MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

VANTRUST CAPITAL

Diciembre 2024

Control de Versiones

Fecha Modificación	Versión	Elaboró / Modifico	Fecha Aprobación directorio	Revisado por
17/01/2017	01			
17/04/2018	02	Gabriel Cayupan		Sandra Rivadeneira Jaime Fernandez
16/04/2020	03	Gabriel Cayupan	Abril 2020	Ivonne Müller Directorio Corredora y AGF
16/07/2021	04	Gabriel Cayupan	Julio 2021	Rodrigo Rossi Directorio Corredora y AGF
31/10/2023	05	Gabriel Cayupan	Noviembre 2023	Comité TI Comité de Riesgo Operacional Gestión de Personas Directorio Corredora
10/12/2024	06	Rodrigo Sanchez	Diciembre 2024	Comité TI Comité de Riesgo Operacional Directorio Corredora

1. INTRODUCCION

Este manual de política de seguridad de información establece los lineamientos generales y específicos aplicables a Vantrust Capital y a todas sus filiales, garantizando un enfoque uniforme en el cumplimiento de las normativas internas y externas. Su propósito es proporcionar directrices claras que permitan a todas las áreas y colaboradores de la organización alinear sus actividades con los estándares de seguridad, eficiencia y transparencia establecidos por la empresa.

Vantrust Capital, en adelante Vantrust o Vantrust Capital, identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la empresa, razón por la cual es necesario que establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información definidas por Vantrust. Para la elaboración de este, se toman como base las normativas y demás regulaciones aplicables, el capítulo décimo segundo del título primero de la norma ISO 27001 y las recomendaciones del estándar ISO 27002

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de Vantrust y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La seguridad de la información es una prioridad para Vantrust y por tanto es responsabilidad de todos, velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

Serán parte integrante estas políticas los procedimientos y documentación que requiera un detalle de los pasos a seguir para cumplir las políticas.

2. OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información de Vantrust Capital, con el fin de regular la gestión de la seguridad de la información al interior de la empresa.

3. ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, Colaboradores y terceros que laboren o tengan relación con Vantrust, para conseguir un adecuado nivel de protección de las

características de seguridad y calidad de la información relacionada.

4. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de Vantrust, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: es un documento en los que los Colaboradores de Vantrust o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de Vantrust, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información, que son autorizados por la empresa con el fin cumplir con sus funciones, esto incluye las conexiones remotas o teletrabajo.

Capacity Planning: es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la empresa para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado, esto debe estar en consecuencia con las necesidades actuales y futuras de la empresa.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que La Sala de TI, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples equipamientos para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Guías de clasificación de la información: directrices para catalogar la información de la empresa y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes a Vantrust.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de Vantrust.

Registros de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de Vantrust. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por

Vantrust o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por Vantrust (amenazas), las cuales se constituyen en fuentes de riesgo.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

En Vantrust la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, Vantrust implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los Colaboradores, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de Vantrust, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política Global de Seguridad de la Información de Vantrust se encuentra en base a las políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de Vantrust. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013.

El Comité de TI de Vantrust tendrá la potestad de modificar la Política General o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de estas. Las modificaciones que efectúe el Comité TI, antes de su entrada en vigencia, deben ser aprobadas por el Directorio de Vantrust.

6. COMPROMISO DE LA DIRECCION

El Directorio de Vantrust aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

El Directorio de la entidad demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los Colaboradores de Vantrust.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

7. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los Colaboradores, personal externo y proveedores de Vantrust. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan. Estas medidas o actividades sancionatorias deben son aplicadas por el área de Gestión de Personas de la empresa.

8. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

8.1. POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACION

Vantrust establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

8.1.1. Normas que rigen para la estructura organizacional de seguridad de la información

Normas dirigidas a: DIRECTORIO Y GERENCIA GENERAL

❖ El Directorio de Vantrust debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

❖ El Directorio debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.

❖ El Directorio debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.

❖ El Directorio debe promover activamente una cultura de seguridad de la información en Vantrust.

❖ El Directorio debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los Colaboradores de la entidad y al personal provisto por terceras partes.

❖ El Directorio y la Gerencia General de Vantrust, deben asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de Vantrust.

Normas dirigidas a: COMITÉ DE TI

❖ El Comité de TI debe actualizar y presentar ante el directorio las Políticas de Seguridad de la Información y la metodología para la clasificación de la información, según lo considere pertinente.

❖ El Comité de TI debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario, de acuerdo con las normativas vigentes.

❖ El Comité de TI debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

❖ El Comité de TI debe asignar las funciones, roles y responsabilidades, a sus Colaboradores para la operación y administración de la plataforma tecnológica de Vantrust. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad debe liderar la generación de lineamientos para gestionar la seguridad de la información de Vantrust y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.

❖ El Líder Ciberseguridad debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

Normas dirigidas a: JEFE DE RIESGO OPERACIONAL

❖ El jefe de riesgo operacional debe planear e instruir las auditorías internas al Sistema de Gestión de Seguridad de la Información de Vantrust a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.

❖ El jefe de riesgo operacional debe ejecutar e instruir revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

❖ El jefe de riesgo operacional debe informar a las áreas responsables los hallazgos de las auditorías y solicitar las mitigaciones correspondientes en un plan con fechas para mejorar o corregir los hallazgos encontrados.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los Colaboradores y personal provisto por terceras partes que realicen labores en o para Vantrust, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

8.2. POLITICA PARA USO DE DISPOSITIVOS MOVILES

Vantrust proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes, tabletas y notebooks, entre otros) institucionales que hagan uso de servicios de Vantrust. Así mismo, velará porque los Colaboradores hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

8.2.1. Normas para uso de dispositivos móviles

Normas dirigidas a: LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad, debe investigar y probar las opciones de protección de los dispositivos móviles institucionales que hagan uso de los servicios provistos por Vantrust.

