POLÍTICA DE SISTEMA DE ACCESOS Y COMUNICACIÓN ENTRE LA ECA Y AR

ADSIB-FD-POLT-004 Unidad de Infraestructura de Servicios

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	Rene Cayo	Jose Machicado	Jannett Ibañez
Cargo:	Profesional en Seguridad de la Información	Jefe de la Unidad de Infraestructura de Servicios	Directora Ejecutiva de la ADSIB
Firma:			
Fecha:			

POLÍTICA DE CERTIFICACIÓN PERFIL DE CERTIFICADO PERSONA NATURAL

Índice

POLÍTICA DE SISTEMA DE ACCESOS Y COMUNICACIÓN ENTRE LA ECA Y AR

1. Seguridad Física

1.1. Instalaciones Técnicas de la AR

Las instalaciones y los puestos de trabajo de una AR pueden ser de 2 (dos) tipos:

a) Ambiente dedicado a las actividades de la AR;
b) Ambiente compartido de la AR con otras actividades o servicios que la entidad brinda.

1.2 Requisitos mínimos de seguridad

Para ambos casos descritos en el punto 1.1 se aplican los siguientes requisitos mínimos de seguridad:

a) Disponer de equipos de prevención de incendios;
b) Armario o gabinete con llave, de uso exclusivo de la AR, para mantener los documentos de la AR.
c) Los circuitos eléctricos de alimentación del equipo de procesamiento de datos serán protegidos por UPS o estabilizadores de tensión.
d) Los circuitos eléctricos y lógicos deberán ser protegidos por cañerías y/o canaletas apropiadas.
e) Los ambientes deben tener instalados controles de seguridad ambientales (sensores de humo, fuego y otros) y monitorización (CCTV)

1.3. Requisitos aplicables para ambientes dedicados

Los siguientes requisitos son exclusivos para las AR que tengan un entorno dedicado, que se complementan a los requisitos del punto 1.2:

a) Revisión del control de acceso del ambiente dedicado, con autorización de acceso, sólo para los oficiales de registros y titulares de certificados;
b) Puerta de entrada única con cerradura reforzada u otros controles de acceso físicos;
c) Paredes y techos que prevengan el acceso no autorizado, construidas de material solido.
d) Iluminación de emergencia;
e) Si el ambiente tiene ventanas o cualquier otra abertura al entorno exterior de la entidad, estos deberán sellarse o ser enrejadas, para evitar el acceso no autorizado;

1.4. Requisitos aplicables para ambientes compartidos

Para las AR que han compartido ambientes, aplicará, además de los requisitos del punto 1.2, también los siguientes requisitos de seguridad:

a) Vigilancia intensiva o monitoreo por vídeo vigilancia en el ambiente de la AR;
b) Control de acceso al edificio o al entorno en el que está instalada la AR.

1.5. Control por sistema de circuito cerrado de televisión y vídeo vigilancia (CCTV)

El control por vídeo vigilancia puede ser llevado a cabo por la propia AR o subcontratar a una empresa externa de seguridad que realice este trabajo. Las cámaras deberán filmar el ambiente y el equipamiento de la AR y las imágenes deben ser mantenidas por 60 días en un ambiente seguro.

1.6. Puestos de registro instalados en Ferias o eventos de corta duración

Para los casos específicos de los puestos de registros de AR instalados en ferias y eventos por un periodo de funcionamiento máximo de 10 días, están exentas las exigencias de seguridad establecidas en los puntos 1.4 y 1.2, desde que los documentos y equipamientos sean llevados para su almacenamiento en una instalación técnica de la AR, al cierre diario de las actividades del puesto de registro.

2. Seguridad Lógica

2.1. Estaciones de trabajo

2.1.1. Las estaciones de trabajo de la AR, incluidos los equipos de computación portátiles deben ser protegidos frente a amenazas y acciones no autorizadas por personas indebidas.

