DAVIVIENDA

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD BANCO DAVIVIENDA PARA PROVEEDORES Y TERCEROS

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD BANCO DAVIVIENDA PARA PROVEEDORES Y TERCEROS

1. Objetivo

Proveer los lineamientos para la gestión de la seguridad de la información y ciberseguridad que debe cumplir todo proveedor y/o tercero que preste un servicio o tenga cualquier tipo de vinculación contractual con Davivienda y para lo cual requiera acceder a cualquier a tipo de información de Davivienda.

2. Alcance

La presente política aplica para los proveedores o terceros de Davivienda que consulten, procesen, almacenen, distribuyan o realicen cualquier tipo de operación sobre la información de Davivienda para la prestación de sus servicios o la ejecución de sus obligaciones contractuales.

3. Normas generales

Los lineamientos estratégicos de Seguridad de la Información y ciberseguridad del Davivienda están orientados a la protección de la información, por ser ésta, uno de los activos de negocio más importantes, esto se logra mediante la institucionalización de políticas y normas que regulen su adecuado tratamiento, de manera que se pueda minimizar su exposición a los diferentes riesgos mediante la generación de una cultura de Seguridad de la Información en los proveedores y/o terceros con los que se tiene un vínculo contractual.

A continuación, se establecen las Políticas Generales de Seguridad de la Información y Ciberseguridad que deben cumplir los terceros o proveedores del alcance:

POLÍTICAS, NORMAS Y ESTÁNDARES DE SEGURIDAD

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA debe contar con Políticas, Normas y Estándares de Seguridad de la Información y Ciberseguridad al interior de su organización; las cuales deben desarrollarse y mantenerse actualizados acorde a los riesgos a los que se ve enfrentada su Organización.

ESTRUCTURA DE SEGURIDAD DE LA INFORMACIÓN

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA debe contar con una estructura de Gestión para iniciar y controlar la implementación de la Seguridad de la Información y Ciberseguridad dentro de su Organización.

ACUERDOS DE CONFIDENCIALIDAD

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA debe velar por el cumplimiento y revisión periódica de los acuerdos de confidencialidad establecidos con DAVIVIENDA, con motivo de la prestación del servicio, con el fin de proteger la información de DAVIVIENDA a la cual tiene acceso.

GESTIÓN DE ACTIVOS DE INFORMACIÓN

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA debe propender por la protección de los activos de información contra amenazas y vulnerabilidades que puedan afectar su Confidencialidad, Integridad y/o Disponibilidad.

CRIPTOGRAFÍA

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA debe establecer métodos criptográficos y/o mecanismos de cifrado para salvaguardar la confidencialidad, integridad y validez de la información confidencial cuando ésta se almacene, transmita o procese.

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN EL RECURSO HUMANO

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA debe mantener un programa de capacitación y transformación de la cultura en Seguridad de la Información y Ciberseguridad al interior de su organización.

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA debe velar por que sus empleados al servicio de DAVIVIENDA cumplan con sus responsabilidades en Seguridad de la Información.

SEGURIDAD FÍSICA Y AMBIENTAL

Todo proveedor y/o tercero que preste servicios en áreas físicas de DAVIVIENDA debe portar siempre el carné que los acredita como empleados de la empresa prestadora y permanecer únicamente en las áreas físicas donde debe desarrollar la labor relacionada con el servicio prestado.

GESTIÓN DE OPERACIONES

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA debe contar con la adecuada gestión de las Operaciones de acuerdo a las mejores prácticas, para mantener activos los servicios de Seguridad en todo momento.

SEGURIDAD DE LAS COMUNICACIONES

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA debe establecer medidas de seguridad en las comunicaciones con el propósito de proteger el intercambio y la transmisión de información, estas medidas deben estar orientadas a salvaguardar la infraestructura de la red, proteger los datos durante su transmisión, garantizar la seguridad de las operaciones en línea y vigilar los canales de comunicación para detectar posibles fallos de seguridad.

Todos los Canales de comunicación que establezca un proveedor y/o tercero con DAVIVIENDA deben contar con mecanismos que brinden seguridad y confianza a DAVIVIENDA. Deben cumplir con las normas de Seguridad de protección de la información en cuanto a Confidencialidad, Integridad y Disponibilidad.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Todas las soluciones tecnológicas de proveedores y/o terceros que vayan a ser utilizadas por DAVIVIENDA deben aplicar una metodología formal de desarrollo y mantenimiento de sistemas de información, en la que se haya considerado desde su inicio la seguridad de la información y ciberseguridad a fin de mantener la Integridad, Confidencialidad y Disponibilidad de la Información en todo su ciclo de vida.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Todo Proveedor y/o tercero que preste servicios a DAVIVIENDA tiene la responsabilidad de cumplir con los procedimientos definidos por DAVIVIENDA para la Gestión de Incidentes y utilizarlos cuando se presente una situación que pueda comprometer los activos de información de Davivienda.

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Todo proveedor y/o tercero que esté relacionado con los procesos y activos críticos para el negocio de DAVIVIENDA, debe contar con un Plan de Continuidad del Negocio y estar preparados para enfrentar ataques contra la Seguridad de la Información.

GESTIÓN DEL RIESGO

Todo proveedor y/o tercero que preste servicios a DAVIVIENDA en los que acceda a información del Banco debe contar con procedimientos para la gestión de los riesgos a los que está expuesta la información con el propósito de que estos sean identificados, analizados, evaluados, tratados y monitoreados acuerdo con su severidad, probabilidad de ocurrencia e impacto en el negocio y definir e implementar los controles necesarios para llegar al nivel de riesgo aceptable

CUMPLIMIENTO DE REGULACIONES VIGENTES

Todo Proveedor y/o tercero que preste servicios a DAVIVIENDA debe cumplir con las regulaciones locales e internacionales de Privacidad, Seguridad de la Información y Ciberseguridad.