LA CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL PRESTADOR DE SERVICIOS DE VALOR AÑADIDO PARA EL ESTADO PERUANO

NOTIFICACIONES ELECTRÓNICAS EN EL MARCO DEL CONTROL GUBERNAMENTAL

	NOMBRE	CARGO	FIRMA	FECHA
Elaborado por:	Gladys Linares Núñez	Profesional de la Subgerencia de Sistemas de Información	Firmado digitalmente por LINARES NUÑEZ Gladys Luz FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 08.07.2020 16:09:25 -05:00	08/07/2020
	Paola Manrique Huertas	Profesional de la Subgerencia de Gobierno Digital	Firmado digitalmente por MANRIQUE HUERTAS Paola Gisselle FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 09.07.2020 14:54:44 -05:00	08/07/2020
	Harry Cernades Gómez	Profesional de la Subgerencia de Operaciones y Plataforma Tecnológica	Firmado digitalmente por CERNADES GOMEZ Harry Alejandro FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 09.07.2020 15:46:28 -05:00	08/07/2020
	César Córdova Véliz	Profesional de la Gerencia de Tecnologías de la Información	Firmado digitalmente por CORDOVA VELIZ Cesar Rolando FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 11:12:18 -05:00	08/07/2020
Revisado por:	Erik Bazán Flores	Subgerente de Sistemas de Información	Firmado digitalmente por BAZAN FLORES Erik Ulises FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 17:40:49 -05:00	08/07/2020
	Ricardo Balbuena Rodríguez	Subgerente de Operaciones y Plataforma Tecnológica	Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 16:56:46 -05:00	08/07/2020
	Raúl Huertas Salazar	Subgerente de Gobierno Digital	Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 16:17:02 -05:00	08/07/2020
Aprobado por:	Amparo Ortega Campana	Gerente de Tecnologías de la Información	Firmado digitalmente por ORTEGA CAMPANA Amparo FAU 20131378972 soft Motivo: Soy el autor del documento Fecha: 10.07.2020 15:21:48 -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 Política de Seguridad de la Información de la Contraloría General de la República para su Prestador de Servicios de Valor Añadido para el Estado Peruano (PSVAEP) tiene por objeto describir el marco general y los lineamientos aplicados por la Contraloría para la gestión y protección de los activos de información que administra el sistema eCasilla-CGR.

3. ALCANCE

La Contraloría provee la infraestructura tecnológica correspondiente al hardware y software necesario para la puesta en funcionamiento de su Sistema de Notificaciones y Casillas Electrónicas.

El contenido de la presente política, así como los procedimientos de gestión que se deriven de ella, serán de cumplimiento obligatorio para el personal involucrado en las operaciones críticas derivadas de la Prestación de Servicio de Valor Añadido del eCasilla-CGR. También será de cumplimiento obligatorio de los proveedores de servicios o terceros que proporcionen sus servicios al PSVAEP.

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 las actividades realizadas desde la creación y activación de la casilla electrónica por asignación obligatoria a (ex)funcionarios o (ex)servidores relacionados con procesos de control y procedimientos administrativos y por solicitud 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, órganos desconcentrados y los órganos de Control Institucional de la Contraloría General de la República, en lo que les corresponda.

4. SIGLAS Y DEFINICIONES

4.1. Siglas

CGR	**:**	Contraloría General de la República
OCI	**:**	Órgano de Control Institucional
TSRA	**:**	Tribunal Superior de Responsabilidad Administrativa

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. MARCO CONTEXTUAL

- Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, y sus modificatorias.
- Ley Nº 27658, Ley Marco de la Modernización de la Gestión del Estado, y sus modificatorias.
- Ley N° 27269, Ley de Firmas y Certificados Digitales, y sus modificatorias.
- Ley N° 29733, Ley de Protección de Datos Personales, y su modificatoria.
- Ley N° 30742, Ley de Fortalecimiento de la Contraloría General de la República y del Sistema Nacional de Control.
- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

- Decreto Legislativo Nº 295, Código Civil.
- Decreto Legislativo N° 681, mediante el cual se dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional como a la producida por procedimientos informáticos en computadoras, y sus modificatorias.
- Decreto Legislativo N° 1246, que aprueba diversas medidas de simplificación administrativa aplicables a todas las entidades de la Administración Pública.
- Decreto Legislativo N° 1310, que aprueba medidas adicionales de simplificación administrativa, y sus modificatorias.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 004-2019-JUS, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales, y sus modificatorias.
- Decreto Supremo N° 066-2011-PCM, mediante el cual se aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0.
- Decreto Supremo N° 004-2013-PCM, mediante el cual se aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 118-2018-PCM, mediante el cual declaran de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.
- Resolución Ministerial N° 125-2013-PCM, que aprueba el Plan de Implementación de la Política Nacional de Modernización de la Gestión Pública 2013-2016.
- Resolución de Secretaría de Gobierno Digital N° 001-2017-PCM/SEGDI, que aprueba el Modelo de Gestión Documental en el marco del Decreto Legislativo N° 1310, y su modificatoria.
- Reglamento de Organización y Funciones de la Contraloría General de la República, vigente.

6. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DEL PSVA

La Contraloría General de la República (CGR) administra y es responsable de la elaboración de todos los documentos normativos de su PSVAEP, incluyendo la presente política. Cada nueva versión de estos documentos será presentada a la Autoridad Administrativa Competente para su revisión y aprobación antes de entrar en vigor y ser puesta a disposición de los usuarios mediante su publicación.

Persona de Contacto
Oficial de Seguridad del PSVAEP: Harry Cernades Gómez
Teléfono: 330-3000 anexo: 1041
Correo electrónico: hcernandes@contraloria.gob.pe

7. EVALUACIÓN DE RIESGOS

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.

Los procedimientos y documentos relacionados aplicados a la Evaluación de Riesgos del PSVAEP están en concordancia con lo establecido en la Política Institucional de Gestión de Riesgos de la Contraloría General de la República y el (PR-GSEG-04)00 Procedimiento Gestión de Riesgos en Seguridad de la Información.

8. CONTROL DE ACCESOS

Se controlará el acceso a la información confidencial generada durante el proceso de generación y entrega de notificaciones electrónicas, en concordancia con lo establecido en el Plan de Privacidad, la clasificación de información y los resultados de la evaluación de riesgos.

La administración del acceso a los usuarios debe considerar que:

- Toda solicitud de acceso físico y lógico, así como la administración de las cuentas de usuario a los activos de información deberá ser realizada conforme a los procedimientos establecidos.
- Sólo se asignarán cuentas de acceso individuales.

El personal que reciba una cuenta de usuario para el acceso a los activos de información deberá hacer uso adecuado de sus contraseñas de acceso, manteniendo la confidencialidad de ésta, no dejando sus estaciones de trabajo desatendidas, solicitando su cambio de contraseña si tiene algún indicio de su vulnerabilidad y seleccionando una contraseña que tenga un nivel adecuado de complejidad.

Es responsabilidad de los propietarios de los activos de información el clasificar la información (física o digital) de acuerdo con lo indicado en los lineamientos definidos para la clasificación de la información. Asimismo, identificar y agrupar a los usuarios, considerando su necesidad de información para el desarrollo de sus funciones o labores que realicen, con la finalidad de establecer los niveles de acceso a la base de datos, sistemas y/o aplicativos, centro de datos, infraestructura de procesamiento de información, archivos físicos y electrónicos, de acuerdo con el resultado de la evaluación de riesgos y los requerimientos de la organización.

Con respecto a los accesos de entidades, organizaciones o instituciones externas que requieran acceder a los servicios (de corresponder), se deberá controlar los accesos lógicos proporcionados de dichas entidades estableciendo interfaces seguras entre la red de datos de la Contraloría y la red de datos de la entidad externa, a nivel de puertos para los que se requieren los servicios. Previo al acceso a los servicios del eCasilla-CGR, dichas entidades externas deben firmar un acuerdo de confidencialidad y un compromiso a salvaguardar la integridad, disponibilidad y confidencialidad de la información que utilice o sea de su conocimiento.

Corresponde a los órganos que conforman el proceso de emisión y entrega de las notificaciones electrónicas establecer un proceso periódico de revisiones de los derechos de acceso tanto de su personal como de los usuarios de entidades externas, así mismo, programar revisiones periódicas de las políticas configuradas en su red de datos.

Es responsabilidad del encargado o supervisor de cada órgano o unidad orgánica solicitar, en el menor tiempo posible, la inactivación de las cuentas de usuario cuando éstos ya no presten sus servicios, o cuando el usuario o entidad externa ya no requiera el acceso a la información del eCasilla-CGR.

Los procedimientos y documentos relacionados aplicados al Control de Accesos del PSVAEP están en concordancia con lo establecido en la Directiva N°007-2016-CG/PROCAL Asignación, Acceso, Uso y Revocación de los recursos Informáticos de la Contraloría General de la República.

