Universidad Estatal a Distancia

Rectoría

Dirección de Tecnología de Información y Comunicaciones

Unidad de Seguridad Digital

Gestión de la Seguridad de las Tecnologías de Información y Comunicaciones

PUNED DTIC-USD 01

Índice

Participantes

Elaboración

Nombre	Puesto	Dependencia
Johnny Saborío Álvarez	Coordinador de la USD	Dirección de Tecnología de Información y Comunicaciones
Michael González Flores	Especialista en Seguridad Informática	Dirección de Tecnología de Información y Comunicaciones
Alejandro Sánchez Rivera	Especialista en Seguridad Informática	Dirección de Tecnología de Información y Comunicaciones

Validación

Nombre	Puesto	Dependencia	Fecha
Francisco Durán Montoya	Director	Dirección de Tecnología de Información y Comunicaciones	25 de setiembre de 2023

Aprobación

Aprobado mediante acuerdo tomado por el Consejo de Rectoría, sesión extraordinaria No. 2318-2024, Artículo VI, inciso 2) celebrada el 27 de mayo del 2024 (REF. CR-2024-935).

Asesoría Técnica

Lic. Carlos Salazar Castañeda, Centro de Planificación y Programación Institucional.
Lic. Paula Martínez Sánchez, Centro de Planificación y Programación Institucional.

1. Propósito

Describir las actividades para la gestión de seguridad de las tecnologías de información, comunicaciones y ciberseguridad, la aplicación de los respectivos controles y medidas que se realizan sobre la infraestructura tecnológica de la Universidad Estatal a Distancia (UNED).

2. Alcance

Este documento debe ser de conocimiento de todas las personas funcionarias UNED y del personal de la Dirección de Tecnología de Información y Comunicaciones, específicamente de la Unidad de Seguridad Digital.

3. Responsabilidades

- La persona coordinadora de la Unidad de Seguridad Digital, es la responsable de la coordinación, planificación, control y seguimiento de las actividades que se realizan en dicha unidad.
- Las personas funcionarias en la Unidad de Seguridad Digital, tienen la responsabilidad técnica de analizar y mitigar las alertas e incidentes de seguridad, que se generan del monitoreo de eventos y ejecutan las solicitudes que indique la persona coordinadora de la Unidad de Seguridad Digital.

4. Definiciones

- **Alerta:** es un aviso reactivo ante una posible amenaza de ciberseguridad, que puede representar un alto riesgo para la infraestructura tecnológica y la información de la UNED.
- **Ambiente de protección**: portal utilizado para configurar los elementos de seguridad y funcionamiento de las aplicaciones, sitios web, Apis e Ips a proteger.
- **Anomalías al reglamento:** cualquier comportamiento que vaya en contra al correcto uso de equipos de cómputo y el acceso a Internet, que incluye material restringido y pornográfico, según lo establecido en el Reglamento para uso de equipos de cómputo e internet de la UNED.
- **Código fuente:** es el texto redactado que puede ser comprendido por un lenguaje de programación determinado, con el fin de desarrollar rutinas, aplicaciones, sistemas, servicios, entre otros.
- **Dashboard:** es una forma de presentar de manera visual mediante un portal web, los datos más importantes a nivel de ciberseguridad de las Apps, servicios, servidores y dispositivos finales; entre otros, de la infraestructura tecnológica que se está monitoreando, mostrando valores estadísticos, tendencias, elementos más críticos o de mayor importancia y relevancia.
- **Detecciones**: son posibles amenazas (tipo malware) que pueden afectar a los dispositivos, que son protegidos mediante la seguridad del punto final.
- **Directorio Activo**: es una base de datos y un conjunto de servicios, que conectan a los usuarios con los recursos de red, que necesitan para realizar su trabajo.

- **Dispositivos tecnológicos:** todo dispositivo tecnológico con funciones similares a un computador o un servidor.
- **Escaneos Dinámicos:** es un tipo de prueba de seguridad, que intenta detectar vulnerabilidades de aplicaciones web, mediante el método de caja negra (Black-Box).
- **Incidente de seguridad:** Un incidente de seguridad es un evento adverso en un sistema de Información, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

5. Documentos Relacionados

- Formulario de autorizaciones FUNED DTIC-USD 01.00.01.
- Guía para la planificación, calendarización y ejecución de los monitoreos y diagnósticos preventivos.
- Instructivo para la atención de alertas e incidentes IUNED DTIC USD 01.01.
- Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones de la Universidad Estatal a Distancia MEGAC-PEGAC.03-PR-06.

