

MANUAL DE ROLES Y RESPONSABILIDADES

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: GTD/SECURESOFT	Nombre: Gabriel Cayupan	Nombre: Roberto Maldonado
Cargo: Proveedor Ciberseguridad externo	Cargo: Jefe de Infraestructura, Redes y Soporte	Cargo: CTO Vantrust.

	Manual de roles y responsabilidades	Revisión 01 Página 2 de 7 Fecha de Aprobación: 31/01/2023
---	--	--

I. Control de revisión

Nº Rev.	Descripción	Fecha.
01	Versión inicial	31/01/2023
02	Revisado sin cambios de fondos.	24/04/2024

	Manual de roles y responsabilidades	Revisión 01 Página 3 de 7 Fecha de Aprobación: 31/01/2023
---	--	--

II. Tabla de Contenido

I. Control de revisión	2
II. Tabla de Contenido.....	3
1 OBJETIVO	3
2 ALCANCE	3
3 ROLES Y RESPONSABILIDADES	4
3.1 Comité de Seguridad de la Información	4
3.2 CTO Corporativo Vantrust	4
3.3 Oficial de seguridad de la Información	4
3.4 Auditor Líder.....	4
3.5 Auditor Interno.....	5
3.6 Auditado.....	5
3.7 Propietario de la Información.....	5
3.8 Custodio de la Información	5
3.9 Usuario.....	6
3.10 Gestor de Monitoreo	6
3.11 Gestor de Soporte y Administración	6
3.12 Gestor de análisis forense.....	7
3.13 Gestor de servicios de ciberseguridad	7
4 REFERENCIAS.....	7

1 OBJETIVO

El objetivo del presente documento es definir los roles y responsabilidades que permitan implementar, gestionar y controlar adecuadamente la Gestión de Seguridad de la Información de VanTrust Capital.

2 ALCANCE

Las disposiciones descritas en el presente documento aplican a todos los colaboradores, proveedores y terceros de VanTrust Capital como Administradora General de Fondos y Corredora de Bolsas, aplican a cada responsable que forma parte de la Gestión de Seguridad de la Información. La Gestión de Seguridad de la Información no es responsabilidad exclusiva del área de Seguridad de la Información, existir roles y responsabilidades asignadas a colaboradores de diferentes áreas. Cada colaborador debe leer, entender e implementar los lineamientos descritos en el documento que están alineadas a la Recopilación Actualizada de Normas – RAN capítulo 20 – 10 (Gestión de Seguridad de la Información y Ciberseguridad) de la Comisión para el Mercado Financiero – CMF de Chile.

Variaciones a este documento no están permitidas sin la aprobación del Comité de TI (Tecnologías de la Información) y del Oficial de Seguridad de la Información, debiendo documentar los motivos de las excepciones implementadas.

3 ROLES Y RESPONSABILIDADES

3.1 Comité de Seguridad de la Información

Es el responsable de aprobar cada vez que existan modificaciones o creaciones de procedimientos y documentos para la Gestión de Seguridad de la Información de VanTrust Capital.

3.2 CTO Corporativo Vantrust

Liderar y dirigir el equipo de Tecnología del Grupo Vantrust, es responsable de todo el equipamiento y sistemas que usa la empresa, para la operación del negocio. Realizar los planes de crecimiento y transformación digital de la compañía.

3.3 Oficial de seguridad de la Información

Es el máximo responsable del mantenimiento y mejora continua para la Gestión de Seguridad de la Información. Tiene como responsabilidad:

- Participar en la creación y revisión de políticas, procedimientos y planes referidos a la seguridad de la información.
- Evaluar, coordinar y monitorear el cumplimiento de políticas, procedimientos y controles referidos a la seguridad de la información.
- Coordinar con el propietario y custodio de la información para la elaboración del inventario de activos de la información y ejecución de la gestión de riesgos.
- Informar los resultados de la Gestión de Seguridad de la Información al Comité de TI (Tecnologías de la Información) y Directorio de la compañía.
- Dar seguimiento a los incidentes de seguridad de la información.
- Promover la difusión de los temas de seguridad de la información mediante charlas de capacitación y concientización.
- Supervisar la ejecución de las actividades que se deriven de los informes de las auditorías en seguridad de la información.

3.4 Auditor Líder

Es el responsable de encabezar al equipo de auditores internos. Tiene como responsabilidad:

- Convocar y realizar la reunión de apertura de auditoría.
- Realizar la reunión de cierre de acuerdo con el plan de auditoría.
- Planificar y dirigir todas las actividades de la auditoría.
- Ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo.

3.5 Auditor Interno

Es el responsable de preparar y llevar a cabo el proceso de auditoría para la Gestión de Seguridad de la Información. Tiene como responsabilidad:

- Revisar la documentación y evidencias de cumplimiento dentro del alcance.
- Llevar a cabo las reuniones de relevamiento de información con el personal involucrado, para corroborar o extender sus indagaciones.
- Generar los informes de las auditorías en seguridad de la información.
- Mantener imparcialidad, objetividad y ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo.
- Otras funciones en el ámbito de su competencia.

3.6 Auditado

Es el colaborador de VanTrust Capital o las personas y entidades públicas o privadas que utilizan la información de la compañía; que se encuentran sujetas a una revisión por parte del equipo de auditores. Tienen como responsabilidad proporcionar al equipo auditor la información necesaria y objetiva para asegurar un proceso de auditoría eficiente y eficaz.

