LA CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

DECLARACIÓN DE PRÁCTICAS DEL PRESTADOR DE SERVICIOS DE VALOR AÑADIDO PARA EL ESTADO PERUANO

NOTIFICACIONES ELECTRÓNICAS EN EL SISTEMA NACIONAL DE CONTROL

	NOMBRE	CARGO	FIRMA	FECHA
Elaborado por:	Gladys Linares Núñez	Profesional de la Subgerencia de Sistemas de Información	LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ Firmado digitalmente por LINARES NUÑEZ Gladys Luz FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 08.07.2020 16:04:53 -05:00	08/07/2020
	Paola Manrique Huertas	Profesional de la Subgerencia de Gobierno Digital	LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ Firmado digitalmente por MANRIQUE HUERTAS Paola Gisselle FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 09.07.2020 14:52:09 -05:00	08/07/2020
	Harry Cernades Gómez	Profesional de la Subgerencia de Operaciones y Plataforma Tecnológica	LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ Firmado digitalmente por CERNADES GOMEZ Harry Alejandro FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 09.07.2020 15:45:40 -05:00	08/07/2020
	Ricardo Salas Silva	Personal de la Subgerencia de Operaciones y Plataforma Tecnológica	LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ Firmado digitalmente por SALAS SILVA Ricardo Augusto FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 08:00:30 -05:00	08/07/2020
	César Córdova Véliz	Profesional de la Gerencia de Tecnologías de la Información	LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ Firmado digitalmente por CORDOVA VELIZ Cesar Rolando FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 11:09:50 -05:00	08/07/2020
Revisado por:	Erik Bazán Flores	Subgerente de Sistemas de Información	LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ Firmado digitalmente por BAZAN FLORES Erik Ulises FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 17:39:49 -05:00	08/07/2020
	Ricardo Balbuena Rodríguez	Subgerente de Operaciones y Plataforma Tecnológica	LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 16:57:51 -05:00	08/07/2020
	Raúl Huertas Salazar	Subgerente de Gobierno Digital	LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 16:14:21 -05:00	08/07/2020
Aprobado por:	Amparo Ortega Campana	Gerente de Tecnologías de la Información	LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ Firmado digitalmente por ORTEGA CAMPANA Amparo FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 15:17:33 -05:00	08/07/2020

Contenido

1. INTRODUCCIÓN

La Contraloría General de la República (CGR) es el órgano superior del Sistema Nacional de Control que cautela el uso eficiente, eficaz y económico de los recursos del Estado, la correcta gestión de la deuda pública, así como la legalidad de la ejecución del presupuesto del sector público y de los actos de las instituciones sujetas a control; coadyuvando al logro de los objetivos del Estado en el desarrollo nacional y bienestar de la sociedad peruana.

Conforme al artículo 16 y el literal c) del artículo 15 de la Ley N° 27785, la Contraloría es el ente técnico rector del Sistema Nacional de Control, dotado de autonomía administrativa, funcional, económica y financiera, que tiene por misión dirigir y supervisar con eficiencia y eficacia el control gubernamental; e impulsar la modernización y el mejoramiento de la gestión pública.

Asimismo, de acuerdo al artículo 4 de la Ley N° 30742, Ley de fortalecimiento de la Contraloría General de la República y del Sistema Nacional de Control, la Contraloría implementa de manera progresiva el procedimiento electrónico, la notificación electrónica, el domicilio electrónico, la casilla electrónica, la mesa de partes virtual y mecanismos similares, en los procedimientos administrativos, procesos de control y encargos legales que se encuentren bajo el ámbito de sus atribuciones, incluyendo aquellos que corresponden al TSRA, estando las personas relacionadas con dichos procesos o procedimientos obligadas a su empleo.

Por tal motivo se ha implementado el Sistema de Notificaciones y Casillas Electrónicas de la Contraloría General de la República (eCasilla-CGR), que permite informar de manera oportuna y confiable a los titulares de las casillas electrónicas sobre la recepción de notificaciones electrónicas con valor legal, de forma segura y garantizando el no repudio de las mismas. Se prevé que este sistema soportará a diversos procesos estratégicos y misionales de la Contraloría.

2. OBJETIVO

La presente Declaración de Prácticas de la Contraloría General de la República para su Prestador de Servicios de Valor Añadido para el Estado Peruano (PSVAEP) tiene por objeto describir los procedimientos y prácticas utilizados en la administración y prestación de los servicios brindados a través del Sistema de Notificación y Casilla Electrónica de la Contraloría General de la República, eCasilla-CGR, bajo el marco del cumplimiento de la Guía de Acreditación de Prestadores de Servicios de Valor Añadido (PSVA) establecida por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) como Autoridad Administrativa Competente (AAC) para la Infraestructura Oficial de Firma Electrónica (IOFE).

3. ALCANCE

La acreditación del Sistema de Notificaciones y Casillas Electrónicas de la Contraloría General de la República (eCasilla-CGR) corresponde a un Sistema de Intermediación Digital que realiza procedimientos con firma digital de usuario final, servicio brindado por la Contraloría cuando actúa como Prestador de Servicios de Valor Añadido para el Estado Peruano.

El alcance de esta acreditación cubre los sistemas, procesos, infraestructura, políticas y procedimientos del eCasilla-CGR. En este contexto se consideran todas las actividades

realizadas desde la solicitud de casilla electrónica por parte de personas naturales o personas jurídicas hasta la recepción de los documentos electrónicos en su casilla electrónica. Las personas que pueden realizar esta solicitud corresponden a personas naturales o personas jurídicas que necesiten recibir notificaciones electrónicas de las unidades orgánicas o de los órganos desconcentrados de la Contraloría General de la República o de los Órganos de Control Institucional, en lo que les corresponda.