6. Normativa relacionada

- Acuerdo de creación de la Comisión Estratégica de Tecnología de Información y Comunicaciones (CETIC)-UNED y sus funciones, sesión: 2406-2015, Artículo II, inciso 1-a).
- Acuerdo de Políticas para el Uso y Seguridad de internet (Sesión 1604-2002, Art. VIII, inciso 2) celebrada el 24 de octubre del 2002).
- Marco de Gobierno y Gestión de TI de la UNED, objetivo de gobierno y objetivo de gestión: seguridad de la información.
- Normas técnicas para el gobierno y gestión de las tecnologías de la información del MICITT, proceso XI Seguridad y Ciberseguridad.
- Políticas para el Uso y Desarrollo de Tecnologías de la Información y la Comunicación de la UNED.
- Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia, capítulo II, artículo 5, incisos: a), b), d), e), f), h), i), m), n), q) y el capítulo VI.

7. Abreviaturas

- **APIs**: Interfaz de programación de aplicaciones.
- **DTIC**: Dirección de Tecnología de Información y Comunicaciones.
- **IPs**: Direccionamiento de Protocolo de Internet.
- **ORH**: Oficina de Recursos Humanos.
- **SOC:** Centro de Operaciones de Seguridad.

- UIT: Unidad de Infraestructura Tecnológica.
- USD: Unidad de Seguridad Digital.
- USI: Unidad de Sistemas de Información.
- UST: Unidad de Soporte Técnico.

8. Descripción del Proceso

8.1. Gestión de alertas e incidentes provenientes del SOC[1].

8.1.1. La persona funcionaria de la USD, recibe correo electrónico o tiquete de alerta e incidentes provenientes del SOC.

8.1.2. La persona funcionaria de la USD designada, realiza el análisis de la información que se adjunta al correo recibido y clasifica su contenido para atender la alerta, dar respuesta y seguimiento respectivo, aplicando lo que indica el **Instructivo para la atención de alertas e incidentes IUNED DTIC USD 01.01**.

8.1.3. Luego de haber realizado la investigación respectiva de conformidad con el **Instructivo para la atención de alertas e incidentes IUNED DTIC USD 01.01**, la persona funcionaria de la USD, procede a gestionar la alerta, según corresponda.

8.1.3.1. Si la alerta se resuelve correctamente, la persona funcionaria de la USD, procede a redactar el correo de respuesta al SOC, para que sea cerrado el tiquete. **Fin de proceso.**

8.1.3.2. Si la alerta no se resuelve correctamente y requiere una reapertura del tiquete, en caso de ser necesario[2], pasa al punto 8.1.3.

Fin de sección.

8.2. Gestión para la atención de estudios, incidentes y/o anomalías de Seguridad Informática

8.2.1. La persona responsable de una dependencia solicitante, que requiera un estudio sobre el uso de equipo de cómputo e internet, realiza la solicitud por medio de un oficio o del **Formulario de autorizaciones FUNED DTIC-USD 01.00.01**, enviado a la USD.

8.2.2. La persona directora de la DTIC o la persona coordinadora de la USD, analiza la solicitud para realizar el estudio respectivo, tal y como se indica en el **Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones de la Universidad Estatal a Distancia MEGAC-PEGAC.03-PR-06.**

---

[1] Equipo externo que brinda soporte a la USD en materia de ciberseguridad.

[2] La actividad 8.1.3.2 se puede repetir de manera indefinida hasta que se descarte el posible incidente y no se presente nuevamente la alerta.

8.2.2.1. En caso de ser aceptada la solicitud, la persona coordinadora de la USD, designa a una persona responsable de la Unidad para atenderla, pasa al punto 8.2.3.

8.2.2.2. En caso de ser denegada la solicitud, la persona directora de la DTIC o persona coordinadora de la USD, remite un oficio con la justificación. **Fin de proceso.**

8.2.3. La persona funcionaria de la USD, instala software para analizar eventos, revisa las últimas actividades realizadas en el equipo de cómputo y ejecuta cualquier otra acción necesaria, en coordinación con las personas funcionarias de las dependencias respectivas, en caso de ser necesario.

