SERVICIOS POSTALES NACIONALES S.A.
TERMINOS DE REFERENCIA PROCESO DE CASILLERO VIRTUAL
GERENCIA DE RIESGOS Y CUMPLIMIENTO
SUBPROCESO SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD
Marzo 12 de 2021

Términos de Cumplimiento en Seguridad de la Información y Ciberseguridad	Cumple (SI/NO)	Relacione y adjunte documentación y evidencias
El proponente posee acción y respuesta con base a las etapas de gestión de Incidentes para la Seguridad de la Información y Ciberseguridad. (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
El proponente posee un SIEM y realiza monitoreo continuo ante amenazas de seguridad y ciberseguridad emergentes. (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
El proponente posee controles de ciberseguridad y ciberdefensa, cuales tiene implementados y de que Norma técnica están basados. (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
El proponente realiza análisis y evaluación de riesgos de sus activos de información con base a metodología ISO 27001. (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
El Proponente realiza monitoreo 7x24x365 de sus activos de información y de tecnología para garantizar la disponibilidad, confidencialidad e integridad de la información y los datos personales de los clientes. (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
El Proponente a través de su CISO (Director de Seguridad de la Información y Ciberseguridad) aplica las recomendaciones e implementa los proyectos de inversión requeridos para prevenir la materialización de riesgos de seguridad de la información, privacidad de la información y ciberseguridad. (Adjuntar copia de la Hoja de Vida, contrato laboral y manual de funciones del CISO)		
Durante el proceso de investigación y análisis de incidentes el Proponente a través de sus sistemas de seguridad puede detectar que hubo perdida de confidencialidad y la integridad de los datos de los clientes. (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		

El Proponente posee planes de contingencia, de recuperación y continuidad del negocio ante ataques informáticos y cibernéticos.		
¿Se realizan los backups de la información, servidores y de los sistemas de información? (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
¿Poseen un ambiente preproductivo o de alta disponibilidad aislado de las redes principales, para ser habilitado en caso de ataques cibernéticos o informáticos? (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
El Proponente este certificado en la Norma ISO 27001:2013 con relación a los servicios que se prestaran a SPN 4-72? (Adjuntar la certificación ISO27001)		
El Proponente posee un SOC (Centro de Operaciones de Seguridad o Ciberseguridad)? (Adjuntar copia del Servicio Contratado)		
El Proponente cuenta con un equipo CSIRT (Equipo de Respuesta a Incidentes de Seguridad) que ayuda minimizar el impacto de los incidentes de seguridad de la información y ciberseguridad en sus procesos? (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
El Proponente bajo que modelo o framework de ciberseguridad (NIST o CIS) implementa mecanismos y mejores practicas técnicas para proteger sus activos de información? (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
El Proponente posee políticas, directivas y procedimientos de Seguridad de la Información y Ciberseguridad aprobados por la Alta Direccion y Junta Directiva? (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
¿Se realizan pruebas de continuidad ante ataques cibernéticos o informáticos? (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
¿La Junta Directiva y la Alta Dirección conoce el impacto al negocio que pueden conllevar los riesgos de seguridad de la información y ciberseguridad en la entidad? (Adjuntar soportes, procedimientos y/o copia de servicios contratados)		
El Proponente y/o sus proveedores relacionados con servicios de pagos electrónicos se encuentran certificados en PCI DSS?		

(Adjuntar procedimientos y/o copia de servicios contratados)		
¿Los canales digitales que suministra los servicios de casillero virtual posee controles de seguridad y ciberdefensa contra el ransomware, phishing, protección de marca y pharming? (Adjuntar procedimientos y/o copia de servicios contratados)		
El proponente asegura los datos de las tarjetas de crédito de los clientes están asegurados ante ataques cibernéticos? (Adjuntar procedimientos y/o copia de servicios contratados)		
El proponente garantizan que la información de las tarjetas de crédito no van a ser clonadas, perdida o robadas? (Adjuntar procedimientos y/o copia de servicios contratados)		
El proponente garantiza que los datos que se pierdan se van a recuperar de manera natural propendiendo por la integridad y encripción de la información? (Adjuntar procedimientos y/o copia de servicios contratados)		
El proponente realiza seguimiento legal y jurídico ante los incidentes de seguridad de la información y ciberseguridad? (Adjuntar procedimientos y/o copia de servicios contratados)		
El Proponente asegura que las notificaciones divulgadas por correo o cualquier otros medio de comunicación hacia los clientes sean auténticos y seguros de confiar? (Adjuntar procedimientos y/o copia de servicios contratados)		
Durante y después de un ataque cibernético garantizan que la información de los paquetes o envíos de los clientes no va a ser alterada o modificada, salvaguardando la integridad de la información? (Adjuntar procedimientos y/o copia de servicios contratados)		
El proponente posee una Póliza de Ciberseguridad o Seguridad de la Información para minimizar los riesgos de la información con relación a los servicios de casillero virtual que se prestan. (Adjuntar procedimientos y/o copia de servicios contratados)		
El proponente realiza ejercicios de Ethical Hacking continuamente hacia sus activos de información, como mínimo dos veces al año. (Adjuntar procedimientos y/o copia de servicios contratados)		