❖ El Líder Ciberseguridad, debe establecer las configuraciones aceptables para los dispositivos móviles institucionales que hagan uso de los servicios provistos por Vantrust, advirtiendo en la entrega de los accesos remotos el procedimiento y el uso reservado de los accesos otorgados a los usuarios de la empresa.

❖ El Líder Ciberseguridad, debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

❖ El Líder Ciberseguridad, debe contar con un procedimiento que establezca que no puede haber información crítica o sensible en los equipos móviles institucionales de Vantrust, esta información debe estar en las carpetas de los Servidores de la Red y/o Sharepoint.

❖ El Líder Ciberseguridad, debe solicitar que se instale un software de antivirus en los dispositivos móviles institucionales.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

❖ Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

❖ Los usuarios no deben realizar instalaciones de programas de ningún tipo, aunque estos sean freeware, todas las instalaciones de programas o utilitarios se debe solicitar al Área de TI de la empresa, de manera formal, para su debida revisión y autorización. Estos deberán ser instalados por el equipo de soporte de Vantrust.

❖ Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

❖ Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

❖ Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

❖ Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

8.3. POLITICA PARA USO DE CONEXIONES REMOTAS - TELETRABAJO

Vantrust establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de Vantrust; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura. Todas las conexiones remotas deberán ser solicitadas al área de TI, quien evaluará en conjunto con las jefaturas de las respectivas áreas la autorización de la conexión remota.

Se procura que los accesos de conexiones remotas sean realizados desde el equipamiento móvil asignado a cargo de cada Colaboradores.

Las conexiones remotas tendrán acceso a los sistemas y servicios de red, como almacenamiento de información en las carpetas compartidas según el mismo perfil que utilizan conectados en la red local de la respectiva oficina.

8.3.1. Normas para uso de conexiones remotas

Normas dirigidas a: COMITÉ DE TI

❖ Comité de TI, deben analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de Vantrust.

Normas dirigidas a: LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de Vantrust.

❖ El Líder Ciberseguridad debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

❖ El Líder Ciberseguridad, debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de Vantrust de manera permanente.

❖ El Líder Ciberseguridad, debe promover que los usuarios protejan físicamente los equipos móviles a cargos de los usuarios, que tengan procedimientos para no perderlos o dañarlos.

Normas dirigidas a: JEFE DE RIESGO OPERACIONAL

❖ El jefe de riesgo operacional debe, dentro de su autonomía, instruir auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica de Vantrust.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Ningún usuario podrá realizar conexión remota en caso de ausencia prolongada, licencia o vacaciones, sin la debida autorización de la Gerencia de Operaciones. De ser requerida información, esta deberá ser solicitada vía mail al jefe de Área con copia a su Gerencia respectiva.

❖ En ninguna circunstancia, un usuario podrá transferir sus credenciales de conexión remota. Estas son individuales e intransferibles,

❖ Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de Vantrust y deben acatar las condiciones de uso establecidas para dichas conexiones.

❖ Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, en ninguna circunstancia, en computadores público, de hoteles o cafés internet, entre otros. De este cumplimiento se debe encargar el área de TI.

9. POLÍTICAS DE SEGURIDAD DEL PERSONAL

9.1. POLÍTICA RELACIONADA CON LA VINCULACIÓN DE COLABORADORES

Vantrust reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos Colaboradores se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los Colaboradores en sus cargos.

9.1.1. Normas relacionadas con la vinculación de Colaboradores

Normas dirigidas a: GESTIÓN DE PERSONAS

❖ Gestión de Personas debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en Vantrust, antes de su vinculación definitiva.

❖ Gestión de Personas debe certificar que los Colaboradores de Vantrust firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Normas dirigidas a: SUPERVISORES, GERENTES Y JEFES DE AREA

- Cada Supervisor, Gerente y jefe de Área debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de Vantrust.

9.2. POLÍTICA APLICABLE DURANTE LA VINCULACION DE COLABORADORES

Vantrust en su interés por proteger su información y los recursos de procesamiento de esta demostrará el compromiso del Directorio en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de Vantrust.

Todos los Colaboradores de Vantrust deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la entidad.

Normas aplicables durante la vinculación de Colaboradores

Normas dirigidas a: DIRECTORIO

- El Directorio debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer Vantrust.

- El Directorio debe promover la importancia de la seguridad de la información entre los Colaboradores de Vantrust y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.

- El Directorio debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente Vantrust, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Normas dirigidas a: LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad, debe diseñar y ejecutar de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

❖ El Líder Ciberseguridad, debe capacitar y entrenar a los Colaboradores de Vantrust en el programa de concienciación en seguridad de la información para evitar posibles riesgos de seguridad.

Normas dirigidas a: GERENCIA GENERAL

❖ La Gerencia general debe aplicar el proceso disciplinario de Vantrust cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los Colaboradores que por sus funciones hagan uso de la información Vantrust, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

9.3. POLÍTICA DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS COLABORADORES

Vantrust asegurará que sus Colaboradores y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

9.3.1. Normas para la desvinculación, licencias, vacaciones o cambios de labores de los Colaboradores

Normas dirigidas a: GESTIÓN DE PERSONAS

❖ Gestión de Personas debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los Colaboradores de Vantrust llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Normas dirigidas a: GESTIÓN DE PERSONAS, GERENCIAS Y JEFES DE ÁREA

❖ Cada Gerente o jefe debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los Colaboradores o personal provistos por terceras partes al jefe de producción y los encargados de dar de baja de todos los sistemas a los Colaboradores, según procedimiento establecido.