8.2.4. La persona funcionaria de la USD, realiza el estudio.

8.2.4.1. En caso de no detectar incidentes o anomalías al reglamento[3], pasa al punto 8.2.5.

8.2.4.2. En caso de detectar un incidente de seguridad o anomalías al reglamento.

8.2.4.2.1. Si se detecta un incidente de seguridad, la persona funcionaria de la USD, ejecuta las acciones necesarias para eliminar el riesgo, mitigar los daños y realizar las labores correctivas que procedan, en coordinación con las unidades de la DTIC que correspondan y/o con las personas funcionarias de las dependencias respectivas, pasa al punto 8.2.5.

8.2.4.2.2. En caso de encontrar anomalías al reglamento, la persona funcionaria de la USD, recopila la evidencia respectiva, que formará parte del informe que será enviado a la persona responsable de una dependencia solicitante, con el fin de que proceda con lo correspondiente, según lo establecido en el Estatuto de Personal y el Estatuto Orgánico, pasa al punto 8.2.5.

8.2.5. La persona funcionaria de la USD, elabora el Informe respectivo, el mismo es aprobado por la persona coordinadora de la USD, luego se envía a la persona directora de la DTIC y a la persona responsable de la dependencia involucrada.

Fin de sección.

8.3. Gestión para la elaboración de los informes de monitoreos en las Sedes Universitarias y en la Sede Central.

8.3.1. Al inicio de cada año laboral, la persona funcionaria de la USD, define las fechas para programar la cantidad de monitoreos a realizarse.

[3] Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia.

8.3.2. La persona funcionaria de la USD, ingresa a la herramienta de monitoreo y elaboración de informes, según lo que indica el **Anexo 2. Actividades de monitoreo.**

8.3.3. La persona funcionaria de la USD, realiza el análisis del monitoreo.
8.3.3.1. Si se detecta anomalías.
8.3.3.1.1. Si corresponde a posibles incidentes de ciberseguridad, la persona funcionaria de la USD, procede a realizar las diferentes actividades para mitigar las amenazas a la infraestructura tecnológica de la Universidad y su información (bloquear direcciones IP, aplicaciones, puertos, entre otros), pasa al punto 8.3.4.
8.3.3.1.2. Si se detectan anomalías al **Reglamento para Uso de Equipos de Cómputo e Internet**, la persona funcionaria de la USD, recopila la evidencia respectiva, que formará parte del informe que será enviado a la persona responsable de la dependencia, con el fin de que proceda con lo correspondiente, según lo establecido en el Estatuto de Personal y el Estatuto Orgánico, pasa al punto 8.3.4.
8.3.3.2. Si no se detectan anomalías y posibles incidentes de ciberseguridad, pasa al punto 8.3.4.

8.3.4. La persona funcionaria de la USD, realiza un informe de cada monitoreo por Sede Universitaria y de la Sede Central, y se lo traslada a la persona coordinadora de la USD, para lo que corresponda.

8.3.5. La persona funcionaria de la USD, realiza un respaldo de los informes en las carpetas respectivas destinadas por la Unidad, según la **Guía para la planificación, calendarización y ejecución de los monitoreos y diagnósticos preventivos.**

Fin de sección.

8.4. Gestión para el monitoreo del Tenant de personas estudiantes y personas funcionarias

8.4.1. La persona funcionaria de la USD, ingresa a la herramienta de monitoreo del Tenant, selecciona la opción de Alertas y filtra por categorías las alertas detectadas.

8.4.2. La persona funcionaria de la USD, analiza cada una de las alertas.
8.4.2.1. Si la persona funcionaria de la USD no detecta un posible incidente en la cuenta del usuario, pasa al punto 8.4.6.

8.4.2.2. Si la persona funcionaria de la USD detecta un posible incidente en la cuenta del usuario, se comunica[4] con la persona funcionaria involucrada.

