CORREO URUGUAYO

Administración Nacional de Correos del Uruguay

Unidad de Servicios Electrónicos

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión: 1.0

Marzo de 2013

Tabla de Contenido

Referencia Normativa

La presente Política utiliza como base para su contenido información publicada como parte de las siguientes normas/estándares:

- Familia ISO-IEC 27000 en general y en particular se consideran todos los aspectos recomendados por ISO-IEC 27002-2005.
- "Trust Service Principles and Criteria for Certification Authorities – Version 2.0" del Canadian Institute of Chartered Accountants.
- "Enterprise Risk Management – Integrated Framework" del Committee of Sponsoring Organizations of the Treadway Commission (COSO ERM)

Mantenimiento y Aprobación de esta Política

El mantenimiento de la presente Política será realizado por la Gerencia de la Unidad de Servicios Electrónicos de la Administración Nacional de Correos y la aprobación de la misma será realizada por la Presidencia de la Administración Nacional de Correos.

Se establece la obligatoriedad de una revisión anual de la presente Política como mínimo y el análisis de la necesidad de introducir cambios de ser pertinentes en el caso de:

- Cambios en la estructura organizativa de la Unidad de Servicios Electrónicos o cambio significativos en la estructura organizativa de la Administración Nacional de Correos.
- Cambios significativos en la normativa que regula los Servicios de Certificación.
- Cambios significativos en la plataforma de hardware y software a través de la cual se proveen los Servicios de Certificación.
- Incidentes de seguridad significativos.

Objetivo

La Administración Nacional de Correos entiende que la Seguridad de la Información (definida como el conjunto de los recursos, componentes y prácticas que garantizan la confidencialidad, integridad y disponibilidad de la información crítica y los mecanismos de procesamiento de la misma) es un requisito fundamental e ineludible para cualquier Entidad de Certificación.

En virtud de lo anterior, el principal objetivo de la presente Política es establecer las guías principales referentes a Seguridad de la Información que la Administración Nacional de Correos entiende que son necesarias para las operaciones de la Unidad de Servicios Electrónicos y en particular para los Servicios de Certificación.

Dichas guías permitirán cumplir con todos los requisitos legales y regulatorios (incluidos especialmente los definidos por la Unidad de Certificación Electrónica) y a

la vez proveer la base para garantizar la confianza de los clientes de los Servicios de Certificación.

Alcance

La presente Política alcanza únicamente a los aspectos de Seguridad de la Información de la Unidad de Servicios Electrónicos, no siendo aplicable a ninguna otra área o unidad de la Administración Nacional de Correos. En aquellos casos donde personal de otras áreas o unidades participe de la provisión de los Servicios de Certificación, será responsabilidad de la Gerencia de la Unidad de Servicios Electrónicos garantizar su cumplimiento de los aspectos de la presente Política que sean relevantes a dicha participación.

Los procedimientos que implementan la presente Política (definidos tanto en la "Declaración de Prácticas de Certificación" como en otros documentos de la Unidad de Servicios Electrónicos) no se consideran como parte de esta Política y por lo tanto la Gerencia de la Unidad de Servicios Electrónicos podrá definir los mecanismos de mantenimiento y aprobación de los mismos que entienda adecuados.

A efectos de facilitar el entendimiento del resto de los capítulos de la presente Política, se definen tres ambientes operativos (AO) que podrán tener requerimientos diferentes según sea necesario:

- AO1 – El ambiente de mayor criticidad donde reside el hardware (servidores, HSMs, etc.) y software que permiten la emisión de certificados y procesos relacionados. Incluye tanto las instalaciones primarias como las de contingencia.

- AO2 – El ambiente operativo directamente asociado al personal de la Unidad de Servicios Electrónicos (oficinas de la Unidad, servidores de desarrollo y equipamiento del personal, etc.)

- AO3 – El resto de las instalaciones de la Administración Nacional de Correos (oficinas de atención al público, etc.) desde donde es posible acceder a alguna funcionalidad vinculada a los Servicios de Certificación o donde se presentan los clientes a realizar los trámites requeridos.

En los casos donde no se haga una referencia específica a los ambientes operativos, los requerimientos establecidos se consideran válidos por igual para todos.

Gestión de Riesgos de Seguridad de la Información

Se establece que todos los controles de Seguridad de la Información que se implementen (sea a través de componentes tecnológicos, procedimientos operativos o cualquier otro medio) estarán basados en un Análisis de Riesgo previo para garantizar tanto su adecuación a las necesidades específicas como una buena utilización de los recursos disponibles.

A tales fines se utilizará la metodología recomendada por COSO ERM para determinar los objetivos (de seguridad) a satisfacer, analizar los riesgos que puedan comprometer los mismos, evaluar dichos riesgos e implementar las acciones correspondientes, según los criterios que defina la Gerencia de la Unidad de Servicios Electrónicos.