Normas dirigidas a: JEFE DE PRODUCCION

❖ El jefe de producción debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe proceder con la modificación o inhabilitación de usuarios.

10. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

10.1. POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

Vantrust como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad de Vantrust, son activos de la institución y se proporcionan a los Colaboradores y terceros autorizados, para cumplir con los propósitos del negocio.

Toda la información sensible de Vantrust, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte El LÍder Ciberseguridad. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

10.1.1. Normas de responsabilidad por los activos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

❖ Las Gerencias, directores y Asesores de Vantrust, deben actuar como propietarios de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

❖ Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.

❖ Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de Vantrust, se encuentran sujetos a auditorías por parte de la Gerencia de Complimiento y a revisiones de cumplimiento por parte de la Oficial de Seguridad.

Normas dirigidas a: COMITÉ DE TI

❖ El COMITÉ DE TI es la propietaria de los activos de información correspondientes a la plataforma tecnológica de Vantrust y, en consecuencia, debe asegurar su apropiada operación y administración.

❖ El COMITÉ DE TI en conjunto con el encargado de Control de Cambios, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de Vantrust.

Normas dirigidas a: JEFE DE PRODUCCION

❖ El jefe de producción es responsable de definir los modelos y las configuraciones generales de las estaciones de trabajo fijas y/o portátiles de los Colaboradores.

❖ El jefe de producción es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los Colaboradores que se retiran o cambian de labores, cuando les es formalmente solicitado.

❖ El Líder Ciberseguridad, debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos de Vantrust.

❖ El Líder Ciberseguridad, debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

❖ El jefe de producción de la Información debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de Vantrust.

❖ El Líder Ciberseguridad debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

Normas dirigidas a: GERENCIAS Y JEFES DE ÁREA

❖ Los Gerentes y jefes de Área, o quien ellos designen, deben autorizar a sus Colaboradores el uso de los recursos tecnológicos, previamente preparados por el encargado de Tecnología.

❖ Los Gerentes y jefes de Área, o quien ellos designen, deben recibir los recursos tecnológicos asignados a sus Colaboradores cuando estos se retiran de Vantrust o son trasladados de área.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los recursos tecnológicos de Vantrust, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de Vantrust.

❖ Los recursos tecnológicos de Vantrust provistos a Colaboradores y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las labores de Vantrust; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

❖ Los Colaboradores no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de Vantrust.

❖ Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

❖ En el momento de desvinculación o cambio de labores, los Colaboradores deben realizar la entrega de su puesto de trabajo al Gerente, Director o Jefe o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

10.1.2. Normas para la clasificación y manejo de la información

Normas dirigidas a: COMITÉ DE TI

❖ Comité de TI debe recomendar los niveles de clasificación de la información propuestos por El Líder Ciberseguridad y la guía de clasificación de la Información de Vantrust para que sean aprobados el Directorio.

❖ COMITÉ DE TI debe proveer los métodos de resguardo de la información, así como debe administrar el software o herramienta utilizado para tal fin.

Normas dirigidas a: LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad, debe definir los niveles de clasificación de la información para Vantrust y, posteriormente generar la guía de clasificación de la Información.

❖ El Líder Ciberseguridad debe socializar y divulgar la guía de clasificación de la Información a los Colaboradores de Vantrust.

❖ El Líder Ciberseguridad debe monitorear con una periodicidad establecida la aplicación de la guía de clasificación de la Información.

Normas dirigidas a: JEFE DE PRODUCCION

❖ El jefe de producción debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.
❖ El jefe de producción debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de esta, acogiéndose a procedimiento establecido para tal fin.

❖ El jefe de producción debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

- El jefe de producción debe administrar el contrato de almacenamiento y resguardo de las cintas de backups, otros medios de almacenamiento y documentos físicos de Vantrust con el proveedor del servicio.

- El jefe de producción debe verificar el cumplimiento de los Acuerdos de Niveles de Servicio y Acuerdos de intercambio con el proveedor de custodia externo de los medios de almacenamiento y documentos de Vantrust.

Normas dirigidas a: COMITÉ DE TI Y LIDER CIBERSEGURIDAD

- El COMITÉ DE TI junto con El Líder Ciberseguridad deben definir los métodos de resguardo de la información de la Entidad de acuerdo con el nivel de clasificación de los activos.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los activos de información deben clasificar su información de acuerdo con las guías de clasificación de la Información establecida.

- Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de Vantrust.

- La información física y digital de Vantrust debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias: verificar las áreas adyacentes a impresoras, escáneres y fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres y fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

- Tanto los Colaboradores como el personal provisto por terceras partes deben asegurarse de que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

10.2. POLITICA PARA USO DE TOKENS DE SEGURIDAD

Vantrust proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque los Colaboradores hagan un uso responsable de estos.

10.2.1. Normas para uso de tokens de seguridad

Normas dirigidas a: AREAS USUARIAS DE TOKENS DE SEGURIDAD

- Cada área usuaria de tokens de seguridad debe asignar un Colaboradores administrador de los mismos con la potestad para autorizar las solicitudes de acceso.