8.4.2.2.1. Si se logra comunicar con la persona funcionaria, pasa al punto 8.4.3.

8.4.2.2.2. Si no logra comunicarse con la persona funcionaria, pasa al punto 8.4.4.

8.4.3. La persona funcionaria de la USD, requiere verificar si la persona funcionaria ha realizado alguna acción, ya que ha llegado un posible incidente en su cuenta de usuario.

8.4.3.1. Si el posible incidente fue generado por la persona funcionaria. Pasa al punto 8.4.5

8.4.3.2. Si el posible incidente no fue generado por la persona funcionaria, la persona funcionaria de la USD, hace un estudio para tomar las acciones correspondientes[5], pasa al punto 8.4.5

8.4.4. La persona funcionaria de la USD, realiza un tiquete de Solicitudes de atención y requerimientos, para proteger la cuenta del usuario a la UIT; además, gestiona las acciones necesarias para la atención del posible incidente.

8.4.5. La persona funcionaria de la USD, registra en la bitácora los hallazgos encontrados relacionados con el compromiso de una cuenta de personas funcionarias.

8.4.6. La persona funcionaria de la USD, cierra la alerta y se detalla las acciones realizadas en la herramienta de monitoreo.

Fin del proceso.

8.5. Gestión de amenazas de seguridad de punto final

8.5.1. La persona funcionaria de la USD, identifica y revisa las alertas visualizadas en la consola de gestión de amenazas de seguridad de punto final.

8.5.1.1. Si la persona funcionaria de la USD no detecta una amenaza en la consola, fin de proceso.

8.5.1.2. Si la persona funcionaria de la USD detecta una amenaza en la consola, pasa al punto 8.5.2.

8.5.2. La persona funcionaria de la USD, realiza el análisis de las detecciones que se visualicen en la consola y efectúa las posibles mitigaciones que se deban realizar, según el tipo de

---

[4] En el caso de las personas estudiantes no se realiza comunicación alguna, sino que la persona funcionaria de la USD toma las acciones a seguir y registra en la bitácora los hallazgos encontrados.

[5] Algunas acciones podrían ser desde bloquear direcciones IP, reestablecer las credenciales, entre otros.

amenaza, de conformidad al **Instructivo para la atención de alertas e incidentes IUNED DTIC-USD 01.01.**

8.5.3. A final de mes, la persona funcionaria de la USD, remite informe a la persona coordinadora de la USD, el cual incluye las detecciones y demás labores realizadas, con respecto a la gestión de amenazas de seguridad de punto final.

Fin de sección.

8.6. Gestión para escaneos dinámicos.

8.6.1. La persona funcionaria de la USD, recibe correo electrónico proveniente de la persona coordinadora o de las personas coordinadoras de proyectos informáticos de la USI, solicitando la ejecución de uno o varios escaneos dinámicos sobre aplicaciones o sistemas web.

8.6.2. Para la programación de los escaneos, la persona funcionaria de la USD utiliza la plataforma SaaS, para la revisión del código fuente, que permite identificar brechas de seguridad, antes de enviar a producción una aplicación o cuando la misma ya se encuentra en funcionamiento.

8.6.3. La persona coordinadora de la USD, solicita la autorización a la persona solicitante de la USI, para proceder con el inicio del escaneo.

8.6.3.1. Si se cuenta con la autorización de parte de la persona solicitante de la USI, pasa al punto al 8.6.4.

8.6.3.2. Si no se cuenta con la autorización de parte de la persona solicitante de la USI. **Fin del proceso.**

8.6.4. La persona funcionaria de la USD, coordina reuniones con la persona coordinadora o las personas coordinadoras de proyectos informáticos de la USI y la persona analista de la USI, responsable de la aplicación o sistema web, con la finalidad de determinar y analizar los detalles técnicos de las aplicaciones que se van a escanear.

8.6.5. Una vez analizadas las aplicaciones, la persona funcionaria de la USD, en caso de ser requerido, solicita las credenciales a las personas funcionarias de la USI[6], para realizar las pruebas y verificar que las mismas funcionen.

8.6.5.1. Si las credenciales funcionan, la persona funcionaria de la USD, ingresa a la herramienta de escaneos dinámicos, para crear la aplicación y programar el escaneo. Pasa al punto 8.6.6.

---

[6] Son las personas analistas y la persona coordinadora de la USI.

