ENTIDAD DE REGISTRO

POLÍTICA DE SEGURIDAD V 1.4

Nombre del documento	Política de Seguridad
Realizado por	GIRASOL PE SCRL
Aprobado por	Responsable de la ER
Código del documento	ER-PS-21032025
Versión	1.4
Fecha	24/01/2025

HISTORIAL DE VERSIÓN		
Versión	**Fecha**	**Descripción**
1.0	01/12/2019	Documento inicial
1.1	01/10/2021	Actualización del documento.
1.2	01/01/2022	Actualización del documento.
1.3	24/01/2025	Se actualiza la introducción
1.4	21/03/2025	En la Sección 1.1 Presentación se agrega certificado de constitución sacs.

INDICE

1. INTRODUCCIÓN

GIRASOL PE SCRL a la que denominaremos "GIRASOL.PE", es una empresa peruana establecida en 2019, dedicada a brindar servicios de Gestión Documental, Trámite Documentario Electrónico, Seguridad Digital, Certificados Digitales y Firma Electrónica.

En el año 2020 GIRASOL.PE logró acreditarse como Entidad de Registro ante la Autoridad Administrativa Competente como Entidad de Registro para brindar a sus clientes servicios de registro o verificación, incluidos representantes legales, empleados o agentes automatizados.

En el año 2023 GIRASOL.PE logró acreditar su software de firma digital Firmeasy (Firma Digital versión 1.0) ante la Autoridad Administrativa Competente desde donde se puede firmar documentos PDF con validez jurídica.

En el año 2024 GIRASOL.PE logró acreditarse como Entidad de Certificación ante la Autoridad Administrativa Competente para proveer servicios de emisión, re-emisión y revocación de certificados digitales.

Los tipos de certificados digitales que proporciona GIRASOL.PE son:

Certificados Digitales de Persona Natural
- Para Persona Natural.
- Para Profesional Independiente
- Para Constitución S.A.C.S
Certificados digitales de Persona Jurídica.
- Para Representante Legal
- Para Vinculación a una entidad
- Para Agente Automatizado
- Para Profesional vinculado a una entidad

- Para Facturación electrónica

GIRASOL.PE adecua sus servicios de certificación digital de acuerdo a las siguientes normativas:

- Guía de Acreditación de Entidades de Registro o Verificación, Entidad de Certificación Digital y Software de Firma Digital del INDECOPI.
- Ley 27269 - Ley de firmas y certificados digitales.
- Decreto Supremo N. 052 - 2008 - PCM Reglamento de la Ley de firmas y Certificados Digitales.
- ETSI EN 319 412-1 (Certificate Profiles; Part 1: Overview and common data structures).

La estructura de este documento está basada en la especificación del estándar RFC 3647- Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

2. VISIÓN GENERAL

Este documento tiene como objetivo describir las operaciones y prácticas utilizadas por GIRASOL.PE como entidad de registro o verificación ER para la gestión de servicios en el marco del cumplimiento de los requisitos de las "Guías de Acreditación de Entidades de Registro o Verificación (ER) " establecida por INDECOPI.

3. ALCANCE

El alcance de la acreditación cubre los servicios de registro que utiliza GIRASOL.PE en la entrega de sus servicios, y que son proporcionados por las Entidades de Certificaciones de LLAMA.PE y GIRASOL.PE.

4. DEFINICIONES Y ACRÓNIMO

- Entidad de certificación – EC

Entidad que brinda la emisión, revocación, renovación, modificación y suspensión de servicios de certificados digitales en el marco de la normativa establecida por IOFE.

- Entidad de registro – ER

  Entidades que realizan el proceso de verificación de identidad de solicitantes de servicios de certificación digital.

- Política de Certificación

  Un conjunto de reglas que indican el marco de aplicabilidad del servicio para la comunidad de usuarios definida.

- Titular

  Una entidad que requiere los servicios provistos por la EC y acepta los términos y condiciones del servicio descrito en este documento.

- Tercero que confía

  Una persona que recibe documentos, registros o notificaciones firmados digitalmente y cree en la validez de las transacciones realizadas.