Normas dirigidas a: ADMINISTRADORES DE LOS TOKENS DE SEGURIDAD

- Los Administradores de los tokens de seguridad deben procesar las solicitudes de dichos tokens según los requerimientos de cada entidad proveedora de éstos y adjuntar la documentación necesaria.

- Los Administradores de los tokens deben recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos.

- Los Administradores de los tokens deben crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades a realizar por cada Colaboradores creado.

- Los Administradores de los tokens deben entregar a los Colaboradores designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta de seguridad para custodia de estos.

❖ Los Administradores de los tokens deben dar avisos a las entidades emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de estos.

❖ Los Administradores de los tokens deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.

Normas dirigidas a: USUARIOS DE TOKENS DE SEGURIDAD

❖ Los usuarios que requieren utilizar los tokens de seguridad deben contar con una cuenta de usuario en los portales o sitios de uso de estos; dichos tokens harán parte del inventario físico de cada usuario a quien se haya asignado.

❖ El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad o sobre asignado para cada token, dentro de caja fuerte o escritorios con llave al interior de las áreas usuarias, de tal forma que se mantengan fuera del alcance de terceros no autorizados.

❖ Los usuarios deben notificar al Administrador de los tokens en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comunique con las entidades emisoras de dichos tokens.

❖ Los usuarios no deben permitir que terceras personas observen la clave que genera el token, así como no deben aceptar ayuda de terceros para la utilización del token.

❖ Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como Colaboradores de Vantrust. En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.

❖ Los usuarios deben mantener los tokens asignados en un lugar seco y no introducirlos en agua u otros líquidos.

❖ Los usuarios deben evitar exponer los tokens a campos magnéticos y a temperaturas extremas.

❖ Los usuarios deben evitar que los tokens sean golpeados o sometidos a esfuerzo físico.❖ Los usuarios no deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.

❖ Los usuarios no deben usar los tokens fuera de las instalaciones de Vantrust para evitar pérdida o robo de estos.

10.3. POLÍTICA DE USO DE PERIFERICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de Vantrust será reglamentado por el encargado de Tecnología, considerando las labores realizadas por los Colaboradores y su necesidad de uso.

10.3.1. Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: COMITÉ DE TI Y JEFE PRODUCCION

❖ El Comité de TI y El jefe de producción deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de Vantrust.

Normas dirigidas a: COMITÉ DE TI

❖ El COMITÉ DE TI debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de Vantrust, de acuerdo con los lineamientos y condiciones establecidas.

❖ El COMITÉ DE TI debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de Vantrust, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

Normas dirigidas a: JEFE PRODUCCION

❖ El jefe de producción debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de Vantrust de acuerdo con el perfil del cargo del Colaboradores solicitante.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los Colaboradores y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Gerencia de Operaciones.

❖ Los Colaboradores de Vantrust y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Gerencia de Operaciones.

❖ Los Colaboradores y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento institucionales asignados.

❖ Los Colaboradores y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de Vantrust.

11. POLÍTICAS DE CONTROL DE ACCESO

11.1. POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

El Comité de TI, como responsable de las redes de datos y los recursos de red de Vantrust, debe propender para que dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

11.1.1. Normas de acceso a redes y recursos de red

Normas dirigidas a: LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad, debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de Vantrust.

❖ El Líder Ciberseguridad, debe asegurar que las redes inalámbricas de Vantrust cuenten con métodos de autenticación que evite accesos no autorizados.

❖ El Líder Ciberseguridad, debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de redes Vantrust, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

❖ El Líder Ciberseguridad, debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red de Vantrust.

❖ El Líder Ciberseguridad debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los Colaboradores y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos Vantrust, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

❖ Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de Vantrust deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

11.2. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

Vantrust establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de Vantrust. Así mismo, velará porque los Colaboradores y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

11.2.1. Normas de administración de acceso de usuarios

Normas dirigidas a LIDER CIBERSEGURIDAD Y JEFE PRODUCCION

❖ El Líder Ciberseguridad debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de Vantrust, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

❖ El jefe de producción previa solicitud de los jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los sistemas de información, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.

❖ El Líder Ciberseguridad, debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información Vantrust; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

❖ El Líder Ciberseguridad debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los Colaboradores se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

❖ El jefe de producción debe autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información de Vantrust.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

❖ Es responsabilidad de los Propietarios de los activos de información, definir los perfiles de usuario y autorizar, juntamente con El Líder Ciberseguridad, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

❖ Los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

Normas dirigidas a: GERENCIAS Y JEFES DE ÁREA

❖ Los Gerentes y jefes de Área deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los Colaboradores que laboran en sus áreas, acogiéndose al procedimiento establecidos para tal fin.

11.3. POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información Vantrust realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

11.3.1. Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de Vantrust deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

❖ Los Colaboradores no deben compartir sus cuentas de usuario y contraseñas con otros Colaboradores o con personal provisto por terceras partes.

❖ Los Colaboradores y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de Vantrust deben acogerse a lineamientos para la configuración de contraseñas implantados por Vantrust.

11.4. POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACION

Comité de TI de Vantrust velará porque los recursos de la plataforma tecnológica y los servicios de red de Vantrust sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

11.4.1. Normas de uso de altos privilegios y utilitarios de administración

Normas dirigidas a: LIDER CIBERSEGURIDAD Y JEFE PRODUCCION

❖ El jefe de producción debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos Colaboradores designados para dichas funciones.

❖ El jefe de producción debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

❖ El Líder Ciberseguridad debe verificar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.