8.6.5.2. Si las credenciales no funcionan, la persona funcionaria de la USD, solicita nuevamente las credenciales, regresa al punto 8.6.5.

8.6.6. La persona funcionaria de la USD, recibe una notificación por correo electrónico, vinculando el resultado del escaneo de la aplicación creada.

8.6.7. La persona funcionaria de la USD, remite correo electrónico a las personas funcionarias de la USI (la persona coordinadora de proyectos informáticos de la USI y la persona analista de la USI responsable de la aplicación), comunicando que el escaneo se realizó.

8.6.8. Si la persona funcionaria de la USI, define que se requiere un acompañamiento de parte de la USD, solicita el espacio.

8.6.8.1. De requerirse el espacio, la persona funcionaria de la USD, programa la reunión para atender las consultas.

8.6.8.1.1. Si las consultas pueden ser atendidas por la USD, fin de proceso.

8.6.8.1.2. Si las consultas no pueden ser atendidas por la USD, la persona funcionaria de la USD, lo eleva a la empresa proveedora para que brinde respuesta. Regresa al punto 8.6.8.

8.6.8.2. De no requerirse el espacio, la persona funcionaria de la USI, continúa con el siguiente escaneo. Fin de proceso.

Fin de sección.

8.7. Gestión para la actualización de productos y licencias de seguridad de los dispositivos tecnológicos.

8.7.1. La persona funcionaria de la USD, recibe una solicitud a través de la plataforma de comunicación, utilizada con las personas funcionarias de la UST.

8.7.2. La persona funcionaria de la USD, solicita a las personas funcionarias de la UST el nombre del equipo o la dirección IP, para actualizar los productos y licencias de seguridad del punto final.

8.7.3. La persona funcionaria de la USD, comunica a la persona funcionaria de la UST, que el equipo cuenta con los productos y licencias de seguridad del punto final actualizados.

Fin de sección.

8.8. Gestión para la protección de APIs, Ips y Sitios Web

8.8.1. La persona funcionaria de la USD, recibe correo electrónico proveniente de la persona directora de DTIC, de la persona coordinadora de la USI o de las personas coordinadoras de proyectos informáticos de la USI o de alguna persona responsable de una dependencia de la Universidad, solicitando la protección de un APIs, Ips o Sitios Web institucional.

8.8.2. La persona funcionaria de la USD, analiza el API, Ips o Sitios Web institucional a proteger y da respuesta al correo electrónico, solicitando los detalles técnicos necesarios para realizar dicha protección.

8.8.3. La persona funcionaria de la USD, configura el ambiente de protección, dentro del entorno de seguridad de API, Ips y Sitios Web.

8.8.4. La persona funcionaria de la USD, en coordinación con la persona responsable del API, Ips o Sitios Web institucional, realizan pruebas de funcionamiento.

8.8.4.1. Si las pruebas fueron satisfactorias, la persona funcionaria de la USD en coordinación con la persona funcionaria de la UIT, implementan de forma permanente la nueva capa de seguridad en el elemento a proteger (API, las Ips o el sitio web), según sea el caso. Pasa al punto 8.8.5.

8.8.4.2. Si las pruebas no fueron satisfactorias.

8.8.4.2.1. En caso de que funcione el API, las Ips o el sitio web, pero requiere ajustes para dejar funcional el elemento a proteger. Pasa al punto 8.8.4.

8.8.4.2.2. En caso de que no funcione el API, las Ips o el sitio web, la persona funcionaria de la USD, elimina del entorno de protección hasta encontrar una solución definitiva, pasa al punto 8.8.5

8.8.5. La persona funcionaria de la USD, realiza un monitoreo permanente del funcionamiento del elemento protegido (API, las Ips o el sitio web), según sea el caso.

Fin de sección.

8.9. Supervisión de la actividad de las cuentas de usuario de funcionarios y estudiantes a nivel del Directorio Activo.

8.9.1. La persona funcionaria de la USD, ingresa a la plataforma de Monitoreo y Auditoría en tiempo real del Directorio Activo.

8.9.2. La persona funcionaria de la USD, revisa cada uno de los gráficos de comportamiento, el Dashboard de alertas y eventos de comportamiento de las cuentas de Directorio Activo, según clasificación (Critical, Trouble y Attention).