4. SIGLAS Y DEFINICIONES

4.1. Siglas

CGR, Contraloría	**:**	Contraloría General de la República
Entidad	**:**	Entidad sujeta a control de acuerdo al artículo 3 de la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, y sus modificatorias.
Ley N° 27785	**:**	Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, y sus modificatorias
OCI	**:**	Órgano de Control Institucional
TSRA	**:**	Tribunal Superior de Responsabilidades Administrativas

4.2. Definiciones

Auxiliar de Casilla Electrónica:	Personal autorizado de los órganos, incluidos los órganos desconcentrados y el TSRA, así como las unidades orgánicas de la Contraloría, y los OCI, que valida la identidad del servidor o ex servidor público, funcionario o ex funcionario público, o titular de la entidad, así como del correcto registro de los datos, para la creación y activación de la casilla electrónica, por asignación obligatoria.
Cargo de Notificación Electrónica:	Es el documento electrónico generado por el Sistema de Notificaciones y Casillas Electrónicas de la Contraloría, cuando el Usuario Notificador realiza la notificación electrónica, como evidencia de haberse entregado la notificación en la casilla electrónica.
Casilla electrónica:	Corresponde al domicilio electrónico que la Contraloría asigna al Usuario Receptor para la recepción de notificaciones electrónicas.
Cédula de Notificación Electrónica:	Es el documento electrónico que firma el Usuario Notificador y que acompaña a los documentos electrónicos a notificar.
Código de usuario:	Identificador único que permite al Usuario Receptor acceder a la casilla electrónica.
Contraseña:	Serie de letras, dígitos y caracteres especiales de carácter confidencial que permiten al Usuario Receptor acceder a su casilla electrónica.
Correo Electrónico Personal Declarado:	Dirección electrónica registrada por el funcionario o ex funcionario público, servidor o ex servidor público, en

	los sistemas informáticos que brindan soporte a los procesos de control o procedimientos administrativos que se encuentren a cargo del Sistema Nacional de Control.
Documento electrónico:	Unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, trasmitida, procesada o conservada por la Contraloría, en virtud de sus obligaciones legales, utilizando sistemas informáticos.[1]
Firma digital:	Es aquella firma electrónica que, utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios que este mantiene bajo su control, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior. Tiene la validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado, que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica–IOFE, y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro II del Código Civil.[2]
Formato de Declaración Jurada de datos personales y autorización del uso de la casilla electrónica:	Es el documento suscrito por la persona natural o el representante legal de la persona jurídica, mediante el cual autoriza la creación y activación de la casilla electrónica, por solicitud de generación voluntaria; así también acredita haber leído los términos y condiciones de su uso.
Formato de Declaración Jurada de datos personales en el marco de la notificación electrónica en el Sistema Nacional de Control:	Es el documento suscrito por el funcionario o ex funcionario público, servidor o ex servidor público, o titular de la entidad, mediante el cual se recaba información de datos personales y acredita haber leído los términos y condiciones del uso de la casilla electrónica, por asignación obligatoria.
Funcionario o servidor:	Es el funcionario o ex funcionario público, o servidor o ex servidor público, que mantiene o mantuvo vínculo laboral, contractual o relación de cualquier naturaleza con alguna de las entidades, y que en virtud a ello ejerció o ejerce funciones en tales entidades; y que está relacionado con los procesos de control y procedimientos administrativos que se encuentren a cargo del Sistema Nacional de Control.
Operador de Casilla Electrónica:	Personal designado por la Contraloría o los OCI que, valida la identidad de la persona natural y del representante legal de la persona jurídica, para la creación y activación de la casilla electrónica, por solicitud de generación voluntaria.

[1] Décimo Cuarta Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo Nº 052-2008-PCM.
[2] Artículo 6 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo Nº 052-2008-PCM.

Proceso de control:	Servicios de control o servicios relacionados que son realizados por la Contraloría o los OCI.
Usuario Emisor:	Personal autorizado de los órganos, incluidos los órganos desconcentrados y el TSRA, así como las unidades orgánicas de la Contraloría, y los OCI, que elabora y suscribe el documento electrónico a ser notificado en la casilla electrónica de un Usuario Receptor.
Usuario Notificador:	Personal autorizado de los órganos, incluidos los órganos desconcentrados y el TSRA, así como, las unidades orgánicas de la Contraloría y los OCI, que suscribe la cédula de notificación electrónica y notifica o gestiona la notificación del documento electrónico del Usuario Emisor en la casilla electrónica del Usuario Receptor.
Usuario Receptor:	Persona natural, persona jurídica, funcionario o servidor, o titular de la entidad, a quien se le ha creado y activado la casilla electrónica.
Supervisor de Casilla Electrónica:	Personal de la Contraloría, perteneciente a la Subgerencia de Gestión Documentaria o la que haga sus veces, quien realiza las actividades de supervisión y organización de información concernientes al proceso de notificación electrónica a través del eCasilla-CGR.
Titular de la entidad:	Máxima autoridad jerárquica institucional de carácter unipersonal o colegiado en una entidad. En caso de órganos colegiados, se entenderá por titular de la entidad, a quien lo preside.

4.3. Acrónimos y abreviaturas

- **AAC** Autoridad Administrativa Competente (CFE del INDECOPI)
- **CC** Common Criteria
- **CEN** Comité Europeo de Normalización
- **CFE** Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica
- **CP** Políticas de Certificación
- **CPS** Declaración de Prácticas de Certificación de una EC
- **CRL o LCR** Certificate Revocation List (Lista de Certificados Revocados)
- **CSP o PSC** Proveedor de Servicios Criptográficos
- **CWA** CEN Workshop Agreements
- **DPSVA** Declaración de Prácticas de Servicios Valor Añadido
- **EAL** Evaluation Assurance Level
- **EC** Entidad de Certificación
- **ECEP** Entidad de Certificación para el Estado Peruano
- **ECERNEP** Entidad de Certificación Nacional para el Estado Peruano
- **ER** Entidad de Registro o Verificación
- **EREP** Entidad de Registro para el Estado Peruano

- **ETSI** European Telecommunications Standards Institute
- **FBCA** Federal Bridge Certification Authority
- **FIPS** Federal Information Processing Standards
- **HASH** Se refiere a una función o algoritmo para generar claves que representen de manera casi unívoca a un documento, registro, archivo o mensaje de datos, en forma de un Resumen Hash.
- **HSM** Hardware Security Module - Módulo de seguridad de hardware.
- **IEC** International Electrotechnical Commission
- **IETF** Internet Engineering Task Force
- **INDECOPI** Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.
- **IOFE** Infraestructura Oficial de Firma Electrónica
- **ISO** International Organization for Standardization
- **NTP** Norma Técnica Peruana
- **OCSP** Online Certificate Status Protocol (Protocolo del estado en línea del certificado)
- **OID** Identificador de Objeto
- **PKI** Public Key Infrastructure (Infraestructura de Clave Pública)
- **PSC** Prestador de Servicios de Certificación Digital
- **ROPS** Registro Oficial de Prestadores de Servicio de Certificación Digital
- **RFC** Request for Comment
- **RPS** Declaración de Prácticas de Registro o Verificación de una ER
- **RUC** Registro Único de Contribuyentes.
- **SHA** Secure Hash Algorithm
- **PSVA** Prestador Servicios de Valor Añadido
- **PSVAEP** Prestador Servicios de Valor Añadido para el Estado Peruano
- **SVA** Servicios de Valor Añadido
- **SID** Sistema de Intermediación Digital
- **TSL** Lista de Estado de Servicio de Confianza
- **TSA** Time Stamping Authority. Autoridad de Sellado de Tiempo

5. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DEL PSVA

La CGR administra y es responsable de la elaboración de todos los documentos normativos de su PSVAEP, incluyendo la presente declaración de prácticas. Cada nueva versión de estos documentos será presentada a la AAC para su revisión y aprobación antes de entrar en vigor y ser puesta a disposición de los usuarios mediante su publicación.