3.7 Propietario de la Información

Es el responsable de la información que se genera y se utiliza en las operaciones de la compañía. Tiene como responsabilidad:

- Generar y mantener el inventario de activos de información, analizar los riesgos y planes de acción para su tratamiento de manera coordinada con el Oficial de Seguridad de la Información.
- Participar en la identificación de nuevos activos de información y en su clasificación de acuerdo a su grado de confidencialidad, integridad y disponibilidad; documentándolos y manteniendo su clasificación y etiquetado debidamente actualizado.
- Definir los usuarios que deben tener permisos de acceso a la información de acuerdo a sus funciones y competencias, revisando periódicamente los niveles de acceso a los sistemas de información a su cargo.
- Sugerir y apoyar en la elaboración de lineamientos y procedimientos de seguridad de la información dentro de sus respectivas áreas y procesos.
- Supervisar y verificar la aplicación de los controles de seguridad con el custodio de la información.

3.8 Custodio de la Información

El área de la seguridad de la información es el responsable de la administración diaria de la seguridad de los activos de información y el monitoreo del cumplimiento de las políticas y los controles de seguridad en los activos de información que se encuentren bajo su administración, y tiene como responsabilidad:

- Administrar los controles relevantes a la seguridad de la información, acorde a las medidas de tratamiento de la información especificadas por los propietarios de la información (restricción de accesos, validación de autenticidad, mecanismos de resguardo, entre otros).
- Cumplir con los controles implementados para la protección de los activos de información asignados para su custodia.
- Colaborar en la investigación de los incidentes de seguridad de la información.
- Identificar oportunidades de mejora y comunicarlas al Oficial de Seguridad de la Información.
- Respalidar, verificar y recuperar la información de los respaldos, manteniendo el registro del resguardo debidamente estructurado que permita tener la disponibilidad de los respaldos de acuerdo a su clasificación.
- Proteger y resguardar los activos de información físicos de accesos indebidos o no autorizados.

3.9 Usuario

Es el colaborador de VanTrust Capital, las personas y entidades públicas o privadas que utilizan la información de la compañía. Tiene como responsabilidad:

- Cumplir con todas las políticas y procedimientos de seguridad de la información.
- Preservar la confidencialidad de las contraseñas acceder a las diferentes aplicaciones, sistemas de información y recursos informáticos.
- Utilizar la información de la compañía estrictamente para los propósitos autorizados.
- Participar en los entrenamientos, capacitaciones y programas de sensibilización en temas de seguridad de la información.
- Reportar cualquier incidente, problema u oportunidades de mejora de seguridad de la información.
- No divulgar o utilizar información contenida en los sistemas, plataformas, aplicativos y otros recursos informáticos que se hayan facilitado en un entorno de trabajo remoto, presencial o mixto / híbrido, para propósitos ajenos a sus funciones o sin la debida autorización.

3.10 Gestor de Monitoreo

Realizar la detección y alertamiento de eventos/incidentes de seguridad.

Seguimiento y/o escalamiento sobre eventos/incidentes de seguridad sin atención.
Coordinación de la activación del WAR ROOM ante incidentes y ejecución de análisis forense (en caso aplique)

Brindar reporte de los eventos/incidentes notificados con una frecuencia semanal.

En caso de contingencia, coordinar y supervisar la transferencia al site de contingencia.

3.11 Gestor de Soporte y Administración

Atender los incidentes de infraestructura que se puedan presentar.

Solicitar apertura de caso con fabricante en caso se requiera y seguimiento de esta.
Ejecutar respaldos de la configuración completa (sin logs y en función a la factibilidad de

la solución) de un (01) firewall Fortinet 100D bajo la modalidad Onpremise, una (01) consola antivirus Kaspersky Endpoint Security bajo la modalidad Onpremise y una (01) consola antivirus Kaspersky Endpoint Security bajo la modalidad Cloud, en la frecuencia:

- Diario (entrega de informe de los últimos 07 días – A solicitud de cliente)
- Mensual (entrega de informe de los últimos 03 meses – A solicitud de cliente).

- Los respaldos para las consolas antivirus serán mediante un Protocolo de Escritorio Remoto – RDP; mientras que el respaldo para el firewall será mediante una conexión de Red Privada Virtual - VPN.
- Los respaldos serán alojados en un repositorio corporativo de la compañía.

Ver documento: Protocolo Activación Pruebas DRaaS

Atender de requerimientos (cambios y consultas sobre la configuración de las políticas de seguridad de los equipos).

Entregar un reporte mensual sobre los cambios realizados en las plataformas administradas.

3.12 Gestor de análisis forense

El equipo de servicios especializados de Secure Soft / GTD solicitará información inicial. Para iniciar el servicio, se enviará al correo: serv.esp@securesoftcorp.com.

Realizar una reunión con los involucrados para entender el incidente y expectativas de los interesados. Los involucrados serían las personas que conocen del incidente al detalle y los interesados podría ser el área de seguridad o las personas que requieren información del análisis forense.

Verificación de la disponibilidad del laboratorio forense de VanTrust Capital.

Evaluación de obtención de las evidencias.

Realizar análisis forense al activo de información.

Realizar informe del análisis forense realizado.

Realizar presentación del informe realizado.

3.13 Gestor de servicios de ciberseguridad

Entregar informe mensual del servicio de ciberseguridad

Realizar reuniones periódicas (mensual) para revisar la calidad del servicio:

- Cumplimiento de SLA's
- Puntos de mejora referente al servicio
- Revisión de acuerdos y/o compromisos

4 REFERENCIAS

Este documento está alineado con los siguientes estándares y políticas:

- Recopilación Actualizada de Normas – RAN capítulo 20 – 10 (Gestión de Seguridad de la Información y Ciberseguridad) de la Comisión para el Mercado Financiero – CMF de Chile.