE en sus diferentes procesos y ámbitos descritos en la Normativa de Seguridad de la Información.
- Coordinar pruebas de escenarios de Ciberseguridad

División de Ciberseguridad

- Gestionar la formulación y ejecución del plan estratégico de Ciberseguridad, en línea con los objetivos del negocio y conforme al marco normativo, legal y regulatorio, en conjunto con el ISO.
- Gestionar la adopción del marco normativo de ciberseguridad de AGCE por parte de terceros prestadores de servicios.
- Asegurar el cumplimiento de la estrategia de Ciberseguridad definida por la organización, así como de las políticas, normas y procedimientos en este ámbito.
- Desarrollar la cultura de Ciberseguridad y entregar los conocimientos que permitan identificar ciberamenazas que pongan en riesgo la información y los activos de AGCE.
- Detectar las amenazas y gestionar los incidentes de Ciberseguridad de manera oportuna, con el objetivo de proteger la infraestructura,

AGCE Financial Group SpA
13 norte #853, Oficina 803, Viña del Mar, V Región, Chile
https://www.agcegroup.cl/

los servicios y operaciones de AGCE.

- Maximizar el uso de las tecnologías de protección existentes e incorporar nuevas.
- Proteger los datos y activos de información de AGCE y sus clientes de las ciberamenazas existentes, bajo los lineamientos del área de Seguridad y los resultados de los análisis de riesgo.
- Definir y mantener la Arquitectura de Ciberseguridad de AGCE.
- Adquirir y analizar información para identificar, rastrear, predecir y contrarrestar intenciones y actividades de ciberatacantes.
- Apoyo en la gestión y control de fraudes.
- Administrar y monitorear el correcto funcionamiento de las herramientas tecnológicas de seguridad implantadas en ambientes de tecnológicos.
- Ejecutar el proceso de revisión de facultades para mantener o eliminar los accesos a los aplicativos administrables.
- Controlar, administrar y monitorear los accesos y privilegios de usuarios.

Gerentes unidades organizacionales

- Asegurar el cumplimiento de la Política al interior del área, y tomar conocimiento de las políticas en incumplimiento y excepciones.
- Velar por la protección de la confidencialidad, integridad y disponibilidad de la información que se procese, transmita y almacene en los procesos y los ámbitos bajo su responsabilidad.

Área de seguridad y prevención de riesgos laborales

- Coordina en conjunto con el Área de Seguridad de la Información las actividades y revisiones orientadas al cumplimiento de la Norma Sobre Puesto de Trabajo Seguro.

AGCE Financial Group SpA
13 norte #853, Oficina 803, Viña del Mar, V Región, Chile
https://www.agcegroup.cl/

3. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Los procedimientos documentados que establezcan y mantengan las unidades deben considerar controles que aseguren que la información de AGCE está protegida de acuerdo a lo establecido en la Normativa de Seguridad de la Información.

En esta Normativa se establecen los requisitos mínimos de seguridad de la información y ciberseguridad que todas las unidades organizacionales de AGCE deben cumplir. Dicha normativa deberá a lo menos abordar:

Gestión de las políticas de seguridad

Se deberá garantizar la revisión periódica de las normas de seguridad (al menos una vez por año calendario), así como garantizar la existencia de mecanismos de difusión y educación enAGCE.

Organización de la seguridad de información

Se deberán definir las responsabilidades específicas en materia de seguridad de la información de las diferentes unidades internas, considerando: la responsabilidad de las unidades de negocios en relación con el cumplimiento de las políticas y normas de seguridad.

Seguridad de los recursos humanos

Se deberán establecer requerimientos y responsabilidades en relación a la gestión de la seguridad de la información para la contratación (antes del empleo), el desarrollo (durante el empleo) y el término o cambio de funciones.
Dichos requerimientos deberán estar alineados con las políticas y normas aplicables en materia de la gestión de los recursos humanos de AGCE.

AGCE Financial Group SpA
13 norte #853, Oficina 803, Viña del Mar, V Región, Chile
https://www.agcegroup.cl/

Gestión de activos

Se deberá considerar la existencia de un inventario y responsables de activos tecnológicos (aplicaciones e infraestructura) así como procesos para mantenerlos.
Se deberá considerar una definición y caracterización para la identificación, priorización y clasificación de los activos con el objetivo de proteger su confidencialidad, integridad y disponibilidad.
Se deberá considerar una metodología para la gestión de la seguridad para los activos expuestos al ciberespacio.