❖ El jefe de producción de restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

❖ El jefe de producción debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean

suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas. El responsable debe ser el encargado de cada Sistema.

❖ El Líder Ciberseguridad debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas. Esta actividad debe estar a cargo del Soporte de usuarios y supervisado por de Seguridad de la información.

❖ El jefe de producción debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

❖ El Líder Ciberseguridad debe validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña de los usuarios administradores acoja el procedimiento definido para tal fin. El Oficial de cumplimento debe revisar los reportes entregados por El Líder Ciberseguridad.

❖ El Líder Ciberseguridad debe revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoría de la plataforma tecnológica y los sistemas de información.

11.5. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

Las Gerencias, Directores o Jefaturas como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

Comité de TI, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Deberá Tener Procedimiento para que los desarrollos cumplan las mejores prácticas para el control de acceso a los sistemas y mantener los LOG para que los cambios a los registros se guarden por un periodo determinado y otros.

11.5.1. Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

❖ Los propietarios de los activos de información deberán realizar una “certificación de los perfiles definidos en los sistemas de información” y los privilegios asignados a los usuarios que acceden a ellos. Se debe establecer un procedimiento de revisión una vez al año.

Normas dirigidas a: COMITÉ DE TI

❖ El Comité de TI debe asegurar que se cumpla el procedimiento para la separación lógica de los ambientes de Pruebas, instruyendo que se deben aplicar estos para las pruebas de nuevos sistemas, realizando instalaciones separadas y creando instancias distintas en las Bases de Datos.

❖ El Comité de TI debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error. N/A no hay ambientes diferenciados, solo Producción. Depende de la aprobación del punto de arriba.

❖ El Comité de TI debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción. Se deben Crear los Procedimientos para los controles de acceso.

❖ El Comité de TI debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
Esto Aplica para todos los desarrollos internos o en los casos que se paga por los sistemas, y donde se acuerda la entrega del Código Fuente de los desarrollos, estos deben se resguardo con los backups.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

❖ Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

❖ Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

❖ Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

❖ Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

❖ Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

❖ Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

❖ Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

❖ Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

❖ Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

❖ Los desarrolladores deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados. Esto se debe realizar en una de las certificaciones anuales que se definirá en un procedimiento.

12. POLÍTICAS DE SEGURIDAD FÍSICA

12.1. POLÍTICA DE ÁREAS SEGURAS

Vantrust proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, sean consideras áreas de acceso restringido. Para esto existen Llaves para el acceso a los dos Sitios de equipamiento.

Se deberá dejar un registro en cada Sala de los accesos con el motivo. Solo para personal autorizado.

12.1.1. Normas de áreas seguras

Normas dirigidas a: GERENCIA CLIENTES Y CALIDAD (ADMINISTRACION).

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por el o la gerente cliente y calidad y jefe producción; no obstante, los visitantes siempre deberán estar acompañados de un Colaborador de dicha dirección durante su visita al centro de cómputo o a los centros de cableado. Se debe solicitar acceso a los encargados de cada Sitio de Máquinas y/o al Gerente de Operaciones.

- Gerencia de cliente y calidad, debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

- Gerencia de cliente y calidad debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un Colaboradores autorizado.

- Gerencia de cliente y calidad debe velar porque los recursos de la plataforma tecnológica de Vantrust ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

❖ Gerencia de cliente y calidad debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

Normas dirigidas a: GERENCIAS Y JEFES DE ÁREA

❖ Los Gerentes y jefes de Área que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.

❖ Los Gerentes y jefes de Área deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los Colaboradores autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros Colaboradores de Vantrust.

Normas dirigidas a: ADMINISTRACIÓN

❖ Administración debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de Vantrust.

❖ Administración debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de Vantrust.

❖ Administración debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.

❖ Administración debe controlar el ingreso de los visitantes a los centros de cableado que están bajo su custodia.

❖ El encargado de Administración debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos, Contrato para mantenimiento de tableros eléctricos, mantenimiento de UPS y otros

❖ Administración debe cerciorarse de que los centros de cableado que están bajo su custodia se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los ingresos y egresos de personal a las instalaciones de Vantrust deben ser registrados; por consiguiente, los Colaboradores y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

❖ Los Colaboradores que realicen trabajos en las instalaciones de Vantrust Capital, deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de Vantrust; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

❖ Los Colaboradores de Vantrust y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

12.2. POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

Vantrust para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de Vantrust que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

12.2.1. Normas de seguridad para los equipos institucionales

Normas dirigidas a: LIDER CIBERSEGURIDAD Y JEFE DE PRODUCCION

❖ El Líder Ciberseguridad debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de Vantrust.

❖ El jefe de producción debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de Vantrust.

❖ El jefe de producción en conjunto con la Coordinación de Administración debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.

❖ El Líder Ciberseguridad debe generar estándares de configuración segura para los equipos de cómputo de los Colaboradores de Vantrust y Soporte TI configurar dichos equipos acogiendo los estándares generados.

❖ El jefe de producción debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de Vantrust y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

❖ El Líder Ciberseguridad debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los Colaboradores de Vantrust, ya sea cuando son dados de baja o cambian de usuario.

❖ El jefe de producción debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas de Vantrust, en particular de las áreas sensibles

Normas dirigidas a: JEFE DE RIESGO OPERACIONAL

❖ El jefe de riesgo operacional tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de la entidad.

Normas dirigidas a: TODOS LOS USUARIOS

❖ El jefe producción es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier Colaboradores de los recursos tecnológicos de Vantrust.

