Prácticas de Seguridad

CA OPTIC

v1.0

ÍNDICE

CONTROL DE DOCUMENTO

Título:	Prácticas de Seguridad		
Asunto:	CA OPTIC		
Autor:	Benito Galán		
Versión:	v1.0	**Fecha:**	20-06-2017
Código:	CPS-OPTIC	**Revisión anterior:**	
Idioma:	Español	**Núm. Páginas:**	17

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	**Versión**	**Motivo del Cambio**
20-06-17	1.0	Primera versión.

1. SEGURIDAD

1.1. Seguridad en las instalaciones de la PKI

La infraestructura de la CA estará desplegada en un datacenter ubicado en España, el cual cuenta con denominación Tier IV y con una disponibilidad 99,99%.

La seguridad del Data Center es uno de los requisitos principales desde su diseño inicial: a los métodos convencionales de detectores de presencia, proximidad e incluso circuito cerrado de televisión, se añaden controles de acceso y control. Únicamente el personal autorizado dispone de acceso a los equipos alojados en el Data Center.

En cuanto a los medios físicos de seguridad, el datacenter dispone de los sistemas más modernos de protección contra incendios, extinción por agentes de nulo impacto ambiental y sistemas de detección de fugas de agua o combustible. Todo ello telegestionado por un sistema central de control y gestión del edificio.

Cuenta con alimentación eléctrica redundante soportada con SAIs y grupos electrógenos. En el diseño de las instalaciones eléctricas existe redundancia de equipos, añadiéndole una serie de elementos alternativos tales como sistemas de by-pass, transferencias de cargas criticas sin cortes de tensión, aislamiento galvánico, red equipotencial de tierra, etc., que permiten asegurar el máximo nivel de disponibilidad eléctrica para los equipos alojados.

El sistema de climatización se realiza mediante equipos autónomos que aseguran unos niveles de temperatura y humedad óptimos para el funcionamiento de los servidores y la electrónica de red.

Cuenta con monitorización y vigilancia permanente 24 horas al día, 7 días a la semana y 365 días al año. El sistema de gestión del edificio centraliza todos los datos sobre la situación y el estado de la infraestructura del edifico y recibe y procesa posibles alarmas. Los sistemas principales conectados y gestionados son: el centro de seccionamiento, el centro de transformación, los grupos electrógenos, los sistemas de alimentación ininterrumpida, los cuadros eléctricos principales de media y baja tensión, la distribución eléctrica, los sistemas de climatización, la detección y extinción de incendios, la detección de humedad y la apertura de puertas.

La infraestructura está conectada de manera directa a Internet mediante circuitos de alta capacidad redundantes, asegurando así alta disponibilidad y calidad de acceso. La red troncal es una red multiservicio, basada en las más novedosas tecnologías, que incorpora los protocolos IP Multicast, BGP4 y MPLS. El acceso de la plataforma a Internet se realiza mediante múltiples conexiones con otras redes IP en puntos de intercambio y carriers de tránsito. Gracias al

protocolo BGP4 se asegura un encaminamiento eficiente del tráfico IP y reacciones dinámicas a cualquier cambio que se produzca en la red Internet.

1.2. Controles Procedimentales

1.2.1. Roles de confianza

Los roles de confianza son los que se describen en las respectivas Políticas de Certificación de forma que se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación. Concretamente:

a) Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

b) Las tareas de Certificación se realizarán por al menos tres personas necesitándose al menos de dos para activar la clave privada de la CA. Estas personas no deben formar parte de las tareas de Sistemas ni de Auditoría.

Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría o Certificación.

1.2.2. Número de personas requeridas por tarea

La CA garantiza al menos dos personas para realizar las tareas que se detallen en las Políticas de Certificación correspondientes.

1.2.3. Identificación y autenticación para cada rol

La CA establecerá los procedimientos de identificación y autenticación de las personas implicadas en roles de confianza.

1.2.4. Adecuada separación de funciones

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona sólo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados. El acceso a recursos se realiza dependiendo del activo mediante información de acceso y contraseña, Certificados Digitales, tarjetas de acceso físico y llaves.

1.3. Controles de Seguridad de Personal

1.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación.

Todo el personal que realiza tareas calificadas como confiables, lleva al menos dos (2) años trabajando en el centro de producción y tiene contratos laborales fijos. Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

La CA se asegurará que el personal de la Unidad de Registro o Administradores de la UR es personal confiable de la organización o de la entidad delegada para realizar las tareas de registro. El Administrador de la UR habrá realizado un curso de preparación para la realización de las tareas de validación de las solicitudes.

En general, la CA retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

1.3.2. Procedimiento de comprobación de antecedentes

La CA realizará los esfuerzos que razonablemente estén a su alcance para comprobar los antecedentes del personal que labora en áreas sensibles de la CA.

La CA realizará las investigaciones pertinentes antes de la contratación de cualquier persona.

La CA nunca asignará tareas confiables a personal con menos de una antigüedad de 6 meses.

1.3.3. Requerimientos de formación

El personal encargado de tareas de confianza ha sido formado en los términos que establecen las Políticas de Certificación.

