PROPÓSITO

Contar con un documento que describa de una manera sencilla los pasos a seguir por todos los colaboradores que conforman la Oficina de Seguridad Informática, a fin de mantener los niveles de seguridad requerido para que la plataforma a nivel nacional del Tribunal Electoral de Panamá funcione adecuadamente.

2.0 ALCANCE

El alcance de este procedimiento es aplicado a toda la plataforma tecnológica y los y usuarios internos y externos de la institución, la mismas contempla desde la definición de las políticas de seguridad, su implementación, así como de las tareas a efectuar en los hardware y software de seguridad y el monitoreo de los mismos.

3.0 RESPONSABILIDADES

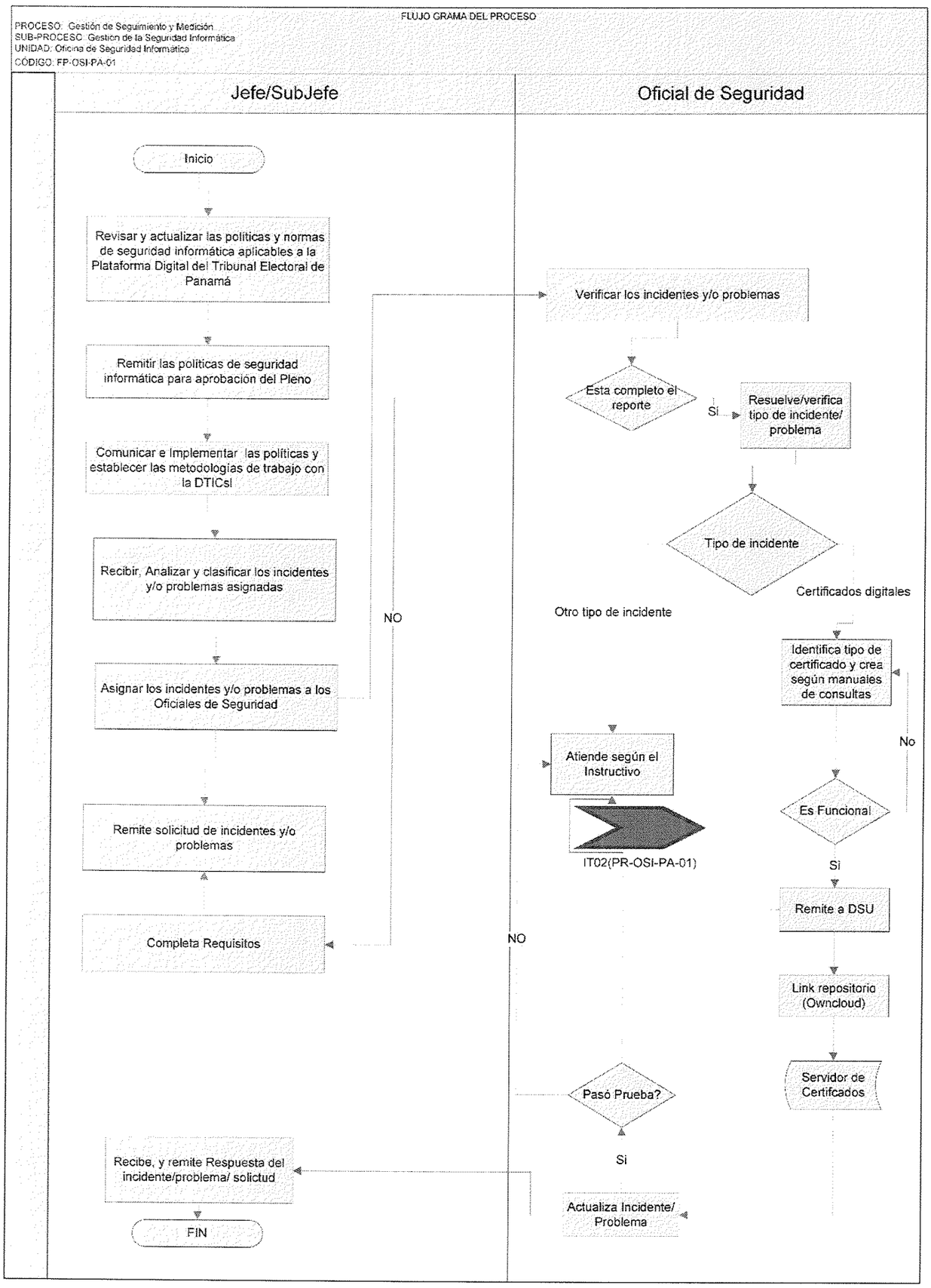
Jefe/Sub Jefe de Seguridad Informática

- Definir las políticas en materia de seguridad informática a implementar en la Institución
- Establecer los alcances de las políticas de seguridad a fin de presentarlas ante la DTICS para su implementación.
- Recibir, analizar, asignar y aprobar las solicitudes, incidentes y/o problemas al Oficial de Seguridad.

Oficial de Seguridad Informática

- Verificar y atender el(los) incidente(s), problema(s) y reporte(s) asignados para ejecutar según instrucciones de trabajo.
- Generar los certificados digitales para. (firmas digitales y Biométrico)
- Generar los filtrados de contenido de Internet (Bloqueo de páginas no permitidas)
- Bloqueo de Correo no deseado (Spam)

4.0 MAPA DE PROCESO



5.0 DESCRIPCIÓN DE LAS ACTIVIDADES

No	Responsable	Actividad
1	Jefe/ Sub Jefe	**Revisar y actualizar las políticas y normas de seguridad informática aplicables a la institución** Para establecer las políticas y normas de seguridad en la institución, el jefe y sub jefe de la Oficina de Seguridad procederán a: 1. Revisar las normas de seguridad ISO 27001, NIST y los estándares de ISM3. 2. Revisar las actualizaciones de los hardware o software que se efectúen a los elementos de seguridad de la institución, a fin de mejorar las políticas previamente establecidas. 3. Efectuar los estudios de mercado a fin de determinar las nuevas metodologías en temas de seguridad de la información aplicable a la institución. 4. Elaborar el documento que contendrá las políticas y normas aplicar, con la descripción de las actividades a efectuar y sus responsables de la implementación, monitoreo y alcance de la mismas. **Nota** Estas políticas serán revisadas y acordadas con la DTIC en cuanto al alcance de las mimas y su implementación. Una vez definidas y/o actualizadas las políticas de seguridad serán remitidas al Pleno para su aprobación.