  Nótese que el término de “titular” de certificado es válido únicamente en el marco de la normativa peruana y su significado se puede desprender a partir de la siguiente cita. Del DS No 052-2008-PCM, “Reglamento de la Ley de Firmas y Certificados Digitales”: Artículo 9°- Del suscriptor dentro de la Infraestructura Oficial de Firma Electrónica, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado.

  En el caso de personas jurídicas, éstas son titulares del certificado digital. Los suscriptores son las personas naturales responsables de la generación y uso de la clave privada, con excepción de los certificados digitales para su utilización a través de agentes automatizados, situación en la cual las personas jurídicas asumen las facultades de titulares y suscriptores del certificado digital. De lo anterior se puede desprender que el titular del certificado es el responsable de los efectos jurídicos generados por la

utilización de un certificado digital.

5. PKI PARTICIPANTES

5.1. Entidad de certificación

LLAMA.PE y GIRASOL.PE, como entidad certificadora autorizada, es una entidad jurídica privada que proporciona los servicios de producción, emisión, gestión, cancelación u otros servicios de certificación digital.

5.2. Entidad de registro

GIRASOL.PE presta los servicios de una entidad de registro que se encarga de verificar la identidad y los poderes de representación del solicitante, para acreditar la validez de la información proporcionada por el solicitante del certificado digital.

5.3. Proveedor de servicios de certificación digital

Un prestador de servicios de certificación es un tercero que presta su infraestructura o servicios tecnológicos a la Entidad de Registro GIRASOL.PE, siempre que la entidad requiera y garantice la continuidad de los servicios prestados a suscriptores y titulares (siempre que hayan contratado servicios de certificación digital).

Actualmente, los servicios de certificación digital que prestará GIRASOL.PE serán provistos por la entidad certificadora Llama.pe y Girasol.pe

5.4. Titular

Titular es la persona natural o jurídica a cuyo nombre se le atribuye el certificado digital y por tanto actúa como responsable del mismo confiando

en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la CPS de LLAMA.PE y GIRASOL.PE.

La figura de Titular será diferente dependiendo de los distintos certificados

emitidos por GIRASOL.PE, como prestadores de servicios de LLAMA.PE y GIRASOL.PE.

5.5. Suscriptor

Según IOFE, el suscriptor es responsable de utilizar la clave privada, que está específicamente vinculada a un documento electrónico que se firma digitalmente con su clave privada. Si el titular del certificado digital es una persona natural, la responsabilidad del suscriptor recaerá sobre él. Si la persona jurídica es la titular del certificado digital, la responsabilidad del suscriptor correrá a cargo del representante legal designado por la entidad. Si el certificado está diseñado para ser utilizado por un agente automatizado, la propiedad del certificado y la firma digital generada a partir del certificado corresponderá a la persona jurídica. A tal efecto, la atribución de la responsabilidad del suscriptor corresponde a la misma persona jurídica.

5.6. Signatario

Se entenderá por solicitante a la persona natural o jurídica que haya obtenido un certificado emitido por CPS bajo LLAMA.PE y GIRASOL.PE. Si se trata de un certificado de persona natural, puede coincidir con la identidad del titular.

5.7. Partes de confía

Son las personas que jurídicas o naturales que deciden optar por servicio de validación y de registro de la ER DE GIRASOL PE, así como los certificados digitales emitidos por la EC LLAMA.PE y GIRASOL.PE, el tercero que confía podría ser titular como no también.

5.8. Entidad a la que se encuentra vinculado el titular

En su caso, la persona jurídica u organización que tenga una relación cercana con el titular a través de la relación acreditada en el certificado.

6. CERTIFICADO DIGITAL

GIRASOL.PE brinda servicios de verificación y registro para usuarios que requieran la emisión, renovación, revocación y distribución de certificados digitales proporcionados por las entidades de certificación de LLAMA.PE y GIRASOL.PE.

7. OBLICACIÓN DE GIRASOL.PE

GIRASOL.PE es responsable de verificar la identidad del suscriptor y / o titular y brinda los servicios de registro o verificación conforme a las guías de acreditación, y el almacenamiento de la información física generada por la ejecución del proceso de ER GIRASOL PE. Si existe un incidente de seguridad que afecte los servicios prestados a ER a través de deberes, garantías financieras y coberturas de seguros, deberá ser asumido por la EC correspondiente.