5.1. Persona de contacto

Responsable del PSVA
Correo electrónico: ecasilla@contraloria.gob.pe

Consultas
Teléfono: 3303000
Correo electrónico: sugerenciasecasilla@contraloria.gob.pe

6. RESPONSABLE DEL REPOSITORIO Y SU PUBLICACIÓN

La CGR gestiona el repositorio de documentos normativos de su PSVAEP, el cual es de acceso público y accesible desde internet en la siguiente dirección:

www.contraloria.gob.pe

El repositorio contiene documentos normativos de acceso público, como la Política del PSVAEP, su Declaración de Prácticas entre otros. La vigencia mínima de estos documentos es de un año contados desde el logro de la acreditación, luego de ello su reconocimiento es revalidado anualmente por las revisiones de supervisión que realiza la AAC.

La frecuencia con que se realizan las actualizaciones de sus documentos normativos queda a criterio de la CGR, quien está a cargo de su gestión. Dichas actualizaciones serán validadas en los seguimientos anuales de la AAC. En caso de cambios mayores, estos serán presentados primero a la AAC para su aprobación antes de modificar los documentos normativos respectivos.

La Contraloría no limita el acceso para lectura de los documentos normativos de su PSVA publicados en su repositorio, pero establece controles físicos y lógicos para impedir que de forma no autorizada se puedan añadir, modificar o borrar registros del mismo.

7. PARTICIPANTES

7.1. Entidades de Certificación

Entidades acreditadas ante la AAC encargadas de gestionar el ciclo de vida de los certificados, particularmente, de su emisión.

7.2. Entidades de Registro

Entidades acreditadas ante la AAC encargadas de validar la identidad de los titulares y suscriptores de los certificados digitales.

7.3. Prestador de Servicios de Valor Añadido: SID

La Contraloría, como PSVAEP acreditado ante la AAC, ofrece un Sistema de Intermediación Digital (eCasilla-CGR) que actúa como tercero de confianza, mediante el cual pone a disposición de personas naturales y personas jurídicas los servicios de notificaciones y casillas electrónicas con el propósito de garantizar la entrega confiable, oportuna y el no repudio de las notificaciones electrónicas sobre los procedimientos seguidos por los servicios de control de la Contraloría y los OCI.

7.4. Prestador de Servicios de Valor Añadido: TSA

Una Autoridad de Sellado de Tiempo acreditada ante la AAC es un tercero de confianza que proporciona la fecha y hora cierta, mediante la impresión de sellos de tiempo, con el propósito de garantizar el momento exacto en que tienen lugar las transacciones.

7.5. Comunidad de Usuarios

En general pueden ser usuarios del Sistema de Notificaciones y Casillas Electrónicas de la Contraloría (eCasilla-CGR) las unidades orgánicas y los órganos desconcentrados de la Contraloría General de la República, así como también los Órganos de Control

Institucional, los cuales requieren generar y entregar notificaciones electrónicas en lo que les corresponda. También forman parte de esta comunidad de usuarios las personas naturales o jurídicas titulares de casillas electrónicas.

7.6. Terceros que confían

Los terceros que confían son todas aquellas personas naturales o jurídicas, que requieren confirmar la validez de las notificaciones electrónicas realizadas, los acuses de recibo o los certificados empleados durante el proceso de notificación.

8. SISTEMA DE NOTIFICACIONES Y CASILLAS ELECTRÓNICAS

El eCasilla-CGR es un sistema informático administrado por la Contraloría, que automatiza las notificaciones en el marco de los procesos de control y procedimientos administrativos a cargo del Sistema Nacional de Control, permitiendo contar con un canal seguro y eficiente de notificación hacia los usuarios receptores.

Por medio de este servicio las unidades orgánicas y los órganos desconcentrados de la Contraloría, así como los Órganos de Control Institucional adscritos al sistema pueden generar notificaciones electrónicas y entregarlas a los administrados suscritos al servicio a través de sus casillas electrónicas. Existe certeza de la hora y fecha de la entrega de cada notificación electrónica, pues por cada una se genera un acuse de recibo de parte del administrador de las casillas electrónicas, el mismo que cuenta con sello de tiempo. Existe también el compromiso de los usuarios administrados de revisar periódicamente su casilla, pues la hora y fecha de entrega de la notificación corresponde al momento de su ingreso a la casilla electrónica y no a la hora y fecha de su lectura.

El eCasilla-CGR está conformado por un sistema despachador de notificación, un firmador para firma desatendida por lotes de agente automatizado, un servicio de casillas electrónicas, un sistema de gestión de usuarios.

Las funciones que ofrece el eCasilla-CGR incluyen:

- Generación y envío de notificación electrónica.
- Generación de evidencias (acuse de recibo) y reportes.
- Gestión de los usuarios del eCasilla-CGR.
- Interfaz para la navegación y administración.

Para poder hacer uso del eCasilla-CGR se necesita que:

- Cada persona natural o jurídica que requiera de este servicio debe solicitar la creación de su casilla electrónica, presentando la documentación requerida y apersonándose a una de las oficinas que la CGR disponga.
- Existe también la creación y activación de la casilla electrónica por asignación obligatoria, a los funcionarios o servidores que se relacionen con procesos de control y procedimientos administrativos, que la Contraloría o los OCI desarrollen, así como a los titulares de las entidades, según corresponda.
- Una vez inscrito el usuario receptor debe emplear las credenciales cada vez que requiera acceder a su casilla electrónica. Sus obligaciones, responsabilidades y condiciones de uso del sistema eCasilla-CGR son detallados en el contrato de afiliación.
- Los diferentes órganos de la Contraloría y OCI que requieran el servicio deben solicitar la inscripción de su personal al eCasilla-CGR como usuario emisor. Una vez dados de alta podrán emitir las notificaciones que correspondan.

De manera automática eCasilla-CGR genera un acuse de recibo firmado con certificado de agente automatizado y con sello de tiempo, cada vez que una cédula de notificación es entregada a una casilla electrónica, como evidencia del momento en que el titular de la casilla electrónica fue notificado.

