Fecha de última modificación 19-08-2022

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CALIDAD

Pago Virtual del SUR, empresa dedicada al desarrollo de plataforma de medios de pagos electrónicos, implementa un Sistema de Gestión de la Calidad y Seguridad de la Información basado en las normas ISO 9001:2015 y PCI DSS 3,2,1 para optimizar el servicio que presta a sus clientes.

Los siguientes principios serán los lineamientos fundamentales para la calidad y seguridad de la información en **Pago Virtual del Sur**:

SATISFACCIÓN DEL CLIENTE:

Conocer y satisfacer las necesidades y expectativas de nuestros clientes, garantizando un compromiso de cumplir los requisitos establecidos por los clientes, por la legislación vigente que sea aplicable a las actividades y servicios desarrollados, los requisitos propios que nuestra organización suscriba, requisitos aplicables a la seguridad de la información, así como del cumplimiento de otras exigencias establecidas por terceras partes.

MEJORA CONTINUA:

Mejorar continuamente la eficacia del sistema de gestión, para garantizar nuestra permanente adecuación a las exigencias de un mercado cada vez más competitivo y un entorno en constante evolución.

CLASIFICACIÓN Y CONTROL DE LA INFORMACIÓN:

La información de negocio de PVS, y todos los recursos TIC relacionados, se encontrarán inventariados, tendrán asignados un propietario, y estarán clasificados según su nivel de confidencialidad y criticidad para el negocio de PVS

ADMINISTRACIÓN DE RIESGOS:

Se evaluarán los riesgos a los que están sometidos los activos TIC de PVS. El departamento de seguridad de la información en conjunto con el propietario del recurso TIC establecerán los riesgos que pueden afectar a dicho recurso, las implicancias de su exposición, modificación o acceso no autorizado y cuáles son las medidas de protección que se implementarán de acuerdo con el análisis de riesgo efectuado.

SEGURIDAD DEL PERSONAL:

Se informará al personal de PVS, ya sea efectivo o contratado, o perteneciente a empresas proveedoras de PVS, desde el momento de su ingreso de las responsabilidades y derechos en materia de uso y

protección de los recursos TIC de la Compañía. Se capacitará con el fin de crear conciencia acerca de la importancia que adquiere este aspecto para la Compañía. Se realizará un seguimiento del uso que se hace de los recursos TIC para impedir daños e interferencias, evitando así, interrupciones en las actividades de PVS

SEGURIDAD FÍSICA Y DE ENTORNO:

Se protegerán adecuadamente todos los recursos TIC y las áreas donde estos residen para evitar accesos no autorizados y daño intencional o fortuito, a través de medidas de protección acorde con la clasificación de criticidad, confidencialidad y riesgo otorgado a cada recurso.

ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES:

Se asegurará la integridad y disponibilidad de los servicios y comunicaciones para garantizar un correcto procesamiento de la información, resguardando la confidencialidad de la misma.

CONTROLES DE ACCESO:

El acceso a los recursos TIC será restringido de acuerdo con los requerimientos de control establecidos por sus propietarios y con la necesidad de saber a fin de utilizarlos. Dicho acceso se asegurará a través de procesos de autenticación, autorización, monitoreo y posterior auditoria.

DESARROLLO Y MANTENIMIENTO DE SISTEMAS:

Los principios de seguridad de la información serán incorporados a los sistemas aplicativos en todo el ciclo de vida de los mismos, incluyendo los procesos de desarrollo, prueba, mantenimiento y puesta en producción de los sistemas aplicativos. Se prevendrán pérdidas, modificaciones o uso inadecuado de los datos, proyectos y sistemas aplicativos de PVS.

ADMINISTRACIÓN DE LA CONTINUIDAD DE NEGOCIO:

Se desarrollarán y mantendrán los planes de recuperación tecnológica y continuidad de negocio, de forma tal de poder responder a eventos no deseados que impacten de manera negativa sobre los procesos de negocio críticos para PVS.

CONFORMIDAD CON LEYES, REGULACIONES Y NORMAS INTERNAS:

Se garantizará que la utilización de los recursos TIC no provoquen infracciones o violaciones de leyes, regulaciones, ni de las obligaciones establecidas por estatutos, normas, reglamentos o contratos vigentes en cada ámbito de actuación. Asimismo, se evaluará y asegurará el cumplimiento de las normas internas (políticas, estándares, procedimientos) relativos a la seguridad de la información y a la calidad de nuestros productos y servicios.