Deberá realizarse al menos un Análisis de Riesgos anualmente.

Estructura Organizativa y Responsabilidades

La responsabilidad general por la gestión de la Seguridad de la Información recaerá en la Gerencia de la Unidad de Servicios Electrónicos, quien velará por el cumplimiento de todos los requerimientos establecidos en la presente Política.

Las responsabilidades por las tareas operativas vinculadas la gestión de la Seguridad de la Información necesarias serán definidas en los procedimientos correspondientes por parte de la Gerencia de la Unidad de Servicios Electrónicos.

Se deberán llevar adelante revisiones independientes de las prácticas de gestión de Seguridad de la Información implementadas, las cuales podrán ser ejecutadas por personal de Auditoría Interna o por auditores externos según lo entienda necesario la Gerencia de la Unidad de Servicios Electrónicos.

Gestión de Activos

Se deberá mantener un inventario actualizado de todos los activos vinculados con la provisión de los Servicios de Certificación, particularmente aquellos asociados con AO1 y AO2. Dicho inventario incluirá cómo mínimo una descripción de cada activo y su dueño, quien será responsable por validar tanto los riesgos como los controles vinculados a dicho activo y los criterios de Uso Aceptable del mismo.

Adicionalmente, los activos de información que formen parte de dicho inventario (independientemente del formato en el que los mismos se mantengan) se deberán clasificar según la siguiente escala y contar con controles congruentes con su nivel de clasificación:

- C0 – Información pública o cuya divulgación no tendría ningún impacto para la Unidad de Servicios Electrónicos.
- C1 – Información generada para uso interno pero cuya divulgación no tendría un impacto significativo para la Unidad de Servicios Electrónicos.
- C2 – Información exclusivamente para uso interno cuya divulgación podría causar impactos negativos en términos económicos, regulatorios de imagen u otro tipo para la Unidad de Servicios Electrónicos.
- C3 – Información secreta cuya divulgación podría ocasionar impactos muy significativos para la Unidad de Servicios Electrónicos, potencialmente comprometiendo la continuidad en el mercado de los Servicios de Certificación.

Gestión de Recursos Humanos

Los roles y responsabilidades de todo el personal de la Unidad de Servicios Electrónicos deberán estar documentados formalmente, mantenerse actualizados e incluir los aspectos específicos de Seguridad de la Información que correspondan.

Todo el personal que trabaje y/o tenga acceso en AO1 y AO2 deberá firmar una carta de aceptación de los términos establecidos en la presente Política. Anualmente, la Gerencia de la Unidad de Servicios Electrónicos deberá coordinar una instancia de capacitación donde se repasen los contenidos de la presente Política, los procedimientos operativos vinculados a la Seguridad de la Información más relevantes y cualquier otro tema que se entienda de interés. Lo mismo será aplicable en el proceso de inducción de cualquier nuevo funcionario de la Unidad.

En lo referente a la revisión del historial e integridad del personal responsable de ejecutar los procesos operativos críticos asociados a los Servicios de Certificación se reitera la importancia del cumplimiento de lo establecido en el TOFUP.

En el caso de incumplimientos graves asociados al cumplimiento de las obligaciones referentes a la Seguridad de la Información, las sanciones a aplicar seguirán los procesos usuales de la Administración Pública.

Seguridad Física y Ambiental

Los ambientes AO1 y AO2 deberán contar con un perímetro de seguridad física que garantice que solamente el personal autorizado puede acceder a los mismos, manteniéndose además una bitácora que registre todos los accesos que se produzcan a AO1. En el caso de AO3 aplicarán los criterios usuales de control de acceso físico de la Administración Nacional de Correos, no requiriendo la presente Política de la implementación de mayores controles.

La Gerencia de la Unidad de Servicios Electrónicos determinará y documentará formalmente quiénes son los funcionarios con acceso autorizado a AO1 y AO2. Cualquier persona que no se encuentre en dicha lista y deba acceder a estos ambientes deberá estar acompañada en todo momento el funcionario que le haya provisto el acceso.

Para AO1 se deberán implementar además controles para prevenir el daño del equipamiento por factores ambientales (incendio, inundación, etc.) en el marco de una Solución de Continuidad Operativa como se define más adelante en la presente Política.

Ninguno de los equipos/componentes en AO1 podrá ser removido de su lugar físico sin una autorización formal y por escrito de la Gerencia de la Unidad de Servicios Electrónicos. Para AO2, la Gerencia de la Unidad de Servicios Electrónicos podrá designar y documentar formalmente aquellos equipos/componentes que entienda que por necesidades operativas están autorizados a ser transportados dentro y fuera de dicho ambiente en forma regular. Para los equipos/componentes en AO2 que no estén presentes en dicha lista, valdrá lo mismo que se estableció arriba para AO1.