El eCasilla-CGR guardará registro de los eventos relacionados con el manejo del domicilio electrónico de cada administrado:

- Se guardará fecha y hora de cada ingreso al sistema.
- Se guardará fecha y hora de cada recepción de notificación.
- Se guardará fecha y hora de cada lectura de notificación

8.1. Creación de la casilla electrónica

La creación y activación de la casilla electrónica se efectúa mediante asignación obligatoria o por solicitud de generación voluntaria.

8.1.1. Por asignación obligatoria

La creación y activación de la casilla electrónica por asignación obligatoria, a los funcionarios o servidores que se relacionen con procesos de control y procedimientos administrativos, que la Contraloría o los OCI desarrollen, así como a los titulares de las entidades, según corresponda, se efectúa conforme a lo siguiente:

1. El Auxiliar de Casilla Electrónica realiza el registro de los datos personales del funcionario o servidor, o del titular de la entidad, en el eCasilla-CGR, consignando el correo electrónico institucional o correo electrónico personal declarado, con el cual se asoció la identidad validada; creándose la casilla electrónica para su posterior activación.

   Excepcionalmente, para los casos en los que no se cuente con el correo electrónico institucional o correo electrónico personal declarado, del funcionario o servidor, o del titular de la entidad, el Auxiliar de Casilla Electrónica realiza el procedimiento de verificación de su respectiva identidad, y le hace entrega o pone a su disposición el “Formato de Declaración Jurada de datos personales en el marco de la notificación electrónica en el Sistema Nacional de Control”, a través del portal institucional u otros medios virtuales que la Contraloría estime pertinente, para su llenado y suscripción.

   A partir de la información consignada en dicho formato, el Auxiliar de Casilla Electrónica registra los datos obtenidos (entre ellos los correos electrónicos) en el eCasilla-CGR, y se crea la casilla electrónica para su posterior activación.

2. El funcionario o servidor, o el titular de la entidad recibe en su correo electrónico, un enlace para la verificación de sus datos personales, que luego de confirmarlos, y haber leído los términos y condiciones del uso de la casilla electrónica, permiten la activación de su casilla electrónica creada, para cuyo acceso recibe en su correo electrónico, sus respectivas credenciales (código de usuario y contraseña).
   Recibidas las credenciales, si la casilla electrónica se hubiese activado utilizando un correo electrónico institucional, en el primer ingreso al eCasilla-CGR con dichas credenciales, el Usuario Receptor debe registrar un correo electrónico personal.

El plazo máximo para el ingreso al enlace para la verificación de datos personales, por parte del funcionario o servidor, o del titular de la entidad, es de diez (10) días calendario, contados a partir del día en que dicho enlace es enviado. El funcionario o servidor, o el titular de la entidad puede solicitar el reenvío del enlace, mediante un mensaje al correo electrónico ecasillacgr@contraloria.gob.pe, dentro del plazo máximo indicado.

3. En caso que el funcionario o servidor, o el titular de la entidad se niegue a suscribir el "Formato de Declaración Jurada de datos personales en el marco de la notificación electrónica en el Sistema Nacional de Control" o registre en él datos incompletos o que carezcan de veracidad, o no ingrese al enlace para la verificación de sus datos personales conforme a lo indicado en el numeral 1. de la presente sección, asume la responsabilidad a que hubiere lugar, conforme a la normativa vigente.

   Sin perjuicio de la responsabilidad señalada en el párrafo precedente, se lleva a cabo la notificación conforme a los casos excepcionales en que, por razones fundamentadas del Usuario Emisor con la conformidad respectiva de la unidad orgánica u órgano de la Contraloría del cual depende, no sea posible realizar la notificación electrónica a la que se refiere el presente documento, el Usuario Notificador realiza o gestiona las notificaciones correspondientes conforme a la normativa específica que regula los procesos de control y procedimientos administrativos, y al Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, supletoriamente.

8.1.2. Por solicitud de generación voluntaria

Las personas naturales o jurídicas que requieran una casilla electrónica, y no estén comprendidas en el alcance de su uso obligatorio, pueden obtenerla mediante una solicitud de generación voluntaria.

La Contraloría se reserva el derecho de crear y activar una casilla electrónica cuando no es obligatorio el uso de ésta.

La creación y activación de la casilla electrónica por solicitud de generación voluntaria se efectúa de acuerdo con lo siguiente:

1. La solicitud de generación voluntaria comprende inicialmente un pre-registro virtual en que la persona natural o el representante legal de la persona jurídica ingresa sus datos en el eCasilla-CGR, con lo cual se efectúa la creación de la casilla electrónica, para posteriormente acercarse a una de las sedes habilitadas por la Contraloría, y así iniciar el trámite de activación de su casilla electrónica, dentro del plazo de treinta (30) días hábiles de recibida la confirmación de la solicitud de generación voluntaria.

   Vencido el plazo antes señalado sin haberse efectuado el trámite de activación, la solicitud de generación voluntaria es cancelada, por lo que la persona natural o representante legal de la persona jurídica debe realizar nuevamente la solicitud de generación voluntaria de casilla electrónica.

2. En la sede de la Contraloría, el Operador de Casilla Electrónica valida la identidad de la persona natural o representante legal de la persona jurídica, y le hace entrega del "Formato de Declaración Jurada de datos personales y autorización del uso de la casilla electrónica", para su llenado y suscripción, y consecuentemente, la persona natural o jurídica reciba en sus correos electrónicos el enlace para la activación de su casilla electrónica así como sus respectivas credenciales (código de usuario y contraseña).

8.2. Activación y vigencia de la casilla electrónica

La casilla electrónica creada es activada con vigencia indefinida. Excepcionalmente, se inactiva por fallecimiento del funcionario, servidor o persona natural, o por extinción de la persona jurídica; así como, a pedido de la persona natural cuando la casilla electrónica hubiera sido solicitada por ésta, siempre que no haya obtenido la calidad de funcionario o servidor.

Las casillas electrónicas de los titulares de las entidades tienen vigencia indefinida; y excepcionalmente, se inactivan por extinción de la entidad. Para el caso de una entidad extinta cuyas funciones son absorbidas por otra entidad, el contenido de la casilla electrónica que se inactiva es enviado a la casilla electrónica de la entidad que absorbió sus funciones; asimismo, en caso de cambio del titular de la entidad, la casilla electrónica es reasignada al nuevo titular de la entidad.

8.3. Uso de la casilla electrónica

1. El Usuario Notificador genera una cédula de notificación electrónica y la suscribe, adjuntando los documentos firmados digitalmente por el Usuario Emisor, correspondientes a los procesos de control o procedimientos administrativos, según corresponda.