1.3.4. Requerimientos y frecuencia de la actualización de la formación

La CA realizará los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y al menos con una frecuencia anual.

1.3.5. Frecuencia y secuencia de rotación de tareas

La frecuencia y rotación de las tareas será definida en el Manual Administrativo de Gestión del Personal de la CA.

1.3.6. Sanciones por acciones no autorizadas

La CA dispone de un régimen sancionador interno, descrito en su política de seguridad, para su aplicación cuando un empleado realice acciones no autorizadas pudiéndose llegar a su cese.

1.3.7. Requerimientos de contratación de personal

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y la requerimientos operacionales empleados por AVANSI.

Cualquier acción que comprometa la seguridad de los procesos aceptados podrían una vez evaluados dar lugar al cese del contrato laboral. Para los requisitos específicos ver el apartado 5.3.1 y las Políticas de Certificación correspondiente.

1.3.8. Controles sobre el personal contratado

Los controles aplicados al personal contratado serán descritos en el Manual Administrativo de Gestión del Talento de la entidad.

1.3.9. Documentación proporcionada al personal

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar una seguridad razonable y garantizar la confiabilidad y competencia del personal en el adecuado cumplimiento de sus funciones.

AVANSI pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las Políticas y la CPS que rigen dichos procesos.

Todo el personal de la CA y RA recibirán los manuales de usuario en los que se detallen al menos los procedimientos para el registro de Certificados, creación, actualización, renovación, revocación y la funcionalidad de la herramienta empleado.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

1.4. Seguridad en la RA

1.4.1. Controles Procedimentales

1.4.1.1. Roles de confianza

Los roles de confianza son los que se describen en las respectivas Políticas de Certificación de forma que se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación. Concretamente:

c) Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

d) Las tareas de Certificación se realizarán por al menos tres personas necesitándose al menos de dos para activar la clave privada de la CA. Estas personas no deben formar parte de las tareas de Sistemas ni de Auditoría.

Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría o Certificación.

1.4.1.2. Identificación y autenticación para cada rol

La UR establecerá los procedimientos de identificación y autenticación de las personas implicadas en roles de confianza, permitiendo el acceso mediante información de acceso y clave, y/o Certificados Digitales.

1.4.1.3. Adecuada separación de funciones

Las funciones disponibles en la UR están asociadas a uno o varios roles de seguridad, impidiendo de esta forma el acceso a funcionalidades no autorizadas a personas que no posean el rol adecuado.

1.4.2. Controles de Seguridad de Personal

1.4.2.1. Procedimiento de comprobación de antecedentes

La UR realizará los esfuerzos que razonablemente estén a su alcance para comprobar los antecedentes del personal que labora en la UR.

La UR realizará las investigaciones pertinentes antes de la contratación de cualquier persona.

La UR realizará los esfuerzos que razonablemente estén a su alcance proveer el entrenamiento necesario al personal que labora con la UR.

La UR nunca asignará tareas confiables a personal con menos de una antigüedad de 3 meses.

1.4.2.2. Requerimientos de formación

El personal encargado de tareas de confianza ha sido formado en los términos que establecen las Políticas de Certificación.

1.4.2.3. Requerimientos y frecuencia de la actualización de la formación

La UR realizará los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y al menos con una frecuencia anual.

1.4.2.4. Requerimientos de contratación de personal

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y los requerimientos operacionales para el uso de la UR.

Cualquier acción que comprometa la seguridad de los procesos aceptados podrían una vez evaluados dar lugar al cese del contrato laboral.

1.4.2.5. Documentación proporcionada al personal

La UR realizará los esfuerzos que razonablemente estén a su alcance para confirmar una seguridad razonable y garantizar la confiabilidad y competencia del personal en el adecuado cumplimiento de sus funciones.

La UR pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las Políticas y la CPS que rigen dichos procesos.

Todo el personal de la UR recibirán los manuales de usuario en los que se detallen al menos los procedimientos para el registro de Certificados, creación, actualización, renovación, revocación y la funcionalidad del software empleado.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

2. CESE DE LA ACTIVIDAD

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar que se minimizan los posibles perjuicios que se puedan crear a los Firmantes/Suscriptores o terceros que confían como consecuencia del cese de su actividad y en particular del mantenimiento de los registros necesarios a efectos probatorios en los procedimientos legales.

En particular:

a) Antes del cese de su actividad realizará, como mínimo, las siguientes actuaciones:

   1. Informará puntualmente a todos los Firmantes/Suscriptores, empleados, terceros que confían, UR's o CA's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 3 meses.

   2. La CA revocará toda autorización a entidades subcontratadas para actuar en nombre de la CA en el procedimiento de emisión de Certificados.

   3. La CA realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los historiales durante el periodo de tiempo indicado a los Firmantes/Suscriptores y terceros que confían.

   4. Las claves privadas de la CA serán destruidas y deshabilitadas para su uso.

b) Proveerá de los fondos necesarios para continuar la finalización de las actividades de revocación hasta el límite contratado a fin de satisfacer los requisitos mínimos en caso de quiebra o por cualquier otro motivo por el que no pueda hacer frente a estos costes por sí mismo.

c) Transferirá todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación.