2	Jefe/ Sub Jefe	**Comunicar las políticas y establecer las metodologías de trabajo con la DTIC a fin de garantizar la seguridad informática en la Institución** Aprobadas por el Pleno las políticas de seguridad de la información se procederán a comunicar las mismas y establecer las metodologías de trabajo con la Dirección de Tecnología de la Información y las Comunicaciones a fin de garantizar la seguridad informática en la Institución e implementarlo. Se efectúan las reuniones de trabajo a fin de establecer los responsables de su implementación, la bitácora de las mismas y los protocolos de seguridad. Esto con el fin de garantizar la seguridad y privacidad de los datos De igual manera se establecerán los mecanismos de supervisión de la administración del control de acceso a la información y el cumplimiento normativo de la seguridad de la información.

3	**Dirección de Tecnología de la Información y las Comunicaciones**	**Recibir las políticas de seguridad actualizadas e implementar en los elementos tecnológicos** Se efectúan las sesiones de trabajo o de reunión, se conocen las las políticas de seguridad actualizadas e implementar en los elementos tecnológicos. Se procede según el protocolo acordado de las Normas de Seguridad una vez efectuados las configuraciones, la Oficina de Seguridad monitorea diariamente todas las reglas y políticas establecidas en las normas de políticas de seguridad implementadas a fin de validar que las mismas corresponden a las establecidas.
4	**Dirección de Tecnología de la Información y las Comunicaciones**	**Remitir solicitud de incidentes y/o problemas** Remitir los diferentes incidentes/problemas/Solicitudes en cuanto a la Seguridad de la plataforma informática de la Institución a través de la herramienta Mesa de Ayuda de la sección de Atención al Usuario.
5	**Jefe/ Sub Jefe**	**Recibir, Analizar y clasificar los incidentes, reportes y/o problemas asignadas.** A través de la herramienta Mesa de Ayuda de la sección de Usuario y de acuerdo a su prioridad, urgencia y disponibilidad de recursos, reciben, analizan y asignan al oficial de seguridad informática los diferentes incidentes y/o problemas. **NOTA**: En caso de que el Jefe no esté y se dé otra situación que amerite que ellos no puedan asignar las solicitudes, se debe asignar a un Oficial de Seguridad Informática la responsabilidad de recibir, analizar y/o asignar las solicitudes, incidentes y/o problemas.
6	**Jefe/ Sub Jefe**	**Asignar los incidentes, reportes y/o problemas** Asignar los incidentes y/o problemas según el tipo de solicitud y de las herramientas empleadas a cada Oficial de Seguridad Informática.
7	**Oficial de Seguridad Informática**	**Verificar los incidentes, reporte y/o problemas** Verificar y atender las órdenes de servicio, siempre y cuando cumplan con los criterios solicitados (Nombre, Apellido, Teléfono oficina, descripción de lo solicitado, aprobación del jefe inmediato, del director nacional y/o de secretaría general).
8	**Oficial de Seguridad Informática**	**Está completo el reporte** **Si está completo Resuelve/verifica tipo de incidente/problema**