   La firma digital añadida o incorporada al documento electrónico garantiza el no repudio del documento electrónico original[3], así como la integridad del contenido y permite detectar cualquier modificación ulterior[4].

2. Con la cédula de notificación electrónica y los documentos electrónicos depositados en la casilla electrónica del Usuario Receptor, se produce la notificación electrónica, generándose el cargo de notificación electrónica, que incluye la fecha y hora de la notificación electrónica, respaldado por el servicio de sellado de tiempo.

3. Al producirse la notificación electrónica, el Usuario Receptor recibe un mensaje de alerta de notificación en sus correos electrónicos u otros medios que la Contraloría disponga. La falta de envío de la alerta de notificación o su no recepción en sus correos electrónicos o medio establecido para esta finalidad, no invalida el acto de notificación realizado en la casilla electrónica.

4. En caso se presenten dificultades para acceder al eCasilla-CGR, el Usuario Receptor puede comunicarlas al correo electrónico ecasillacgr@contraloria.gob.pe.

8.4. Cargo de notificación (acuse de recibo)

Realizado el depósito del acto a notificar en la casilla electrónica, el eCasilla–CGR genera un cargo de notificación que incluye la fecha y hora de la notificación respaldado por el servicio de sellado de tiempo.

8.5. Recepción de las notificaciones electrónicas

- El usuario receptor, a través del eCasilla – CGR, visualiza principalmente la lista de notificaciones pendientes de leer, pudiendo ver el detalle de la notificación y los archivos adjuntos enviados por el usuario emisor.

[3] En el segundo párrafo del artículo 4 del Reglamento de la Ley de Firmas y Certificados Digitales, y sus modificatorias se señala: "*La firma digital generada en el marco de la Infraestructura Oficial de Firma Electrónica garantiza el no repudio del documento electrónico original.* (...)".

[4] Conforme a lo establecido en el artículo 6 del Reglamento de la Ley de Firmas y Certificados Digitales, y sus modificatorias.

- Adicionalmente, el usuario receptor podrá visualizar la lista de notificaciones leídas o recibidas.

8.6. Olvido de contraseña de acceso a la Casilla electrónica

En caso de que el usuario receptor de la casilla electrónica no pueda acceder a la misma por olvido de la contraseña de acceso, debe generar una nueva contraseña a través del eCasilla–CGR.

9. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES

9.1. Generación de las claves

La generación del par de claves para firma del agente automatizado del eCasilla-CGR se debe realizar en un ambiente provisto de las medidas de seguridad apropiadas, por personal designado que ocupe roles de confianza dentro de la entidad, empleando al menos un control de acceso dual y con los permisos limitados al cumplimiento de esta tarea.

Una vez generado el par de claves y obtenido el certificado de una EC acreditada se procederá a instalar el certificado y clave privada en un servidor con sistema operativo Windows Server, el cual estará configurado en un modo de operación compatible con FIPS 140-2.

Los detalles y procedimientos empleados en la generación de las claves se encontrarán debidamente documentados indicando entre otras cosas la identificación del personal que fuera encargado, la identificación del dispositivo criptográfico y los detalles de las claves generadas (algoritmo de generación de claves, tamaño de claves, y algoritmo de firma de su certificado).

9.2. Protección de la clave privada

La Contraloría asegura que la clave privada de firma de su agente automatizado permanece confidencial e íntegra, para lo cual:

- De usar módulo criptográfico este deberá contar con certificación FIPS 140 -2 o CWA 14167-2.
- De no usar módulo criptográfico asegurar que el medio en el que se almacene la clave privada sea compatible con FIPS 140-2.

Si se realiza un respaldo de la clave de firma, esta deberá ser copiada, almacenada y recuperada sólo por personal que ocupa roles de confianza, usando al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del PSVA.

Cualquier copia de la clave deberá ser protegida por la clave secreta del módulo criptográfico antes de ser almacenada fuera del dispositivo.

9.3. Distribución de la clave pública

La clave pública de firma del agente automatizado estará disponible para los terceros que confían a través de su certificado de clave pública.

El certificado debe ser emitido por una EC reconocida por la IOFE, bajo una política que provea un nivel de seguridad equivalente o superior a la DPSVA.

9.4. Re-emisión de la clave

En caso la EC que emite el certificado de agente automatizado soporte re-emisión de certificado, el tiempo de vigencia del mismo no debe ser mayor que el periodo de vigencia de los algoritmos y tamaños de claves, conforme al reconocimiento de la IOFE.

9.5. Término del ciclo de vida de la clave privada

La emisión de las notificaciones y acuses de recibo se realizará en plena vigencia de los certificados digitales usados, particularmente del certificado de agente automatizado del eCasilla-CGR. Se emplea un software de firma acreditado que rechazará cualquier intento de emitir una notificación o acuse de recibo si la clave privada de firma ha expirado o ha sido revocada.

Una clave privada llega al final de su ciclo de vida si:

- El certificado asociado a expirado.
- El certificado asociado ha sido revocado. Esto puede haber sido motivado debido a que la clave se ha visto comprometida, o se han detectado debilidades en su algoritmo de firma, en su algoritmo hash o en el tamaño de clave.

Cuando el certificado digital de agente automatizado llegue a su fin se realizarán las siguientes acciones:

- Se procederá a desactivar el certificado del sistema del eCasilla-CGR.
- Se programará el procedimiento de destrucción segura de la clave de dicho certificado (centros de datos Principal y Contingencia). En caso de haberse generado backup de dicha clave también deberá realizarse el borrado seguro de dicha copia.
- En paralelo se deberá gestionar la emisión de un nuevo certificado.

Para la destrucción segura de una clave privada de agente automatizado se seguirán las instrucciones propias del fabricante para el módulo de seguridad de hardware (HSM) empleado. Los procedimientos serán llevados a cabo por personal adecuado según los roles de confianza.

10. CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

La Contraloría, en caso de contar con módulo criptográfico para el sistema eCasilla-CGR, se encarga de la seguridad del hardware criptográfico a lo largo de su ciclo de vida. Particularmente se garantiza que:

- El hardware del módulo criptográfico no debe ser manipulado durante su transporte.
- El hardware del módulo criptográfico no debe ser manipulado durante su almacenamiento.
- La instalación, activación y duplicación de la clave de firma en el hardware del módulo criptográfico debe ser realizado sólo por personal que ocupa roles de confianza, usando al menos un control de acceso de dos personas en un ambiente físico seguro.
- El hardware del módulo criptográfico funciona correctamente.

- Las claves de firma que son almacenadas en un módulo criptográfico son borradas antes de que el dispositivo sea retirado y su certificado revocado de ser el caso.