❖ Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los Colaboradores y personal provisto por terceras partes deben acoger las instrucciones técnicas de proporcione El jefe de producción.

❖ Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de Vantrust el usuario responsable debe informar a encargado de TI o de Soporte con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

❖ La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de Vantrust, solo puede ser realizado por los Colaboradores del soporte de TI, o personal de terceras partes autorizado por Vantrust.

❖ Los Colaboradores de Vantrust y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

❖ Los Colaboradores de Vantrust y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

❖ Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

❖ Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

❖ Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

❖ En caso de pérdida o robo de un equipo de cómputo Vantrust, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

❖ Los Colaboradores de Vantrust y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

13. SEGURIDAD EN LAS OPERACIONES

13.1. ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

El Comité de TI, encargado de administración de los recursos tecnológicos que apoyan los procesos Vantrust, asignará funciones específicas a sus Colaboradores, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la

información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos serán adecuadamente controlados y debidamente autorizados.

Comité de TI proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de Vantrust, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

13.1.1. Normas de asignación de responsabilidades operativas

Normas dirigidas a: COMITÉ DE TI

❖ Comité de TI debe efectuar, a través de sus Colaboradores, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de Vantrust.

❖ El Comité de TI, a través de sus Colaboradores, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Normas dirigidas a: EL LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica de Vantrust.

13.2. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

Vantrust proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus Colaboradores y personal provisto por terceras partes frente a los ataques de software malicioso.

13.2.1. Normas de protección frente a software malicioso

Normas dirigidas a: LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de Vantrust y los servicios que se ejecutan en la misma.

❖ El Líder Ciberseguridad, debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

❖ El Líder Ciberseguridad, debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

❖ El Líder Ciberseguridad, a través de sus Colaboradores, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

❖ El Líder Ciberseguridad, a través de sus Colaboradores, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la Gerencia de Operaciones; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

❖ Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

❖ Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de

fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

❖ Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al soporte de TI y Ciberseguridad, para que, a través de ella, el COMITÉ DE TI tome las medidas de control correspondientes.

13.3. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

Vantrust certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo del Comité de TI, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

13.3.1. Normas de copias de respaldo de la información

Normas dirigidas a: JEFE DE PRODUCCION

❖ El jefe de producción a través de sus colaboradores debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

❖ El jefe de producción debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

❖ El jefe de producción a través de sus Colaboradores debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

❖ El jefe de producción debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

❖ El jefe de producción debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos información de Vantrust.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con Comité de TI, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Es responsabilidad de los usuarios de la plataforma tecnológica de Vantrust identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

13.3.2. Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Normas dirigidas a: LIDER CIBERSEGURIDAD Y JEFE PRODUCCION.

❖ El Líder Ciberseguridad, en conjunto con el jefe de producción debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de Vantrust.

❖ El Líder Ciberseguridad, a través del Comité de revisión de logs, deben definir de manera periódica cuáles monitoreos se realizarán de los registros de auditoría sobre los aplicativos donde se opera los procesos misionales de Vantrust. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado.

❖ El jefe de producción a través de sus Colaboradores debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.

❖ El Líder Ciberseguridad y jefe de producción deben certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de Vantrust. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

Normas dirigidas a: JEFE DE RIESGO OPERACIONAL

❖ El jefe de riesgo operacional debe determinar los periodos de retención de los registros (logs) de auditoría de los recursos tecnológicos y los sistemas de información de Vantrust.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

❖ Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.

❖ Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por el Encargo de Seguridad de la Información.

❖ Los desarrolladores deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoría que brinden información adicional a la estrictamente requerida.

13.4. POLITICA DE CONTROL AL SOFTWARE OPERATIVO

Vantrust, a través de Comité de TI, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado. Debe ser responsabilidad del soporte que los SO tengan actualizaciones y parches al día.

13.4.1. Normas de control al software operativo

Normas dirigidas a: LIDER CIBERSEGURIDAD Y JEFE PRODUCCION

❖ El Líder Ciberseguridad debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en Vantrust.

❖ El Líder Ciberseguridad, debe asegurarse que el software operativo instalado en la plataforma tecnológica de Vantrust cuenta con soporte de los proveedores.

❖ El jefe de producción debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.

|

❖ El Líder Ciberseguridad, debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

❖ El Líder Ciberseguridad, debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de Vantrust.

.

13.5. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

Vantrust, a través de Comité de TI y el Líder Ciberseguridad, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

13.5.1. Normas para la gestión de vulnerabilidades

Normas dirigidas a: JEFE CIBERSEGURIDAD

❖ El Líder Ciberseguridad debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de estas.

❖ El Líder Ciberseguridad debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Normas dirigidas a: COMITÉ DE TI

❖ Comité de TI debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.

❖ El Comité de TI, a través de sus Colaboradores, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

❖ El Comité de TI, debe revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

14. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

14.1. POLÍTICA DE GESTION Y ASEGURAMIENTO DE LAS REDES DE DATOS

Vantrust establecerá, a través del Comité de TI, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.
De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de Vantrust.

14.1.1. Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: COMITÉ DE TI

- El Comité de TI debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de Vantrust.

- El Comité de TI debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

- El Comité de TI debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

- El Comité de TI debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de Vantrust, acogiendo buenas prácticas de configuración segura.

- El Comité de TI debe instalar protección entre las redes internas Vantrust y cualquier red externa, que este fuera de la capacidad de control y administración de Vantrust.

- El Comité de TI debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de Vantrust.