		Resolver el incidente y/o problemas asignados. **NOTA**: Si un Oficial de Seguridad Informática atendió uno o más casos por teléfono, correo electrónico, Microsoft Teams, Net Meeting u otro medio para resolver una o más situaciones y la orden de servicio la tiene asignada otro Oficial de Seguridad Informática, éste podrá reasignar la orden y/o las órdenes al Oficial de Seguridad Informática que realizó la atención.
8.1	**Oficial de Seguridad Informática**	**Si no está completo el reporte,** solicitar a la DTIC completar los datos o requerimientos faltantes.
9	**Oficial de Seguridad Informática**	**Verificar qué tipo de reporte o incidente es.** verificar que tipo de reporte deberá atender para seguir las directrices que correspondan.
9.1	**Oficial de Seguridad Informática**	**Identificar tipo de certificado digital y crea según manuales de consultas,** para ello procede a: • Emisión de certificado digitales para firma digital, cada usuario se le solicita la cedula y su nombre para que luego firme su documento no sean alterados. • Emisión del certificado digital para Dispositivos tipo Web, por cliente es de tipo de autenticación • Emisión del certificado digital Sistema Biométrico. Solicita la cedula y serial del equipo para los hospitales.
9.1.1	**Oficial de Seguridad Informática**	**Validar que el certificado creado es funcional** **Si es funcional, remite al soporte técnico para su instalación** En caso de que no pueda entrar el certificado, debido a que le formatearon el pc y/o este corrupto el mismo, se vuelve al primer punto en caso de que no se encuentre el certificado en el repositorio de certificados digitales.
9.1.1.1	**Oficial de Seguridad Informática**	**Colocar el certificado digital en el Link repositorio (Owncloud).** • Exportar desde en un Servidor los certificados de SVI. • Traspasar por medio de un correo electrónico a las empresa privadas y públicas, y luego te llaman para pedir la contraseña del portal.
9.1.2.	**Oficial de Seguridad Informática**	**Si no es funcional el certificado, procede a verificar nuevamente** • Volver a enviar el mismo certificado digital para su reinstalación en sitio en caso no es funcional.
9.2	**Oficial de Seguridad Informática**	**Otro tipo de Incidente** **Si el incidente o reporte asignado corresponde a:** a. Actualización de los sistemas de seguridad informática b. Soporte a Software de Seguridad