11. AUTENTICACIÓN

Se emplea autenticación mediante usuario y contraseña. Se prevé que en el futuro se empleará autenticación mediante certificado digital en cuyo caso se deberá verificar la validez del mismo antes de autorizar su acceso, esto es:

- El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.
- El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no hayan expirado y no se encuentran revocados. La verificación de revocación se puede realizar mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.
- El sistema deberá verificar que el certificado del usuario final tiene como propósito autenticación, conforme a la RFC 5280.

12. CIFRADO

El eCasilla-CGR no realiza funciones de cifrado de datos mediante certificados digitales.

13. CANALES SSL

En caso de que el eCasilla-CGR implemente canales seguros SSL se deberá asegurar que:

- Al momento de descifrar la información, el sistema no copia la clave privada sin cifrar fuera del módulo criptográfico. La clave privada siempre se mantiene dentro del módulo criptográfico.
- El sistema verifica que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no permite el acceso.
- El sistema verifica que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no hayan expirado y no se encuentren revocados. La verificación de revocación se puede realizar mediante los mecanismos CRL u OCSP. En caso de ser CRL, se verifica la vigencia y autenticidad de la CRL.
- El sistema verifica que el certificado del usuario final tiene como propósito de cifrado de clave, conforme a la RFC 5280.

14. PETICIÓN DE SELLOS DE TIEMPO

Se deben cumplir requisitos que garanticen su confiabilidad:

- El formato de petición es conforme a la RFC 3161.
- El sistema verifica que el certificado con el que se firma el sello de tiempo corresponde a una Entidad de Certificación reconocida por la IOFE.
- El sistema verifica que el certificado con el que se firman los sellos de tiempo no se encuentre revocado.
- El sistema verifica que el certificado con el que se firman los sellos de tiempo no se encuentre expirado.
- El sistema verifica la firma del sello de tiempo para corroborar que los datos son íntegros.

15. GESTIÓN Y OPERACIÓN DEL SID

15.1. Gestión de la seguridad

La Contraloría asegura que los procedimientos de administración y gestión aplicados son adecuados y correspondan a las mejores prácticas reconocidas, en tal sentido:

- Mantiene bajo su control la gestión, administración u operación del eCasilla-CGR para todos los aspectos de la provisión del servicio dentro del alcance de esta política.
- Su infraestructura de seguridad de la información se basa en la ISO/IEC 27001. Cualquier cambio que pueda impactar en el nivel de seguridad es aprobado por el Responsable del PSVA.
- Garantiza la seguridad de la provisión del Servicio del eCasilla-CGR. Cabe mencionar además que las funciones del PSVA no han sido tercerizadas.
- Garantiza la implementación y el establecimiento de una Política de Seguridad cuyo alcance cubra todas las operaciones críticas del SVA.
- Garantiza la publicación y comunicación de esta DPSVA y su Política de Seguridad a todos los empleados que participan de las operaciones del eCasilla-CGR

15.2. Gestión y clasificación de activos

Todos los elementos relativos a la gestión y clasificación de activos se encuentran en documentación interna manejada por la Contraloría.

Para cada subproceso vital o crítico que se desarrolla en el ámbito del proceso de generación de notificaciones electrónicas, se deberá efectuar el análisis y evaluación de riesgos, teniéndose en consideración tanto las amenazas internas como externas; asimismo, se identificarán, evaluarán e implementarán las opciones de tratamiento del riesgo que permitan mitigar el impacto de los activos de información.

15.3. Seguridad en el trato con terceros

Las funciones del PSVAEP no han sido tercerizadas. Sin embargo, de requerir tercerizar algunas funciones del eCasilla-CGR a otra organización o entidad, la seguridad debe ser mantenida. En ese caso, sigue siendo la Contraloría la responsable de los servicios que brinda, incluyendo aquellos que pudieran ser realizados por terceros proveedores.

Las responsabilidades de terceros, cuando sus servicios sean requeridos, deberán ser definidos en los contratos. Así también serán establecidos los controles que deberán ser implementados para asegurar el cumplimiento de esta política de seguridad por parte de los terceros proveedores.

Cuando aplique, es responsabilidad de la Contraloría declarar las prácticas relevantes de tercerización a todas las partes interesadas.

15.4. Seguridad del personal

Los trabajadores, contratistas y consultores designados para gestionar la infraestructura del eCasilla-CGR son considerados como “personal de confianza”. Se designan, de manera oficial, los roles incluyendo sus funciones, responsabilidades y riesgos, mediante un contrato de trabajo u orden de servicio, según corresponda.

La Contraloría asegura que el personal y las prácticas contractuales soporten la confiabilidad de las operaciones del eCasilla-CGR. En tal sentido:

- Se debe emplear personal que posea conocimiento especializado, experiencia y calificaciones necesarias para ofrecer los servicios, de acuerdo con las funciones que debe cumplir cada rol.
- Los roles y responsabilidades referidas al cumplimiento de la Política de Seguridad, son documentados en las descripciones de las funciones de cada rol, identificándose los roles de confianza de los cuales dependen las operaciones del eCasilla-CGR.
- Las funciones del personal del PSVA (temporal y permanente) son definidas considerando los criterios de separación de derechos y mínimo privilegio.
- El personal ejecuta sus funciones y procedimientos en función de los procedimientos establecidos y la Política de Seguridad.
- El PSVA asegura que su personal gerencial tome conocimiento de las tecnologías relacionadas a los servicios del eCasilla-CGR, como firma digital, gestión de certificados digitales, sello de tiempo, gestión de casillas electrónicas, notificaciones electrónicas, conocimientos de los procedimientos y responsabilidades de seguridad para la gestión de personal, experiencia en seguridad de la información y evaluación de riesgos.
- El PSVA verifica que todo el personal en roles de confianza se encuentra libre de conflicto de interés que pueda perjudicar la imparcialidad de las operaciones del eCasilla-CGR.
- Los roles de confianza incluyen las siguientes responsabilidades:
  - Oficial de seguridad: Responsable de administrar la implementación de las prácticas de seguridad
  - Administrador de sistemas: Autorizados a instalar, configurar y mantener la integridad de los sistemas del PSVA
  - Operador de sistemas: Responsable de operar la integridad de los sistemas en el día a día. Autorizados para ejecutar sistemas de respaldo y recuperación.
  - Auditor de sistemas: Autorizados a ver archivos y logs de los sistemas del SVA
- El personal es formalmente asignado a cumplir los roles de confianza, por parte del responsable de la seguridad.
- La Contraloría no asignará en roles de confianza o administración a cualquier persona que es conocida por tener una participación en un crimen serio u otra ofensa la cual afecta su idoneidad para su puesto. El personal no obtiene acceso a funciones de confianza hasta completar todas las verificaciones necesarias.