9. SEGURIDAD DEL PERSONAL

Se debe asegurar que el personal, contratista y terceros reciban y comprendan sus responsabilidades respecto al uso y tratamiento de los activos de información, con la finalidad de reducir el riesgo de hurto, fraude o mal uso de la información. Así mismo, se deberá asegurar la implementación de controles de seguridad relacionados al personal, antes, durante y finalizado el empleo o servicio brindado dentro del proceso de emisión y entrega de notificaciones electrónicas.

Antes del empleo:

- Los perfiles de usuario deberán ser definidos en base a las funciones que se van a desarrollar y las responsabilidades que les competan.
- Se deben implementar controles para la selección y contratación del personal, a fin de verificar la veracidad de los datos proporcionados por los postulantes, así como sus antecedentes penales y policiales. Para el caso de quienes vayan a desarrollar roles de confianza, se podría incluir la verificación de sus antecedentes crediticios.
- Para los servicios efectuados por terceros, la verificación de los datos del personal la efectuará el proveedor del servicio. La Contraloría se reserva el derecho de verificar dicha documentación.
- Cada una de las personas que presta servicios en el proceso de emisión de notificaciones electrónicas debe firmar un acuerdo de confidencialidad o un documento de compromiso de aceptación o cumplimiento, según corresponda, para salvaguardar la integridad, disponibilidad y confidencialidad de la información que utilice o sea de su conocimiento.

Durante el empleo:

- Toda persona que preste servicios en el proceso de emisión y entrega de notificaciones electrónicas debe recibir charlas de inducción en materia de Seguridad de la Información.
- Se deben desarrollar actividades de capacitación continua, dirigidas a mantener actualizados los conocimientos del personal respecto al uso y reserva de la información, así como a las políticas y procedimientos relevantes para sus funciones.
- Para los casos de tercerización de servicios se informará al prestador del servicio cuáles son los criterios que deberá considerar para la seguridad de la información, así como también, se monitoreará y revisará su cumplimiento.
- Todo incumplimiento de la Política de Seguridad de parte del personal o proveedores deberá ser informado al Oficial de Seguridad del PSVA para su análisis, evaluación y comunicación al órgano correspondiente, a fin de que éste proceda a la sanción que corresponda en concordancia con la normativa correspondiente, o en el caso de proveedores, para su comunicación a la Subgerencia de Abastecimiento, Gerencia de Administración y a la Oficina de Seguridad y Defensa Nacional para la sanción que corresponda de acuerdo a la Ley de Contrataciones del Estado o a lo establecido en el contrato.

Finalización del empleo:

- Todo cambio o finalización de funciones deberá realizarse de acuerdo con los procedimientos de la Contraloría, incluyendo le devolución de los bienes asignados. De

igual modo, se deberá solicitar al retiro de los accesos de su personal a la información o servicios.

10. SEGURIDAD FÍSICA

Se deben implementar controles de seguridad física con la finalidad de prevenir accesos no autorizados a los ambientes en que se procesa o resguarda información confidencial, y de esta manera, evitar el daño o pérdida de los archivos de información críticos.

Se deben delimitar los perímetros del ambiente en que se procesa o resguarda la información sensible, así como, establecer controles físicos de entrada y salida. Se deben instalar controles de seguridad contra incendios, aniegos y otros, que permitan alertar en casos de emergencia.

Los ambientes serán diseñados e implementados adecuadamente para la seguridad del personal y de los recursos que albergan. Se deberá, así mismo, establecer controles de acceso a los ambientes, al uso de las llaves de estos, y asignar a los responsables respectivos. También se debe definir e implementar un plan de evacuación en caso de desastre.

Estas políticas de seguridad física se deben considerar también para los ambientes de contingencia.

11. SEGURIDAD DE COMUNICACIONES Y REDES

Se deben establecer responsabilidades y procedimientos documentados de operación asociado al procesamiento de información y recursos de comunicaciones, con el objetivo de evitar daños, accesos no autorizados, mal uso de los activos de información, garantizar la seguridad de los datos y la disponibilidad de los servicios utilizados a través de la red de la la Contraloría y del internet.

En lo posible se segregarán las tareas y se implementará un procedimiento de gestión de cambios, con la finalidad de prevenir modificaciones no autorizadas en los equipos de comunicaciones y redes.

La Contraloría asegurará que los datos disponibles en los repositorios públicos se encuentren protegidos, así mismo, deberá garantizar la disponibilidad de éstos.

12. MANTENIMIENTO DE EQUIPOS Y SU DESECHO

Se debe asegurar la disponibilidad e integridad de los equipos a través de un adecuado plan de mantenimiento preventivo especialmente para los equipos críticos, el cual se realizará según el procedimiento establecido por la Contraloría, documentándose los incidentes que ocurren antes, durante y después del mantenimiento.