		c. Soporte de Hardware de Seguridad d. Monitoreo Reactivo e. Monitoreo a las políticas de cumplimiento f. Filtrado de contenido en páginas WEB g. Generación de certificados de dispositivos VPN y Firma Digital h. Bloqueo de Correo no deseado (Bandeja de entrada y salida) Procederá a ejecutar lo descrito en el **instructivo IT02(PR-OSI-PA-01) Para la seguridad de los sistemas informáticos o aplicativos de la institución por parte del Oficial de Seguridad.**
9.2.1	Oficial de Seguridad Informática	**Verificar que lo actuado pase las pruebas** **Si pasa las pruebas procede a actualizar el reporte o incidente.** Detallar los trabajos que se efectuaron y a solución brindada en la mesa de ayuda.
9.2.2	Oficial de Seguridad Informática	**Si no pasa las pruebas, proceder a verificar según el instructivo.** Proceder a revisar los puntos descritos en el **instructivo IT02(PR-OSI-PA-01) Para la seguridad de los sistemas informáticos o aplicativos de la institución por parte del Oficial de Seguridad** para corregir y validar la funcionabilidad de la solución a dar, para ello se le solicita al usuario que nos indique con impresión de pantalla el error específico
10.	Oficial de Seguridad Informática	**Actualizar Incidente/Problema y lo remite al Jefe y Sub Jefe de la Oficina.** Proceder a actualizar en la mesa de ayuda, el reporte asignado indicando el problema y la solución efectuada. y se lo envía al jefe para su actualización. En caso de al momento de efectuar la solución detecta una situación que atañe con las políticas de seguridad por parte del usuario del equipo o de la cuenta, procederá a efectuar el reporte al Jefe y Sub Jefe de la Oficina a fin de proceder según lo establecido por la Oficina de seguridad.
11	Jefe/ Sub Jefe	**Recibir, y remitir Respuesta del incidente/problema/ solicitud.** Recibir las respuestas a los reportes asignados por los oficiales de seguridad, a fin de garantizar que las asignaciones de la oficina se atiendan con la debida atención y prontitud. En el caso de recibir reportes de usuarios que atañen contra las políticas de seguridad aprobadas por el PLENO procederá a informar a los Directivos de la unidad a la que corresponde el colaborar y de darse reincidencias informar al PLENO para acciones a tomar y proceder con las investigaciones que amerite.

12	**Dirección de Tecnología de la Información y las Comunicaciones**	**Recibir Respuesta del incidente/problema/ solicitud** Recibir el cierre de los reportes por parte del Oficial de Seguridad.

6.0 REFERENCIAS DOCUMENTALES

Código	Nombre del documento
IT02(PR-OSI-PA-01)	**Para la seguridad de los sistemas informáticos o aplicativos de la institución por parte del Oficial de Seguridad**
N/A	**Política y Normas de Seguridad Informática**
N/A	**Manual de Usuario de SVI III.**

7.0 DEFINICIONES

Política y Normas de Seguridad para la Red Informática	Documento que especifica que políticas y normas que pueden y deben hacer a fin de regular los procedimientos y recursos asociados y cuando deben ser aplicados, quien y cuando los debe aplicar a un proyecto, proceso, producto o contrato específico.
Certificado Digital	es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet.
Monitoreo Reactivo	Monitoreo que permiten ajustar parámetros y configuraciones en el caso de que uno de estos logre ganar acceso no autorizado, el cual incluye la vigilancia de los IPS, Y FIREWALL.
Filtrado de contenido	Controlar qué contenido (páginas web, sitios de reuniones) se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web.
VPN	Una red privada virtual (RPV) que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
Firma Digital	es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento, el cual se genera en formato PDF.
Correo no deseado	Bloqueo de correo dudosa procedencia o que no esté autorizado por la institución a recibir .

8.0 REGISTROS

Código	Nombre	Tiempo de almacenaje	Responsable de mantener
N/A	**Filtrado de contenido**	**2 años**	**Oficial de seguridad**
N/A	**Correo no deseado (Spam)**	**2 años**	**Jefe de seguridad**

N/A	**Firma digital , aplicativo WEB y Biométrico**	**2 años**	**Oficial de seguridad**