15.5. Seguridad física y del entorno

Se implementan controles que impiden el retiro no autorizado de equipos, información, medios de almacenamiento, software relativo a los servicios críticos del eCasilla-CGR. En tal sentido:

- Los medios de administración de los sistemas del eCasilla-CGR son operados en el centro de datos de la Contraloría, el cual es un ambiente protegido con controles físicos de acceso para proteger de acceso no autorizado a los sistemas y datos:
- Se definen perímetros de seguridad que protegen las operaciones y sistemas críticos del SVA.
- Controles de seguridad física y ambiental son implementados para proteger los medios que alojan los recursos informáticos, los recursos informáticos, y los medios usados para soportar su operación. Estos incluyen: protección de acceso físico,

protección contra desastres naturales, detección y protección contra incendios, contingencia en cortes de energías y comunicaciones, colapso de la estructura, aniego, protección contra robo, ruptura, recuperación en caso de desastres, conforme a los resultados del análisis de riesgos.

- Se tienen controles para impedir el retiro no autorizado de equipos de información, medios de almacenamiento, software relativo a los servicios críticos del eCasilla-CGR.

15.6. Gestión de operaciones

La Contraloría brinda la seguridad necesaria para que los componentes de sus sistemas se encuentren seguros y sean correctamente operados, todo ello bajo un mínimo riesgo de falla.

- La integridad de los componentes informáticos y la información son protegidos contra virus, software malicioso o no autorizado.
- Se implementan y ejecutan procedimientos de reporte y respuestas a incidentes de seguridad y mal funcionamiento de las operaciones del eCasilla-CGR.
- Los medios de almacenamiento usados en los sistemas críticos del eCasilla-CGR están protegidos contra modificación o acceso no autorizados.
- Se establecen procedimientos para todos los roles de confianza y administrativos que impactan en la provisión de servicios del eCasilla-CGR.
- Se implementan procedimientos para asegurar la adecuada planificación de activos y nuevos sistemas a fin de evitar incompatibilidades con otros sistemas y vulnerabilidades de seguridad.
- La limpieza de los ambientes es la adecuada para no dañar los equipos, y el personal es supervisado para evitar robos de medios de almacenamiento e información.

15.7. Manejo de medios y seguridad

Todos los medios son manejados de manera segura conforme a la clasificación de activos. Los medios de almacenamiento que contienen datos sensibles deben ser eliminados de manera segura cuando ya no sean requeridos.

15.8. Planificación del sistema

Las demandas de capacidad de los sistemas deben ser monitoreadas y deben realizarse proyecciones de la demanda futura a fin de asegurar la disponibilidad de los sistemas de procesamiento y almacenamiento.

15.9. Reporte y respuesta a incidentes

La Contraloría planea actuar de manera oportuna y coordinada para responder de manera rápida a los incidentes y limitar el impacto de los vacíos de seguridad. Todos los incidentes son reportados tan pronto como sea posible.

15.10. Seguridad en redes

- Se define una política de acceso en redes.
- Las redes están protegidas de acceso no autorizado.
- Se separa la zona de constante acceso con la red interna de procesamiento y almacenamiento de información crítica. De acuerdo con los diferentes niveles de

seguridad, se separan las redes de datos de los sistemas de procesamiento central del eCasilla-CGR.

- El acceso a dominios de redes internas del eCasilla-CGR está protegido de acceso no autorizado incluyendo a suscriptores y terceros que confían. Los firewalls están configurados para prevenir todos los protocolos y accesos no requeridos para la operación del eCasilla-CGR.
- Se implementan sistemas de detección de intrusos para prevenir accesos de código malicioso o no autorizado.

15.11. Monitoreo

Medios de monitoreo y alarmas son implementados para detectar, registrar y actuar oportunamente sobre accesos no autorizados o intentos irregulares de acceso a recursos. En tal sentido, se planifica el monitoreo de:

- La continuidad y seguridad de las operaciones.
- Los registros de auditoría y los reportes de eventos sobre errores y advertencias en el funcionamiento de los sistemas del eCasilla-CGR.

15.12. Intercambio de datos y software

Las vulnerabilidades y riesgos de seguridad relacionados al intercambio de datos y software son evaluados y manejados de manera apropiada de acuerdo con su impacto sobre las operaciones del eCasilla-CGR.

15.13. Gestión de acceso a los sistemas

Como el sistema se encuentre integrado a un sistema de gestión de usuarios, se cumple lo siguiente:

- Permite la asignación de cuentas de usuario para controlar los accesos a los sistemas, permite la modificación o remoción oportuna de accesos.
- Diferencia las cuentas de administración de las cuentas de usuario.
- El sistema permite controlar al personal respecto de las acciones críticas que realiza en los sistemas del eCasilla-CGR, generando registros de auditoria.

15.14. Archivo

La información crítica y sensible, que es archivada está protegida contra daño ambiental o intencional, así como acceso de lectura y modificación no autorizados.

15.15. Desarrollo y mantenimiento de sistemas confiables

Se realiza un análisis de los requerimientos de seguridad que deben ser cubiertos en las etapas de diseño y especificación de los proyectos de desarrollo de sistemas del eCasilla-CGR, para asegurar que dichos requerimientos son considerados en los sistemas críticos.

15.16. Control de cambios

Se debe implementar procedimientos de control de cambios para poner en producción modificaciones o parches de emergencia de aplicaciones críticas de software del eCasilla-CGR, a fin de evitar posteriores fallas o incompatibilidad con otros sistemas.

16. TÉRMINO DE LA ORGANIZACIÓN QUE ADMINISTRA EL SVA

16.1. Término del PSVA

El PSVA adopta las medidas necesarias para que su finalización no afecte de manera significativa a los suscriptores y terceros que confían.

16.1.1. Preparación antes del término

- El PSVA pone a disponibilidad de los suscriptores y terceros que confían la información concerniente a su terminación
- El PSVA da término a las autorizaciones de todos los subcontratistas que actúan en nombre del PSVA,
- Asegura el cumplimiento o compensación por los servicios comprometidos de soporte o garantía

17. REGISTROS DE AUDITORÍA

El sistema debe permitir registrar los eventos críticos.

17.1. Eventos registrados

Los eventos que son registrados están relacionados a las transacciones de autenticación y generación de firma digital.

17.2. Protección de los registros

Los eventos son registrados de tal forma que ellos no puedan ser borrados o destruidos dentro del periodo de tiempo que son requeridos como evidencia (excepto si son transferidos a medios de almacenamiento de largo plazo).