Girasol.pe cuenta con línea telefónica o correo electrónico para que pueda decepcionar las peticiones, quejas o reclamos de los suscriptores y titulares, así como los mencionados podrían acercarse a la oficina de ER de Girasol.pe, indicando su queja o reclamo o petición.

8. POLÍTICA DE LA INFORMACIÓN

El objetivo de seguridad de Entidad de Registro es garantizar la autenticidad e integridad de la información clave en el proceso de registro a través de la gestión de los riesgos de seguridad y la aplicación de políticas y estándares para las actividades clave de las operaciones de marca de tiempo estandarizadas por parte de los empleados y terceros subcontratados. Cumplir con las obligaciones de ER en materia de leyes, reglamentos y contratos.

De acuerdo con la identificación y evaluación de los activos en la operación del registro, así como la identificación de las amenazas y vulnerabilidades de estos activos clave, la evaluación del impacto del riesgo, ya se pueden esperar las

medidas de control ER que ocurra durante el proceso de registro Impacto severo y moderado.

9. SEGURIDAD FÍSICA

9.1. Ubicación del local

La ubicación y el diseño de las instalaciones de la Entidad de Registro deben anticipar inundaciones, terremotos y otros desastres naturales; y desastres provocados por el hombre, como incendios, disturbios provocados por el hombre y otras formas de desastres, de modo la ER GIRASOL.PE debe contar con el reconocimiento previo por parte del Instituto Nacional de Defensa Civil permanece válido.

9.2. Seguridad física del personal y el equipamiento

Con el fin de proteger al personal y equipos en las instalaciones de la ER, es decir, para garantizar la seguridad personal de los equipos y del personal, se deben implementar las siguientes medidas de control:

- Señalización del área segura.
- Equipado con extintores.
- No debe haber cables expuestos.
- Uso de estabilizador y supresor de sobretensiones.
- Se cuenta con certificado de defensa civil vigente cumpliendo los controles de infraestructura evaluados por INDECI el cual se mantiene vigente.

9.3. Equipos informáticos

Los equipos informáticos se encuentran en ambientes restringidos y es utilizado por personal autorizado, el acceso a terceros es autorizado a través del registro de visitantes.

Los equipos informáticos son sometidos a mantenimiento como mínimo una vez por personal externo bajo supervisión.

Cuando ya no se utilice un equipo se procederá a realizar un formato de bajo nivel u otro tipo para que la información dentro del equipo no pueda ser recuperada.

Las computadoras deben tener un bloqueo automático como máximo de 7 minutos después de la sesión iniciada.

9.4. Perímetros de seguridad y control de acceso físico

El área de archivo de documentos en papel y documentos electrónicos debe protegerse continuamente para evitar el acceso no autorizado:

- Se encuentra en oficina separada con respecto al área de atención al público.
- Solo el personal autorizado puede ingresar.
- Se deben registrar las entradas y salidas del personal.
- Pueden ingresar terceros y personal de limpieza bajo la autorización del Supervisor de seguridad, deben estar identificados, y deben estar registrados y supervisados durante su ingreso al área.
- La entrada y salida de documentos del armario deben registrarse
- Debe estar bloqueado cuando no esté en uso.
- Al asignar nuevo personal se debe verificar su historial, realizar un proceso de inducción sobre los permisos y seguridad, documentos normativos de la ER y las funciones que les competen.

Las operaciones de verificación y registro se pueden realizar en la organización del cliente o en cualquier otro lugar definido por el cliente en presencia del operador de registro Equipos informáticos, y el operador de registro será responsable de proteger la información proporcionada por el cliente.

9.5. Protección contra la exposición al agua

La instalación debe protegerse de la exposición al agua. En particular, el área de archivo debe mantenerse alejada del área de ingreso de agua o

humedad en el techo o la pared contigua.

9.6. Protección contra incendios

La instalación debe tomar las siguientes medidas de protección y contra incendios:

a) Está prohibido fumar o generar humo o fuego en el área de archivos y sala de emergencias.
b) Debe haber un extintor de incendios visible para extinguir incendios en equipos electrónicos y documentos en papel.
c) Las copias de documentos y archivos electrónicos que tengan los requisitos del registrador y el contrato entre el titular y el suscriptor deben guardarse en un lugar de emergencia protegido por la persona responsable de ER para evitar el acceso no autorizado.