Control de accesos

Se deberán establecer procesos y requisitos en relación a:

- Establecer las responsabilidades del usuario en relación al uso de claves y de sus dispositivos electrónicos (estación de trabajo, notebook u otro asignado).
- Gestión de accesos de usuario que establezca procedimientos para la identificación, asignación y revisión de privilegios.
- Control de acceso a redes considerando la segregación de las redes y la limitación de la conectividad de red al máximo posible.
- Control de acceso a los sistemas operativos considerando estándares para la definición y mantención de claves.
- Control de acceso a las aplicaciones e información considerando el perfilado de dichos accesos.
- Controles de movilidad y teletrabajo.

Criptografía

Se deberán establecer procesos y requisitos en relación a:

- Aprobación e implementación de algoritmos criptográficos para la protección de la información.
- Controles de seguridad sobre llaves criptográficas.

Seguridad física y del ambiente

Se deberán establecer requisitos sobre definiciones y normas para sectores o de áreas restringidas de instalaciones físicas, perímetros de seguridad, seguridad en el control de acceso, sistemas de alarmas de protección ante amenazas.

Dichos requerimientos deberán establecer medidas adicionales de seguridad para centros decómputo y comunicaciones.

AGCE Financial Group SpA
13 norte #853, Oficina 803, Viña del Mar, V Región, Chile
https://www.agcegroup.cl/

Seguridad de las operaciones

Se deberán establecer requisitos con respecto a lo menos:

- La operación tecnológica debe incorporar una correcta segregación de funciones entre los ambientes de desarrollo, prueba (QA) y producción.
- Controles de seguridad contra software malicioso.
- Controles para el uso de medios de almacenamiento.
- Monitoreo y auditoría de las actividades realizadas sobre la red y sobre los sistemas.

Seguridad de las comunicaciones

Se deberán establecer requisitos con respecto a lo menos:

- Controles de seguridad con respecto a las redes de comunicación (firewall, firewall aplicativos, IPS (sistemas de prevención de intrusos), entre otros.
- Controles para el acceso de terceros autorizados a la red.
- Controles para la realización de servicios de comercio electrónico.
- Monitoreo y auditoría de las actividades realizadas sobre la red y sobre los sistemas.

Adquisición, desarrollo y mantenimiento de sistemas

Se deberán considerar, para el desarrollo y mantenimiento de sistemas participación y/o requerimientos de seguridad, en particular para aplicaciones del tipo web y de alta transaccionalidad, que aseguren aspectos tales como el correcto procesamiento en las aplicaciones, la aplicación de controles criptográficos (cuando aplique), la seguridad de los archivos de sistemas, la seguridad durante el proceso de desarrollo y soporte. Adicionalmente y de acuerdo a la criticidad de los servicios, se deberán realizar pruebas tendientes a identificar las potenciales vulnerabilidades en servidores, aplicaciones y contenidos asociados.

AGCE Financial Group SpA
13 norte #853, Oficina 803, Viña del Mar, V Región, Chile
https://www.agcegroup.cl/

Relación con proveedores

En relación a entidades externas (seguridad de la información en relación a proveedores) se deberán considerar requerimientos que permitan identificar los riesgos derivados de la externalización y los controles dispuestos para mitigarlos.
Se deberán establecer mecanismos de control para el manejo de información en proveedores críticos.

Lo anterior en concordancia con lo definido en las políticas de Riesgo Operacional, Administración y Selección de Proveedores y Externalización de Servicios, y Normativa de Ciberseguridad para Proveedores.

Gestión de Incidentes de seguridad de la información

Se deberá mantener registro de incidentes, eventos y vulnerabilidades. Adicionalmente deberán estar definidos los procesos y equipos de respuesta a un evento de seguridad, así como para el análisis forense de los incidentes de seguridad relevantes tendientes a identificar la causa raíz y establecer planes de acción en los casos que sea necesario Se deberán considerar pruebas ante amenazas de Ciberseguridad.

Cumplimiento

Todas las unidades de AGCE son responsables del cumplimiento de esta política, y en particular las Divisiones de Ciberseguridad y Operaciones y Tecnología. La División de Control Global de Riesgos revisará periódicamente (al menos una vez por año) las prácticas de seguridad de la información, en relación al cumplimiento de la presente política.

4. EXCEPCIÓN

En caso de ser necesario realizar una desviación o incumplimiento a la presente política, se deberá cumplir el procedimiento de excepción definido por la Gerencia de Riesgo Operacional. Se asignará un plazo de vigencia conforme al riesgo asociado, luego el nivel de exposición al riesgo debe ser nuevamente evaluado y autorizado. Sin perjuicio de lo anterior, la excepción no podrá tener una duración superior a un año.

AGCE Financial Group SpA
13 norte #853, Oficina 803, Viña del Mar, V Región, Chile
https://www.agcegroup.cl/