3. CONTINGENCIA

3.1. Recuperación en Caso de Compromiso de la Clave o Desastre

La CA realizará los esfuerzos que razonablemente estén a su alcance para confirmar, en caso de desastre o compromiso de la clave privada de la CA, que ésta será restablecida tan pronto como sea posible.

Cualquier fallo en la consecución de las metas marcadas por la recuperación, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la CA para implementar dichos procesos.

3.1.1. La clave de la CA se compromete

La CA tratará el compromiso o el compromiso sospechado de la clave privada de la CA como un desastre.

En caso de compromiso, la CA tomará como mínimo las siguientes medidas:

a) Informar a todos los Firmantes/Suscriptores, terceros que confían y otras CAs con los cuales tenga acuerdos u otro tipo de relación del compromiso.

b) Indicar que los Certificados e información relativa al estado de la revocación firmados usando esta clave pueden no ser válidos.

3.1.2. Instalación de seguridad después de un desastre natural u otro tipo de desastre

La CA reestablecerá los servicios críticos dentro de las 48 horas posteriores a un desastre o emergencia imprevista.

La CA dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descrito en el plan de continuidad de negocio.

4. PROTECCIÓN DE DATOS PERSONALES

La CA cumplirá con todos los requisitos impuestos por la legislación aplicable en materia de protección de datos, en concreto, los referidos en la Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.

4.1. Política de Comunicación de Datos Personales

4.1.1. Datos Personales de Empleados de la CA y UR

Los datos de carácter personal de los empleados de la CA y de la UR únicamente serán cedidos cuando una disposición legal lo autorice o cuando sea estrictamente necesario para el cumplimiento y desarrollo de la relación laboral pactada con la empresa. En particular, está prevista la cesión de los datos de carácter personal en los supuestos que a continuación se exponen:

- A los organismos públicos a cuya comunicación resulte obligada la empresa como consecuencia del cumplimiento de obligaciones legales.

En todo caso, los datos comunicados serán exclusivamente los que resulten ser adecuados, pertinentes y no excesivos. Si desea cualquier información adicional o quiere ejercer los derechos de acceso, cancelación y oposición respecto a estas cesiones podrá utilizar los medios descritos anteriormente.

5. PROCEDIMIENTOS

5.1. Introducción

Todos los procedimientos en los que el personal de una UR está involucrado se describen detalladamente en los distintos manuales de operaciones y usuarios distribuidos debidamente.

En concreto, los procedimientos que al menos se describen serán: registro de Certificados, creación, actualización y renovación y revocación.

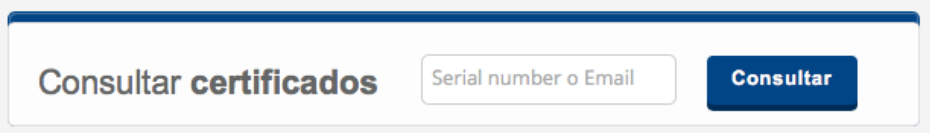
5.2. Registro de Certificados

Todos los Certificados gestionados por la RA son registrados y monitorizados desde el software puesto a disposición de los distintos roles autorizados, según se detalla en el capítulo 3 del manual para el rol registrador con referencia: MAN-REGISTER-OPTICCA-V1.0.PDF o versión superior.

Por otra parte, las claves públicas correspondientes a los Certificados gestionados por la UR estarán disponibles en un repositorio público, accesible desde la página principal de la UR.

https://ca.optic.gob.do/ra

La búsqueda de claves públicas se permitirá a partir del número de serie del Certificado o del email principal asociado a éste.



Para cada clave pública localizada, se mostrará información relativa a:

- Número de Serie
- Common Name
- Estado del Certificado
- Fecha de emisión
- Fecha de caducidad
- Fecha de renovación (si procede)
- Tipo de Certificado

5.3. Creación de Certificados

El proceso de creación de Certificados podrá ser iniciado por el propio suscriptor, desde la parte pública de la RA, o bien por el propio registrador, tal y como se explica en el capítulo 2.2 del manual registradores con referencia MAN-REGISTER-OPTICCA-V1.0.PDF o versión superior.

5.4. Actualización de Certificados

Todo proceso relacionado con la actualización de los datos asociados a un Certificado gestionado por la UR es explicado en el capítulo 3 del manual registradores con referencia MAN-REGISTER-OPTICCA-V1.0.PDF o versión superior.

5.5. Renovación de Certificados

El proceso de renovación de Certificados podrá ser iniciado por el propio suscriptor, desde la parte pública de la UR, o bien por el propio registrador, tal y como se explica en el capítulo 3 del manual registradores con referencia MAN-REGISTER-OPTICCA-V1.0.PDF o versión superior.

5.6. Revocación de Certificados

El proceso de revocación de Certificados podrá ser iniciado por el propio suscriptor, desde la parte pública de la UR, o bien por el propio registrador, tal y como se explica en el capítulo 3 del manual registradores con referencia MAN-REGISTER-OPTICCA-V1.0.PDF o versión superior.