9.7. Archivo de material

Los documentos electrónicos y en papel (contratos de suscriptor y solicitudes de servicio de registro) y los materiales especiales (en formato de membrete específico de ER) deben estar protegidos en el área de archivo, contenedores a prueba de fuego y deben estar ubicados en múltiples lugares para eliminar la siguiente posición A relacionada arriesgar.

Solo el personal autorizado debe tener acceso a estos contenedores.

9.8. Gestión de residuos

Documentos electrónicos y en papel (contrato de abonado y solicitud de servicio de registro) y materiales especiales (formato de membrete ER) que deben ser eliminados o destruidos de manera irreversible.

9.9. Copia de seguridad externa

Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y

suscriptores debe ser guardada en un lugar de contingencia protegida por el responsable de la ER, contra acceso no autorizado.

10. GESTIÓN DE ROLES

10.1. Roles de confianza

El rol de confianza debe definirse de la siguiente manera:

- Persona responsable
- Supervisor de seguridad
- Responsable de la privacidad de los datos.
- Ejecutivo de registro
- Auditor

Estos roles deben ser asignados formalmente por el jefe de la ER.

La descripción de los roles debe incluir tareas que pueden y no pueden realizarse al desempeñar estos roles, y aquellos que realizan las funciones anteriores deben realizar claramente las mismas tareas. Se debe obtener una prueba escrita de sus conocimientos.

10.2. Número de personas requeridas por labor

Los cambios en los documentos normativos requieren la autorización del responsable de Urgencias y del responsable de seguridad y privacidad, roles que no son incompatibles y pueden ser asumidos por el mismo puesto.

El auditor siempre debe ser una persona independiente en el funcionamiento del registro.

10.3. Identificación y autenticación para cada rol

Los roles confiables deben usar control de acceso físico para acceder a áreas de archivos y control de acceso lógico para comunicarse con CI. El control de acceso al sistema de registro depende de la configuración del sistema de cada CB en lugar de ER.

10.4. Roles que requieren funciones por separado

El auditor asignado por INDECOPI debe ser siempre una persona independiente en el funcionamiento del registro.

11. GESTIÓN DEL PERSONAL

11.1. Acuerdos de confidencialidad

Se debe exigir a los empleados y contratistas que cumplan las cláusulas de confidencialidad y las regulaciones de no divulgación de información confidencial o privada, así como las regulaciones que rigen las transacciones en el marco de la IOFE, las regulaciones relacionadas con el sistema de trabajadores y los derechos de privacidad establecidos en el Anexo 6 de las Directrices de certificación de ER Cualquier otra ley relevante en la que se basan los estándares marco.

Esta información debe proporcionarse a sus empleados y contratistas por escrito, y las declaraciones escritas sobre toda esta información deben obtenerse de estas personas.

Esta información debe incluirse en todos los contratos de trabajo o servicios.

11.2. Cualidades y requisitos, experiencia y certificados

El rol de confianza debe tener conocimiento y capacitación sobre operaciones de registro digital, políticas de seguridad de la información y políticas y planes de privacidad de datos.

Del mismo modo, deben tener experiencia relacionada con problemas de autenticación digital.

11.3. Procedimiento para verificación de antecedentes

Los antecedentes de todos los empleados, contratistas y candidatos externos deben ser verificados de acuerdo con las leyes vigentes y regulaciones relacionadas, quienes deben participar y tener acceso al

sistema de operación y registro, incluyendo:

- Investigación de antecedentes penales
- Verificación de antecedentes policiales
- Verificación de antecedentes crediticios

Quienes desempeñan el papel de confianza deben conocer la sensibilidad y el nivel de valor de los activos y transacciones protegidos por las actividades de las que son responsables.

11.4. Requisitos de capacitación

Todos los empleados de las organizaciones que participan en el servicio de registro deben recibir la formación adecuada relacionada con sus funciones laborales y actualizar periódicamente las políticas y procedimientos de la organización:

- El equipo y el software necesarios para su funcionamiento.
- Todos los aspectos de RPS, políticas de seguridad, planes de privacidad y otros documentos relacionados que afectan las funciones de RPS.
- Requisitos legales sobre sus funciones.
- Su papel en la planificación de emergencias.
- Cambiar permanentemente la contraseña del correo electrónico.