9.0 CONTROL / HISTORIAL DE CAMBIOS

Control / Historial de Cambios			
Revisión	**Autor**	**Fecha**	**Descripción del(los) Cambio(s)**
00	Kathiel Avila	Octubre 2009	Emisión del documento por 1ª vez
01	Kathiel Avila	Noviembre 2009	Revisión y Corrección de Responsabilidades y Diagrama.
02	Kathiel Avila	Marzo 2010	Actualización de nombre, propósito y alcance, se modificó el mapa, se documentaron los procedimientos. Se cambiaron los procedimientos PR-IN-PA-13 Y PR-IN-PA-27 y se convirtieron en instrucciones de trabajo. En estos es que se hace la liberación de las órdenes de servicio. Se eliminó el procedimiento PR-IN-PA-11, ya que este después de una revisión se verifico que se podía fusionar con este procedimiento descrito en este documento para que así quedase un solo procedimiento y dos instrucciones de trabajo.
03	Kathiel Avila	Septiembre 2010	Se agrega el puesto de Asistente de Seguridad Informática.
04	Kathiel Avila	Noviembre 2010	Cambio en la descripción de las actividades. Cambio en el diagrama de flujo. Actualización en las definiciones de términos.
05	Kathiel Avila	Abril 2011	Cambio en la segunda nota.
06	Kathiel Avila	Octubre 2011	Cambio en la nomenclatura del código.
07	Kathiel Avila	Abril 2012	**NOTA**: En caso de que el Jefe de Seguridad Informática y/o la Asistente de Seguridad Informática no esté (n), quien ellos designen como Jefe de Seguridad Informática a.i. y/o otra situación que amerite que asignen a un Oficial de Seguridad Informática la responsabilidad de recibir, analizar y/o asignar las solicitudes, incidentes y/o problemas. **NOTA**: Si un Oficial de Seguridad Informática atendió uno o más casos por teléfono, correo electrónico, Teamviewer, net meeting u otro medio para resolver una o más situaciones y la orden de servicio la tiene asignada otro Oficial de Seguridad Informática este podrá reasignar la

			orden y/o las ordenes al Oficial de Seguridad Informática que realizo la atención.
08	Kathiel Avila	Mayo 2012	Se agrega logo de la empresa que certifica.
09	Kathiel Avila	Enero 2013	Se quita el logo de la empresa que certifica.
10	Kathiel Avila	Enero 2013	Se modifica asistente de la dirección.
11	Anibal Almengor	Septiembre 2014	Se modifica el flujo del proceso e instrucciones de trabajo, se incluye las instrucciones de trabajo IT03 e IT04, se incluyen las actividades 7 y 8 referentes a estas mismas instrucciones de trabajo.
12	Anibal Almengor	Enero 2015	Se modifica el flujo del proceso donde se incluye que, si no cumple con los requisitos la orden de servicio de incidente y/o problema se cierra el flujo, título de la instrucción IT01, se modifica el título de asistente a Sub Jefe. En la actividad 2 se incluye que también el Sub Jefe de Seguridad Informática puede asignar incidentes y/o problemas al Oficial de Seguridad Informática. Se reubicaron las notas en las actividades 1 y 3.
13	Anibal Almengor	Enero 2015	Se modifica el título de la IT02 de Instalación y Mantenimiento de Software y Hardware de Seguridad a Soporte a Software y Hardware de Seguridad. Se Elimina instrucción de trabajo IT04. Se modifica las actividades 1, 4, 5, 6 y 7.
14	Anibal Almengor	Noviembre 2015	Se modificó el alcance del procedimiento y se cambió el título de asistente a Sub Jefe de Seguridad Informática.
15	Anibal Almengor	Septiembre 2016	Se eliminó la tarea de otorgar permisos dentro de la red.
16	Anibal Almengor	Octubre 2016	Se añadió la actividad de revisión de equipos.
	Anibal Almengor		• Creación de la Unidad de Seguridad Informática Sesión del Pleno 23 del 2 de mayo del 2017.

17	Anibal Almengor	Agosto 2018	• Cambio de los códigos de la documentación (procedimientos, instructivos, formatos). • Se agrega la actividad # 1. • Se modifica el propósito del documento. • Se modifica el Flujograma del Procedimiento. • Eliminación del instructivo IT01(PR-OSI-PA-01). • Eliminación del instructivo IT03(PR-OSI-PA-01). • Eliminación del instructivo IT04(PR-OSI-PA-01). • Modificación del paso # 6 para colocar lo descrito en el instructivo IT01(PR-OSI-PA-01). • Modificación del paso # 8 para colocar lo descrito en el instructivo IT03(PR-OSI-PA-01). • Modificación del paso # 9 para colocar lo descrito en el instructivo IT04(PR-OSI-PA-01). Se agrega la actividad # 10.
18	Anibal Almengor	Enero 2021	• Se modifica Título Unidad de Seguridad Informática. • Se modifica el flujo general y la narrativa del procedimiento • Se modifica el instructivo IT02(PR-OSI-PA-01) a fin de consolidarlo en un documento para uso del oficial de seguridad.