Antes del desecho o reúso de los equipos se revisará que toda información sensible haya sido removida o sobre escrita, con la finalidad de prevenir el acceso no autorizado a información sensible.

El reemplazo, decomiso, manipulación y desecho, tanto del hardware como del software, se realizará de acuerdo con los criterios establecidos por la Contraloría para el correcto uso de los equipos.

13. CONTROL DE CAMBIOS Y CONFIGURACIÓN

Se debe asegurar un control satisfactorio de todos los cambios realizados a los equipos, software y procedimientos. En lo posible se deberá garantizar la posibilidad de revertir los cambios efectuados sin éxito.

Se deberá realizar y aprobar los cambios en los sistemas y recursos de tratamiento de información; así mismo, previo al cambio se efectuará un análisis de impacto a los sistemas y proceso, comunicando el cambio a todos los involucrados. Se ha dispuesto que todo cambio o modificación que se realice al sistema sea debidamente documentado, y además que dichas modificaciones se efectúen, de preferencia, fuera del horario de atención a los clientes o en horas de menor demanda.

14. PLANIFICACIÓN DE CONTINGENCIA

Los órganos que tienen la responsabilidad de desarrollar y proporcionar los servicios de emisión y entrega de notificaciones electrónicas que se brindan a los usuarios, implementarán un Plan de Contingencia a nivel de servicios, que les permita reaccionar ante una posible interrupción en las actividades críticas del proceso y en el tiempo requerido por la Contraloría.

Para establecer el Plan de Contingencias se identificarán procesos críticos para el servicio prestado, los eventos que puedan ocasionar interrupciones en estos procesos, y los planes o acciones que se deberán efectuar para mantener y recuperar las operaciones, así como el período en que estos deberán recuperarse.

Se deberá establecer pruebas periódicas del Plan de Contingencias, que permitan evaluar su eficacia y efectuar su actualización, de ser el caso.

15. RESPUESTA A INCIDENTES

Se deberá clasificar, comunicar y atender los incidentes de manera rápida, eficaz y sistemática, a fin de garantizar el restablecimiento del servicio afectado en el menor tiempo posible.

Para el caso de los incidentes que afecten la seguridad de la información, se deberá establecer que toda persona (personal o proveedor) que presta servicios en el proceso de emisión y entrega de notificaciones electrónicas deberá comunicar oportunamente al Oficial de Seguridad del PSVA o persona designada, cuando se haya detectado o tomado conocimiento del incidente, para que puedan ser atendidos conforme al procedimiento establecido. Adicionalmente, los encargados de supervisar la seguridad de la información y privacidad de datos deberán llevar un registro de los incidentes de seguridad ocurridos en su ámbito de alcance, monitoreando la implementación de las acciones correctivas o preventivas que ameriten.

16. AUDITORÍAS Y DETECCIÓN DE INTRUSIONES

Se programarán como mínimo una auditoría al año. Al término de la auditoría el área o persona auditada deberán implementar en el menor tiempo posible las acciones correctivas y preventivas identificadas.

Se deberán ejecutar pruebas periódicas de detección de intrusiones, así como, implementar controles que permitan alertar los intentos de acceso no autorizados.

Los sistemas y procesos (manuales o automáticos) deberán contar con registros de auditoría actualizados, los mismos que deben brindar información de la acción ejecutada, la hora, fecha, identificación del personal, software y hardware utilizado, según corresponda.

17. MEDIOS DE ALMACENAMIENTO

Se debe asegurar la protección de los documentos, medios informáticos, datos de entrada y salida y documentación del proceso de emisión y entrega de notificaciones electrónicas de las ocurrencias como daño, modificación, robo o acceso no autorizado.

Se debe establecer un procedimiento para la administración de los medios de almacenamiento de información, y los controles de seguridad requeridos para el almacenamiento, uso y protección de la información, considerándose también el uso de los medios de almacenamiento removibles, el proceso de eliminación segura de información, la planificación y ejecución de copias de seguridad, así como su proceso de restauración.

18. ADMINISTRACIÓN DE CLAVES

Se deben asegurar la confidencialidad de las claves criptográficas y se implementarán los controles requeridos de acuerdo con el nivel de seguridad acreditado.

19. CONFORMIDAD

Este documento ha sido aprobado por la Gerencia de Tecnologías de la Información, facultada por la Contraloría para cumplir con las funciones de Prestador de Servicios de Valor Añadido (PSVA), y tiene carácter normativo sobre todos los servicios correspondientes al sistema de Notificaciones y Casillas Electrónicas, por lo que cualquier incumplimiento por parte de las personas mencionadas en el alcance de este documento, será comunicado a dicha gerencia.