11.5. Frecuencia y requisitos de las capacitaciones

Los cursos de formación deben realizarse una vez al año, y deben realizarse cuando el contenido cubierto por la formación inicial cambie significativamente, y cada vez que el personal responsable se incorpore, cambie o roten.

11.6. Frecuencia y secuencia de la rotación en el trabajo

No se implementará la rotación de trabajadores.

Si hay nuevos trabajadores, serán capacitados antes de las actividades

designadas.

11.7. Sanciones por acciones no autorizadas

Para los empleados que implementan violaciones de seguridad, acciones no autorizadas reales o potenciales y son realizadas por una persona en un rol de confianza, debe haber un procedimiento disciplinario formal y la persona debe ser suspendida inmediatamente de cualquier rol que confíe en mí.

Las sanciones antes mencionadas deben estar estipuladas en el contrato de cada empleado y / o contratista.

11.8. Requerimiento de los contratistas

El personal contratado para fines específicos en la operación de ER será evaluado por antecedentes penales, conocimientos y experiencia. Del mismo modo, no debería tener derecho a acceder al área de archivo, ni tendrá derecho a acceder al sistema de registro proporcionado por EC.

11.9. Documentación suministrada al personal

El personal debe contar con la documentación necesaria para el desempeño de sus funciones:

- Declaración de responsabilidad y autorización.
- Manuales de los equipos de software que se deben operar.
- Todos los aspectos de RPS, políticas de seguridad y otros documentos relacionados con funciones.
- Normativa aplicable a sus funciones.
- Documentos sobre su papel en la planificación de emergencias.

12. PROCEDIMIENTOS DE REGISTRO DE AUDITORIAS

12.1. Tipos de eventos registrados

CB proporciona un sistema de información confidencial, por lo que solo se

puede acceder a ER a través de la Web. En este sentido, el registro de auditoría es gestionado y definido por CB.

El contrato entre el propietario y el suscriptor y los requisitos para el proceso de registro se conservarán como evidencia de las transacciones y auditorías realizadas.

ER genera informes para los siguientes eventos:

- Proximidad física a áreas sensibles.
- Cambios personales.
- Informe completo sobre intentos de intrusión física en la infraestructura que soporta el sistema de autenticación.
- El registro de auditoría de eventos debe registrar la hora, la fecha y el identificador de software / hardware.

12.2. Frecuencia del procesamiento de registro

El registro de auditoría debe procesarse y revisarse al menos una vez al mes para detectar actividad sospechosa o inusual.

El manejo de los registros de auditoría debe incluir la verificación de que dichos registros no han sido manipulados.

12.3. Periodo de conservación del registro de auditorías

El contrato entre el suscriptor y el titular y los requisitos para el proceso de registro deben conservarse durante al menos diez (10) años.

12.4. Protección del registro de auditoría

Se protegerá el área de almacenamiento del contrato de suscriptores y titulares y las solicitudes del proceso de registro para evitar el acceso no autorizado, y se registrará la entrada y salida de personal.

Siempre que hayan transcurrido al menos 10 años, la destrucción de los documentos de auditoría solo podrá realizarse con la autorización del INDECOPI.

12.5. Copia de seguridad del registro de auditoría

Todas las solicitudes y contratos físicos serán generados con copia y los documentos electrónicos tendrán una copia por los Operadores de Registro. Las copias serán almacenadas en un lugar diferente como contingencia, protegidas contra acceso no autorizado por el responsable de la ER.

12.6. Auditoría

Las auditorías internas se realizarán en la sala de emergencias al menos una vez al año.

La evaluación técnica de INDECOPI se realizará una vez al año, siempre que INDECOPI lo requiera.

12.7. Notificación al titular que causa un evento

Las notificaciones automáticas dependen de los sistemas de la EC, para todos los eventos relacionados con el uso de los certificados por parte de un titular.

13. ARCHIVO DE REGISTROS

13.1. Tipos de documentos archivados

ER almacena los siguientes documentos:

- Todos los datos relacionados con el certificado, incluidos los contratos suscriptor / titular.
- Datos relacionados con su identidad.
- Solicitudes de emisión y revocación de certificados.
- Estado de la certificación.
- El tipo de documentos proporcionados en la solicitud de certificado.
- El número de identificación único proporcionado en el documento anterior.
- Todos los certificados emitidos o emitidos.