2.1.2. Las estaciones de trabajo de la AR, incluidos los equipos de computación portátiles, deben recibir, por lo menos, las siguientes configuraciones de seguridad:

a) Control de acceso lógico al sistema operativo;
b) La exigencia de utilizar contraseñas fuertes y seguras;
c) Políticas de contraseñas y bloqueo de cuentas;
d) Logs de auditoría del sistema operativo activo que registre:

- Inicio y apagado del sistema;
- Intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios de los sistemas de operaciones de la RA;
- Cambios en la configuración de la estación;
- Intentos de acceso (login) y de salida del sistema (logoff) ;
- Intentos no autorizados de acceso a los archivos del sistema;
- Intentos de iniciar, eliminar, habilitar y deshabilitar a los usuarios y de actualizar y recuperar sus claves.

e) Tener implementados Procedimiento Contra Infección de Software Malicioso (MALWARE);
f) Firewall personal activado, con permisos de acceso mínimo necesarios para las actividades. Este requerimiento puede ser sustituido por firewall institucional, para los equipos instalados en redes que tienen tal dispositivo;

g) Protector de pantalla accionado como máximo 5 (Cinco) minutos de inactividad y exigiendo para su desbloqueo la contraseña del usuario;
h) Sistema operativo actualizado, con la aplicación de las correcciones necesarias;
i) Utilizar solamente el software necesario para llevar a cabo las actividades del oficial de registro;
j) Impedimento de acceso remoto, a través de otro equipo conectado a la red utilizado por la AR, excepto para las actividades de soporte remoto;
k) Utilización de fecha y hora GMT-4.

2.1.3 Los logs de auditoría del sistema operativo deben ser almacenados localmente por un período mínimo de 40 días.

2.1.4 El análisis de los logs solamente se llevará a cabo en caso de sospecha de acceso no autorizado para conocer las actividades realizadas en los equipos.

2.1.5 Es deseable que el Oficial de Registro no posea el perfil de administrador o contraseña de root de los equipos, dejando esa tarea delegada a terceros de la propia entidad, a fin de permitir la segregación de funciones.

3. Conectividad, comunicación y seguridad, Sistema AR

3.1. Modalidades de acceso entre la ECA y la AR

La AR deberá contar con un sistema de AR de acuerdo a las siguientes modalidades de acceso entre la ECA y la AR:

- Modalidad 1: Sistema propio de la AR que cumpla con lo especificado en la normativa vigente y los procesos establecidos por la ECA.
- Modalidad 2: Sistema de AR-ADSIB implementado en la infraestructura de la AR.
- Modalidad 3: Sistema de AR-ADSIB implementado en la infraestructura de la ECP accedido mediante internet desde la AR.

3.2. Requisitos mínimos de cada modalidades de acceso entre la ECA y la AR

	Modalidad 1	**Modalidad 2**	**Modalidad 3**
Conectividad	CO1	CO1	No aplica
Internet	INTS1	INTS1	INTA1
Centro de Procesamiento de Datos	CPD1	CPD1	No aplica
Convenios	CONV1	CONV1	No aplica

CO1: Para tener una conexión restringida en el intercambio de datos entre la Agencia de Registro (AR) y la Entidad Certificadora Pública (ECP), se utilizará una de las redes siguiente:

- Red Estatal promovida por la AGETIC.
- Red SIGMA Ministerio de Economía y Finanzas.
- En caso de no estar disponible ninguna de las anteriores Redes se utilizara una conexión VPN.

INTA1: La Agencia de Registro (AR) deberá disponer de un Servicio de Internet Asimétrico con un ancho de banda suficiente que garantice el acceso al sistema proveído por la Entidad Certificadora Pública (ECP), la ECP recomienda tener dos proveedores de internet para garantizar el acceso al sistema de la ECA.

INTS1: La Agencia de Registro (AR) deberá tener un Servicio de Internet Simétrico con un ancho de banda suficiente que garantice el acceso al sistema a los usuarios que requieren tener certificados digitales.

CPD1: La Agencia de Registro (AR) deberá tener un Centro de Procesamiento de Datos (CPD) que cumpla con estándares establecidos, para albergar el sistema de la Agencia de Registro. Así mismo se recomienda contar con los siguientes documentos:

- POLÍTICA DE CONTROL DE ACCESO
- POLÍTICA DE SEGURIDAD DE LA RED
- POLÍTICA DE SEGURIDAD PARA LA IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS
- POLÍTICA DE PANTALLAS Y ESCRITORIO LIMPIOS
- PROCEDIMIENTO DE SEGREGACIÓN DE USUARIOS Y ASIGNACIÓN DE USOS Y PRIVILEGIOS
- PROCEDIMIENTO CIERRE DE SESIÓN POR INACTIVIDAD

CONV1: La Agencia de Registro (AR) deberá firmar convenios con el SEGIP y SERECI para validar datos del usuario.

4. VERSIONES:

Versión	Fecha de Revisión	Descripción del cambio	Revisado por	Aprobado por	RES. ADM.	Fecha de aprobación
1	8/11/2018	• Elaboración del documento	Jose Machicado			