En el caso de que sea necesario decomisionar algún equipo/componentes que resida en AO1 o AO2, dicho proceso deberá incluir mecanismos que garanticen que toda la información en los mismos ha sido destruida en forma segura.

Gestión de las Operaciones

A efectos de garantizar la consistencia de las tareas y la seguridad de las mismas, todos los procedimientos operativos y de gestión asociados a los Servicios de Certificación deberán estar documentados formalmente y aprobados por la Gerencia

de la Unidad de Servicios Electrónicos. Dichos procedimientos se deberán mantener actualizados, realizándose los procesos de análisis y corrección de los mismos con la periodicidad que los propios procedimientos especifiquen. A continuación en este capítulo (y en capítulos siguientes), se establecen requerimientos mínimos para algunos de dichos procesos.

Cualquier cambio que se realice sobre la infraestructura, configuración o aplicativos de AO1 deberá ser documentado formalmente antes de su ejecución y aprobado por la Gerencia de la Unidad de Servicios Electrónicos. Para AO2, aquellos cambios que potencialmente puedan tener un impacto sobre los Servicios de Certificación deberán recibir el mismo tratamiento.

Las funciones de desarrollo y operación de los sistemas en AO1 y en aquellos de AO2 directamente vinculados a los Servicios de Certificación deberán estar segregadas y en particular deberá garantizarse que quienes introducen un cambio en un aplicativo/servicio no cuentan con el acceso para poner dicho cambio en producción sin pasar por el procedimiento de control de cambios mencionado en el párrafo anterior. Adicionalmente, las tareas operativas de los Servicios de Certificación (particularmente la emisión de certificados digitales) deberán estar segregadas de las tareas de monitoreo/auditoría de los sistemas vinculados.

Se deberá contar con un procedimiento formal de planificación de la capacidad, a ejecutarse como mínimo anualmente, para garantizar que la infraestructura puede soportar razonable la carga que se espera para el corto y mediano plazo.

Todo el equipamiento de tecnología informática existente en AO1, AO2 y AO3 deberá contar con mecanismos actualizados periódicamente de protección contra código malicioso.

Todas las aplicaciones y datos en AO1 y AO2 que estén vinculados a los Servicios de Certificación deberán contar con procedimientos de respaldo adecuados y alineados con la Solución de Continuidad Operativa que se define más adelante en la presente Política.

Gestión de las Comunicaciones

Se deberán implementar controles en las facilidades de telecomunicaciones para restringir al máximo posible las comunicaciones externas con los ambientes vinculados a los Servicios de Certificación y para que las comunicaciones que se habiliten sean estrictamente requeridas para la provisión del servicio a los clientes.

En particular, no se permitirá ningún tipo de acceso desde Internet (u otras redes externas) a AO1.

Todas las comunicaciones externas a AO1 y AO2 deberán estar encriptadas utilizando algoritmos y largos de clave apropiados.

Cualquier cambio a la configuración de los elementos de seguridad que estén implementando la segregación entre los distintos ambientes deberá aplicar los procedimientos de gestión de cambios mencionados previamente.

Control de Acceso

La definición de los niveles de acceso a los sistemas involucrados en los Servicios de Certificación será realizada por la Gerencia de la Unidad de Servicios Electrónicos. Dicha definición deberá ser revisada periódicamente para garantizar que siempre se encuentre alineada con las funciones asignadas a los funcionarios correspondientes.

Para el acceso a cualquiera de los sistemas/componentes de AO1 se deberá contar al menos con mecanismos de autenticación de doble factor.

La Gerencia de la Unidad de Servicios Electrónicos podrá habilitar el acceso mediante una Red Privada Virtual (VPN) a los funcionarios de la Unidad de Servicios Electrónicos que requieran del mismo para llevar adelante sus tareas operativas.

Adquisición, Desarrollo y Mantenimiento de Sistemas Informáticos

Los requerimientos de seguridad de cualquier aplicación involucrada en la provisión de los Servicios de Certificación deberán estar documentados formalmente y aprobados por la Gerencia de la Unidad de Servicios Electrónicos. Estos requerimientos incluirán en particular aquellos relacionados con los mecanismos criptográficos que deban incluirse en dichos aplicativos y todos sus parámetros vinculados (protocolos, algoritmos de encriptación, largos de claves, etc.)

La puesta en producción de cualquier sistema en AO1 o AO2 deberá seguir los criterios definidos previamente en cuanto a la utilización del procedimiento de gestión de cambios.

El acceso al código fuente de cualquiera de las aplicaciones involucradas en la provisión de los Servicios de Certificación deberá estar limitado exclusivamente al personal que requiera de los mismos para tareas de desarrollo y mantenimiento de sistemas y que haya sido aprobado formalmente por la Gerencia de la Unidad de Servicios Electrónicos. No se permitirá en ningún caso la existencia de dicho código fuente en ningún equipo o medio que no forme parte de AO1 o AO2.