- Clave pública de CI.
- Pista de auditoría.
- Políticas y prácticas de certificación.

13.2. Periodo de conservación

Cualquier información indicada en el certificado, contrato con el suscriptor y el tipo de sección del evento archivado se conservará durante al menos (10) años.

13.3. Protección del archivo

Las medidas de seguridad que se utilizarán para asegurar la confidencialidad de los datos proporcionados por suscriptores y titulares de manera física serán asignadas a personal calificado para el procesamiento y digitalización de documentos, dotándolos de valor legal (microforma) a través de un notario jurado en informática certificado por el Colegio de Abogados.

Las empresas (micro formularios) que puedan confiar en sus documentos para proporcionar valor legal para la digitalización recibirán un certificado técnico adecuado para la producción de micro formularios emitido por SGS.

1. El programa de GIRASOL.PE exportará los documentos reales del suscriptor y los transportará a la fábrica de la empresa para su digitalización.
2. El documento se traslada de la empresa contratada a un estado de elaboración y digitalización.
3. Ingresar documentos digitales en sistemas de control de calidad y metadatos.
4. El notario público juramentado firmará los documentos y actas de la reunión para acreditar los trámites seguidos.
5. Nos propusimos fabricar soportes (DVD, CD, CD, etc.)

6. Entregar el soporte y los documentos originales a GIRASOL.PE
7. Verifique los documentos recibidos con los documentos entregados y luego proceda a destruir los documentos físicos.

13.4. Destrucción de archivos

Después de la digitalización y conversión a microforma, el documento con los datos proporcionados por el suscriptor y el titular será destruido de manera segura en la sala de emergencias; este proceso será supervisado por el supervisor de seguridad y ejecutado por el custodio.

13.5. Procedimiento para obtener y verificar la información del archivo

Mensualmente, la integridad del archivo debe ser verificada.

14. RECUPERACIÓN FRENTE AL COMPROMISO O DESASTRE

14.1. Plan de contingencia

ER mantiene un plan de contingencia que define las operaciones, los recursos y los registros de personal utilizados para restablecer y mantener el proceso de emisión y retiro de inquietudes, en caso de que un evento intencional o inesperado inutilice o degrade los recursos y servicios de certificación.

El plan asegura que los servicios de registro para el proceso de emisión y revocación se puedan reanudar en un máximo de 24 horas.

Durante cada auditoría o evaluación de compatibilidad, el plan debe evaluarse al menos una vez y los resultados deben proporcionarse al auditor o consultor de compatibilidad junto con información sobre las acciones correctivas que puedan ser necesarias.

14.2. Compromiso de la clave privada

Si la clave privada de un empleado en un rol de confianza se ve

comprometida, se debe revocar el certificado y se debe solicitar un nuevo certificado.

15. CONFIDENCIALIDAD DE LA INFORMACIÓN DE LA ER

15.1. Información considerada confidencial

ER mantiene la siguiente información confidencial: Materiales de ER conservados comercialmente: planes y diseños de negocios, información de propiedad intelectual e información que puede dañar sus operaciones normales.

- Información sobre suscriptores y titulares, incluidos los contratos, información que puede permitir a partes no autorizadas determinar la existencia o naturaleza de la relación entre suscriptores y titulares;
- Información que puede permitir que partes no autorizadas establezcan una descripción general de las actividades del suscriptor y del titular.

15.2. Información que puede ser publicada

- Para obtener información sobre la revocación o suspensión de certificados, esta publicación puede estar limitada a suscriptores legítimos, titulares o terceros de confianza sin revelar los motivos de la revocación o suspensión del certificado.
- Información del certificado (si el suscriptor ha autorizado esta información en el contrato del suscriptor) y su estado.
- La publicación puede estar limitada a suscriptores legítimos, titulares o terceros de confianza.

16. CONFIDENCIALIDAD

Este documento ha sido aprobado por la gerencia de ER. Si empleados, contratistas y terceros mencionan alguna infracción dentro del alcance de este documento, serán comunicados a la agencia para implementar

las sanciones correspondientes.