14.2. POLÍTICA DE USO DEL CORREO ELECTRONICO

Vantrust, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre Colaboradores y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

14.2.1. Normas de uso del correo electrónico

Normas dirigidas a: LIDER CIBERSEGURIDAD Y JEFE DE PRODUCCION

- El jefe de producción debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.

- El jefe de producción debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

- El Líder Ciberseguridad, debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.

- El Líder Ciberseguridad, debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

- El Líder Ciberseguridad, debe generar campañas para concientizar tanto a los Colaboradores internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún Colaboradores de Vantrust o provisto por un tercero, en ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.

- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de Vantrust. El correo institucional no debe ser utilizado para actividades personales.

- Los mensajes y la información contenida en los buzones de correo son propiedad de Vantrust y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Los usuarios de correo electrónico institucional tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los Colaboradores de Vantrust y el personal provisto por terceras partes.

- No es permitido el envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por Vantrust y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

14.3. POLÍTICA DE USO ADECUADO DE INTERNET

Vantrust consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en Vantrust.

14.3.1. Normas de uso adecuado de internet

Normas dirigidas a: COMITÉ DE TI

- El Comité de TI debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

- El Comité de TI debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

- El Comité de TI debe monitorear continuamente el canal o canales del servicio de Internet.

❖ El Comité de TI debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

❖ El Comité de TI debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Normas dirigidas a: JEFE CIBERSEGURIDAD

❖ El Líder Ciberseguridad debe generar campañas para concientizar tanto a los Colaboradores internos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los usuarios del servicio de Internet de Vantrust deben hacer uso de este en relación con las actividades laborales que así lo requieran.

❖ Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

❖ No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

❖ No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y Comité de TI, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

❖ No está permitido el intercambio no autorizado de información de propiedad de Vantrust, de sus clientes y/o de sus Colaboradores, con terceros.

14.4. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

Vantrust asegurará la protección de la información con Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. Vantrust propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

14.4.1. Normas de intercambio de información

Normas dirigidas a: GESTION DE PERSONAS

- El área de Gestión de Personas, en acompañamiento con El Líder Ciberseguridad, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre Vantrust y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por Vantrust a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.

Normas dirigidas a: JEFE CIBERSEGURIDAD

- El Líder Ciberseguridad debe definir y establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación Vantrust, reciben o envían información de los beneficiarios de Vantrust, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de esta.

- El Líder Ciberseguridad debe velar porque el intercambio de información de Vantrust con entidades externas se realice en cumplimiento de las Políticas de seguridad para el intercambio de información aquí descritas, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Los propietarios de los activos de información deben velar porque la información de Vantrust o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

- Los propietarios de los activos de información deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de estos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.

- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

- Los propietarios de los activos de información deben autorizar los requerimientos de solicitud/envío de información de Vantrust por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

- Los propietarios de los activos de información deben asegurarse de que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de Vantrust, así como del procedimiento de intercambio de información.

Normas dirigidas a: COORDINACION DE CORRESPONDENCIA

- La Coordinación de Correspondencia debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.

- La Coordinación de Correspondencia debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por el Vantrust, y que estos permitan ejecutar rastreo de las entregas.

Normas dirigidas a: COMITÉ DE TI

- El Comité de TI debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Normas dirigidas a: TERCEROS CON QUIENES SE INTERCAMBIA INFORMACION DE Vantrust

- Los terceros con quienes se intercambia información de Vantrust deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de Vantrust, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.

- Los terceros con quienes se intercambia información de Vantrust deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

Normas dirigidas a: TODOS LOS USUARIOS:

- Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de Vantrust o de sus beneficiarios.

- No está permitido el intercambio de información sensible de Vantrust por vía telefónica.

15. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

15.1. POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

Vantrust asegurará que el software adquirido y desarrollado tanto al interior de Vantrust, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él. Las áreas propietarias de sistemas de información, Comité de TI y el Encargado de la Seguridad de la Información, incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

15.1.1. Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN, COMITÉ DE TI Y LIDER CIBERSEGURIDAD

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de Vantrust formalmente asignada.

❖ El Comité de TI debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

❖ Las áreas propietarias de los sistemas de información, en acompañamiento con la Gerencia de Operaciones deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

❖ Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

❖ El Líder Ciberseguridad. Debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

15.2. POLÍTICA DE DESARROLLO SEGURO, REALIZACION DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

Vantrust velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por Vantrust.

15.2.1. Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Normas dirigidas a: COMITÉ DE TI

❖ El Comité de TI debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

❖ El Comité de TI debe asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

❖ El Comité de TI, a través de sus Colaboradores, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información

estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

Normas dirigidas a: LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad, debe verificar que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

16. POLÍTICAS QUE RIGEN DE LA RELACION CON TERCERAS PARTES

16.1. POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES

Vantrust establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los Colaboradores responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

16.1.1. Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas dirigidas a: COMITÉ DE TI Y LIDER CIBERSEGURIDAD

❖ El Comité de TI y El Líder Ciberseguridad deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

❖ Comité de TI y El Líder Ciberseguridad, deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

Normas dirigidas a: COMITÉ DE TI

❖ El Comité de TI debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de Vantrust.

Normas dirigidas a: LIDER CIBERSEGURIDAD Y JEFE PRODUCCION

❖ El jefe producción de la Información debe evaluar y aprobar los accesos a la información de Vantrust requeridos por terceras partes.