Cualquier modificación realizada sobre las aplicaciones involucradas en la provisión de los Servicios de Certificación o cualquier nuevo sistema/aplicación que se vaya a introducir con estos fines deberá ser sometida a un procedimiento formal de prueba/validación. La Gerencia de la Unidad de Servicios Electrónicos será responsable de definir el procedimiento específico y la documentación requerida dependiendo de la criticidad del sistema/aplicación a probar.

Gestión de Incidentes de Seguridad

La Gerencia de la Unidad de Servicios Electrónicos deberá establecer uno o más canales de comunicación adecuados para el reporte de cualquier tipo de incidente de seguridad y un procedimiento para su documentación y seguimiento.

Todo el personal de la Unidad de Servicios Electrónicos así como el resto del personal de la Administración Nacional de Correos que participe de alguna forma en los Servicios de Certificación deberá ser instruido en cómo detectar y reportar incidentes de seguridad a través de los canales que se hayan definido. Aquellos que

tengan alguna responsabilidad en la ejecución del procedimiento de respuesta ante dichos incidentes deberán ser además capacitados en estas funciones particulares.

La respuesta ante cualquier incidente deberá buscar en primera instancia la contención de dicho incidente para minimizar su impacto (incluyendo acciones de contingencia si corresponde) para luego pasar a un análisis detallado del incidente, su impacto y sus causas a efectos de preparar y ejecutar un plan de remediación. En cualquier caso, todo el ciclo de vida del incidente de seguridad deberá ser documentado formalmente como referencia futura y como justificación de las acciones que se hayan tomado en virtud del mismo. En particular, la documentación deberá reflejar todas las evidencias del incidente que se recaben por si resultara necesario o deseable implementar acciones legales.

Continuidad de las Operaciones

La Gerencia de la Unidad de Servicios Electrónicos será responsable por la implementación de una Solución de Continuidad Operativa que garantice la posibilidad de mantener las operaciones de los Servicios de Certificación aún en el caso de que una contingencia importante afecte significativamente a los recursos necesarios para llevar adelante dichos servicios.

Dicha Solución de Continuidad deberá incluir tanto Planes Preventivos (tendientes a reducir la probabilidad de caer en una contingencia o minimizar el impacto de algún escenario en particular) como Planes de Recuperación (los cuales indicarán las acciones a llevar a cabo para recuperar las operaciones en el caso de la indisponibilidad de alguno de los recursos críticos).

Será responsabilidad además de la Gerencia de la Unidad de Servicios Electrónicos el definir una Ventana de Tolerancia (tiempo máximo que los Servicios de Certificación pueden estar interrumpidos hasta que dicha interrupción cause un impacto inaceptable en el negocio) y garantizar que los planes estén alineados con dicha ventana.

La Solución de Continuidad Operativa (y en particular todos los planes que la componen) deberá ser evaluada y mantenida como mínimo anualmente (incluyendo la prueba de los planes) para garantizar que sigue manteniendo su validez.

Cumplimiento Legal y Regulatorio

La provisión de los Servicios de Certificación será realizada con el máximo nivel de cumplimiento de todos los requisitos legales y regulatorios que a la misma apliquen.

Será responsabilidad de la Gerencia de la Unidad de Servicios Electrónicos implementar los requerimientos que le hayan sido comunicados previamente por el Área de Asesoría Legal en relación a todos los aspectos contractuales y vinculados a cualquier otro tipo de normativa legal.

En lo referente a los aspectos regulatorios (requisitos de la UCE, normas internacionales aplicables a los Servicios de Certificación, etc.) será responsabilidad de la Gerencia de la Unidad de Servicios Electrónicos el realizar un seguimiento de los mismos y evaluar la implementación de los cambios correspondientes.

Monitoreo y Auditoría

Todos los sistemas involucrados directamente en los Servicios de Certificación deberán guardar pistas de auditoría de la actividad de los usuarios en los mismos así como cualquier incidente/problema detectado por los sistemas. Dichas bitácoras deberán tener controles de acceso adecuados para garantizar que las mismas sean confiables y no puedan ser alteradas en forma no autorizada.

La Gerencia de la Unidad de Servicios Electrónicos deberá definir un procedimiento de revisión de las pistas de auditoría con una periodicidad y alcance congruente con la criticidad de las mismas.

Control de Cambios

Versión	Fecha	Cambios realizados	Aprobación Versión 1.0
1.0	Marzo 2013	Primera versión que recoge los criterios generales que ya se venían usando en la División Servicios Electrónicos.	Lic. Javier Lago Unidad Servicios Electrónicos

Aprobación Gerencia General			
17	04	2013	
Visto Bueno Asesoría Jurídica			
17	04	2013	
Aprobación Presidencia			
18	04	2013	