17.3. Eventos significativos

Son registrados las solicitudes o transacciones de autenticación, firma digital o cifrado (en caso se implemente). Se consideran como eventos significativos para el eCasilla-CGR:

- Fecha y hora de autenticación de los usuarios
- Fecha y hora de notificación, cuando se realiza la notificación con el depósito de los documentos en la casilla electrónica.
- Fecha y hora de lectura, cuando el usuario receptor visualiza por primera vez la notificación.
- Fecha y hora de cambio en la configuración de usuarios
- Fecha y hora de cambio en la configuración del sistema

18. AUDITORÍA

Cada PSVA acreditado debe ser auditado anualmente por la AAC, respecto a la correcta operación de los servicios de registro.

Como parte de dicha auditoría anual se revisan los registros, el archivo, los procedimientos y controles implementados.

El auditor debe cumplir con los siguientes requisitos:

- Estar autorizado por la AAC.
- Ser independiente de la Contraloría y no haber realizado trabajos para ella dentro de los dos años anteriores a la ejecución de la auditoría.

19. CERTIFICADOS DE AUTENTICACIÓN

En una primera etapa la Contraloría no empelará certificados de autenticación para los usuarios del eCasilla-CGR. Se empleará autenticación mediante usuario y contraseña.

20. ASPECTO LEGALES DE LA OPERACIÓN DEL PSVA

20.1. Políticas de reembolso

No aplican reembolsos por el Servicio del eCasilla-CGR.

20.2. Cobertura de Seguro de Responsabilidad Civil

La Contraloría debe mantener una póliza de responsabilidad civil por un monto no menor a USD 35 000.

20.3. Información confidencial y/o privada

La Contraloría debe mantener de manera confidencial la siguiente información:

- Material comercialmente reservado de los Prestadores de Servicios de Certificación, de los usuarios del eCasilla-CGR y de los terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual.
- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores de empresa y los terceros que confían.
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- Se debe asegurar la reserva de toda información que mantiene, la cual pudiera perjudicar la normal realización de sus operaciones.

20.4. Información no privada

No se considera como privada y por tanto será tratada como pública aquella información que se incluye en los certificados.

Entre la información que puede hacerse pública:

- Datos de identificación que figuran en el certificado digital del suscriptor, tales como: nombre completo, número del DNI y RUC.
- Usos y límites de uso de los certificados digitales.
- Información personal que los titulares o suscriptores soliciten o autoricen que se haga pública.
- Período de validez del certificado digital, así como la fecha de emisión y caducidad de este.
- Número de serie del certificado digital.
- Información que no contravenga lo expuesto en la ley de Protección de datos personales.

20.5. Derechos de propiedad intelectual

En caso de aplicar, la Contraloría debe declarar cláusulas contractuales respecto de obligaciones y derechos relacionados a la propiedad intelectual.

20.6. Notificaciones y comunicaciones entre participantes

Para todos los efectos de las comunicaciones entre el PSVA, los usuarios y terceros que confían, se tendrá como referencia el domicilio real o electrónico que hubieren señalado, en donde se tendrán por válidamente realizadas todas las comunicaciones que pudieran serles cursadas.

20.7. Procedimientos de resolución de disputas

En caso de presentarse cualquier disputa o reclamo en relación con los derechos u obligaciones que se alude en el presente documento, la persona deberá presentar dicho reclamo en la sede principal de la Contraloría, elaborando un resumen de los aspectos más relevantes de la reclamación y acompañando los documentos sustentatorios correspondientes. La Contraloría resolverá en primera instancia el aludido reclamo.
Agotada la vía anteriormente indicada y en caso el reclamante no se encontrara conforme, se podrá recurrir en vía administrativa ante la Autoridad Administrativa Competente, con sujeción a lo establecido para tales efectos por la Ley N° 27444 – Ley del Procedimiento Administrativo General.

20.8. Conformidad con la ley aplicable

La ley aplicable para todos los efectos de la presente Declaración de Prácticas de Prestador de Servicio de Valor Añadido es la normativa peruana en materia de firmas y certificados digitales, es decir, principalmente la Ley N° 27269, Ley de Firmas y Certificados Digitales, y su Reglamento (Decreto Supremo N° 052-2008-PCM), así como las disposiciones contenidas en la Guía de Acreditación de Prestador de Servicios de Valor Añadido (PSVA) y sus anexos. Así como lo establecido mediante Decreto Supremo N° 070-2011-PCM y el Decreto Supremo N° 105-2012-PCM.

Finalmente, serán también aplicables las normas y lineamientos que en materia de certificación digital pudiera dictar la Autoridad Administrativa Competente.

La Contraloría es responsable de velar por el cumplimiento de la legislación aplicable establecida en los párrafos precedentes, al momento de prestar sus servicios.

20.9. Extensión de garantías

La Contraloría no realizará pago de indemnización alguna, salvo lo correspondiente a las obligaciones derivadas de la ejecución del seguro por responsabilidad que corresponde contratar de conformidad con lo que disponga para dichos efectos la Autoridad Administrativa Competente.

20.10. Indemnizaciones

Las indemnizaciones a las cuales pudiera estar obligada la Contraloría en su condición de Prestador de Servicio de Valor Añadido, se sujetará a lo detallado en la póliza de Seguro de Responsabilidad Civil que deberá adquirir de conformidad con lo detallado para dichos efectos por la Autoridad Administrativa Competente.

20.11. Fuerza Mayor

De aplicar, la Contraloría asegura que en la información a ser provista a los usuarios del eCasilla-CGR, se incluyan las cláusulas de fuerza mayor que correspondan.

21. BIBLIOGRAFÍA.

En la redacción del presente documento se utilizó:

- Ley N° 27269, de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo Nº 052-2008-PCM, y sus modificatorias, el Decreto Supremo N° 070-2011-PCM y Decreto Supremo N° 105-2012-PCM.
- Ley N° 29733, de Protección de Datos Personales.
- ANEXO 1: Marco de la Política de Registro para la Emisión de Certificados Digitales de la Guía de Acreditación de Entidades de Registro ER, versión 3.3, expedido por la AAC.
- RFC 3647 “Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Frameworktk” del Internet Engineering Task Force (IETF) (que sustituye a la RFC 2527).
- Norma Marco sobre Privacidad para los países integrantes del APEC, aprobada en la 16º Reunión Ministerial del APEC, Santiago de Chile, 17 y 18 de noviembre de 2004.
- Norma Técnica Peruana “NTP-ISO/IEC 17799:2013 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición (de uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática conforme lo dispone la Resolución Ministerial Nº 246-2007-PCM publicada el 25 de junio de 2007).