❖ El Líder Ciberseguridad debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

❖ Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de Vantrust a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de esta, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

16.2. POLÍTICA DE GESTION DE LA PRESTACION DE SERVICIOS DE TERCERAS PARTES

Vantrust propenderá por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

16.2.1. Normas de gestión de la prestación de servicios de terceras partes

Normas dirigidas a: COMITÉ DE TI

❖ El Comité de TI debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de Vantrust.

❖ La Gerencia de Operaciones y El Líder Ciberseguridad deben verificar las condiciones de comunicación segura, y transmisión de información desde y hacia los terceros proveedores de servicios.

Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

❖ Los Supervisores de contratos con terceros deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

❖ Los Supervisores de contratos con terceros, con el apoyo de El Líder Ciberseguridad, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

17. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

17.1. POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

Vantrust promoverá entre los Colaboradores y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

El Directorio o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

17.1.1. Normas para el reporte y tratamiento de incidentes de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

❖ Los propietarios de los activos de información deben informar a El Líder Ciberseguridad, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Normas dirigidas a: LIDER CIBERSEGURIDAD

❖ El Líder Ciberseguridad debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

❖ El Líder Ciberseguridad debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente.

❖ El Líder Ciberseguridad debe investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re- ocurrencia.

❖ El Líder Ciberseguridad debe, con el apoyo con el Comité de TI, crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Normas dirigidas a: COMITÉ DE TI

❖ El Comité de TI debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Es responsabilidad de los Colaboradores de Vantrust y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

❖ En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los Colaboradores deben notificarlo al área de Ciberseguridad para que se registre y se le dé el trámite necesario.

18. POLÍTICAS DE INCLUSION DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

18.1. POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACION

Vantrust proporcionará los recursos suficientes para proporcionar una respuesta efectiva de Colaboradores y procesos en caso de contingencia o eventos catastróficos que se presenten en Vantrust y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de estos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. Vantrust mantendrá canales de comunicación adecuados hacia Colaboradores, proveedores y terceras partes interesadas.

Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

Normas dirigidas a: COMITE DE TI Y JEFE PRODUCCION

- El Comité de TI, junto con el jefe de producción, deben reconocer las situaciones que serán identificadas como emergencia o desastre para Vantrust, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

- El Comité de TI, junto con el jefe de producción, deben liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres

- El Comité de TI, junto con el jefe de producción, deben realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

- El Comité de TI, junto con el jefe de producción, producto del análisis BIA deben seleccionar las estrategias de recuperación más convenientes para Vantrust.

- El Comité de TI, junto con el jefe de producción, deben validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

|

- El Comité de TI, junto con el Líder Ciberseguridad y jefe producción, deben asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

- El jefe de producción debe elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

- El Líder Ciberseguridad y jefe de producción deben participar activamente en las pruebas de recuperación ante desastres y notificar los resultados al Comité de TI.

Normas dirigidas a: GERENCIAS Y JEFES DE ÁREA

- Los Gerentes y jefes de Área deben identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

18.2. POLÍTICA DE REDUNDANCIA

Vantrust propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para Vantrust.

18.2.1. Normas de redundancia

Normas dirigidas a: COMITÉ DE TI Y EL LÍDER CIBERSEGURIDAD

- El Comité de TI y el Líder Ciberseguridad deben analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para Vantrust y la plataforma tecnológica que los apoya.

- El Comité de TI debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de Vantrust.

❖ El Comité de TI, a través de sus Colaboradores, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de Vantrust.

19. POLÍTICAS DE CUMPLIMIENTO

19.1. POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

Vantrust velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

19.1.1. Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a: LA ASESORÍA JURIDICA

❖ La Asesoría Jurídica y El Líder Ciberseguridad deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a Vantrust y relacionados con seguridad de la información.

Normas dirigidas a: COMITÉ DE TI y EL LÍDER CIBERSEGURIDAD

❖ El Comité de TI debe certificar que todo el software que se ejecuta en Vantrust esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

❖ El Líder Ciberseguridad debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de Vantrust para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Normas dirigidas a: TODOS LOS USUARIOS

❖ Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

❖ Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

19.2. POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la de Ley de Protección de Datos de Carácter Personal", en adelante Ley N° 19.628, por la cual se dictan disposiciones para la protección de datos personales, Vantrust a través de Líder Ciberseguridad, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales el Vantrust, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla Vantrust, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, Vantrust exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus Colaboradores, estableciendo los controles necesarios para preservar aquella información que Vantrust conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de Vantrust y no sea publicada, revelada o entregada a Colaboradores o terceras partes sin autorización.

19.2.1. Normas de privacidad y protección de datos personales

Normas dirigidas a: AREAS QUE PROCESAN DATOS PERSONALES

- Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de Vantrust o de sus Colaboradores de cual tengan conocimiento en el ejercicio de sus funciones.

- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Normas dirigidas a: USUARIOS DE LOS PORTALES VANTRUST

- Los usuarios de los portales de Vantrust deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.

- Los usuarios de los portales de Vantrust deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales de Vantrust.

- Los usuarios de los portales de Vantrust deben aceptar el suministro de datos personales que pueda hacer Vantrust a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoría interna o externa.

20. APROBACIÓN

20.1. ÚLTIMA APROBACIÓN POR DIRECTORIOS

Fecha Acuerdo de aprobación DIRECTORIO VANTRUST CAPITAL CORREDORES DE BOLSA S.A.	Diciembre 2024 23/12/2024
Fecha Acuerdo de aprobación DIRECTORIO VANTRUST CAPITAL AGF S.A.	Diciembre 2024 23/12/2024