8.9.2.1. Si se encuentran anomalías, la persona funcionaria de la USD, analiza la información para mitigar cualquier incidente de seguridad.

8.9.2.1.1. Si la alerta puede ser mitigada por la persona funcionaria de la USD, la ejecuta y procede a cerrar la alerta. **Fin de proceso.**

8.9.2.1.2. Si la alerta no puede ser mitigada por la persona funcionaria de la USD, solicita el apoyo de las personas funcionarias de la UIT para ser atendida y posteriormente, ejecutan la remediación y proceden a cerrar la alerta. **Fin de proceso.**

8.9.2.2. Si no se encuentra anomalías, **fin de proceso**

Fin de proceso.

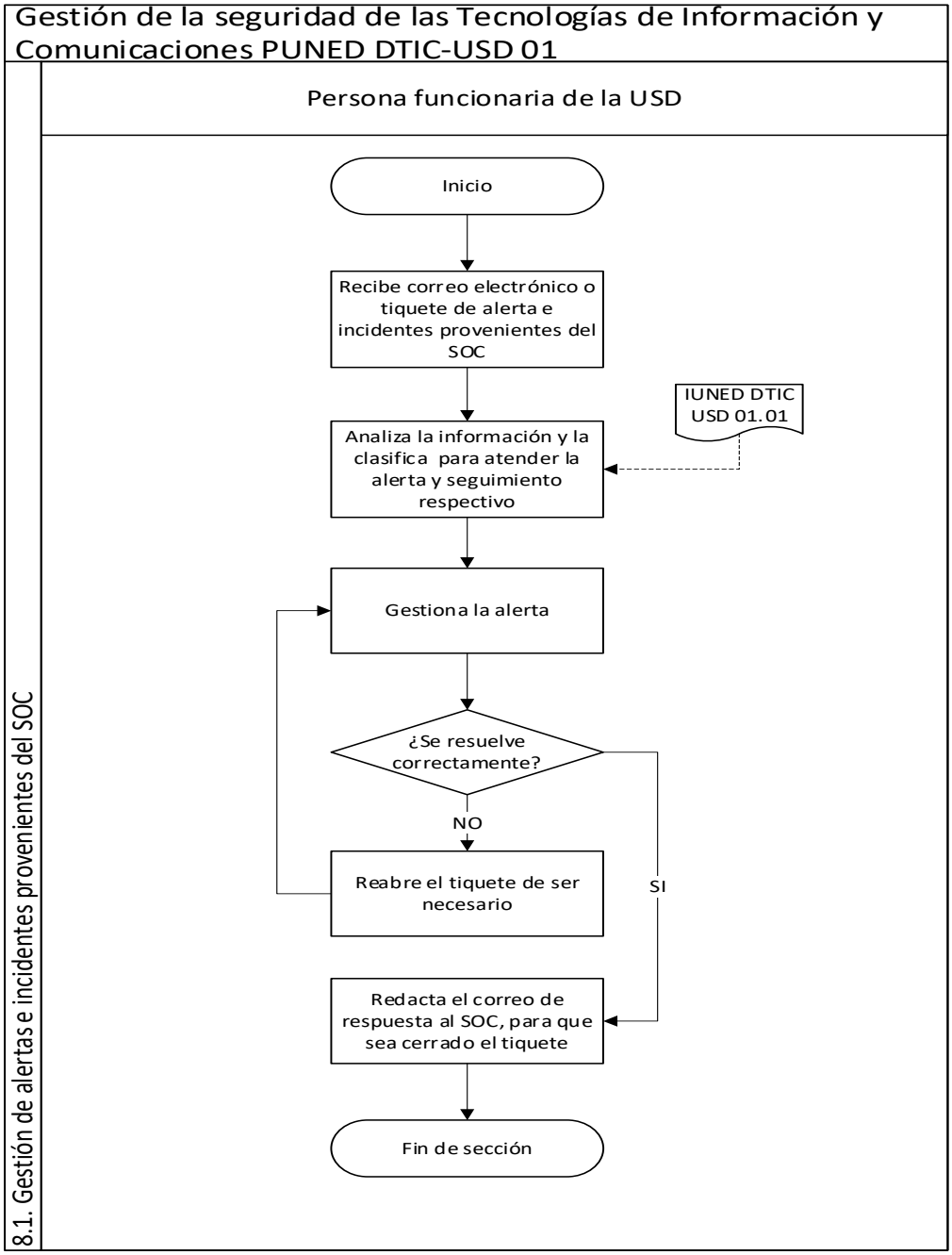
10. Control de Cambios

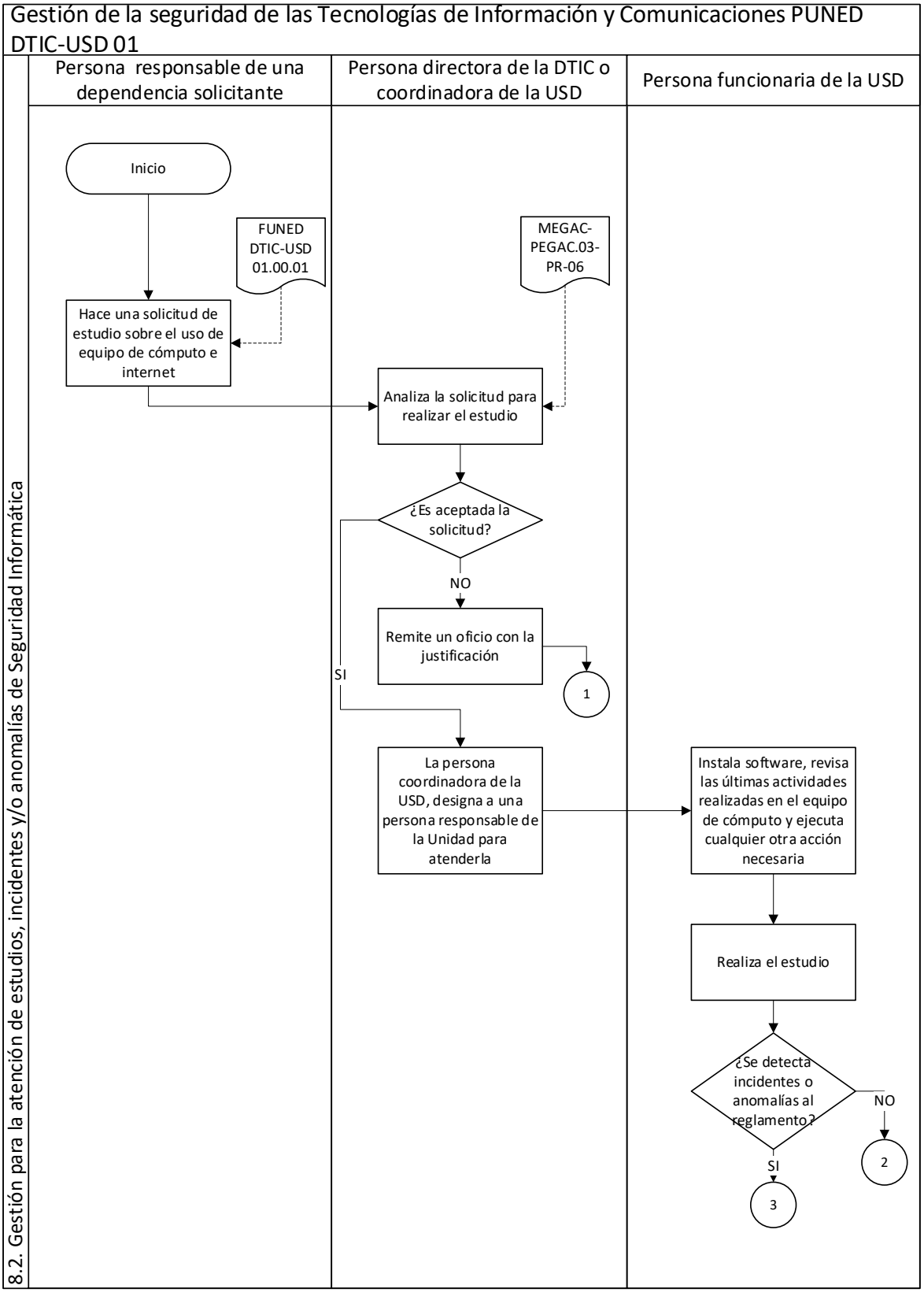
Información versión anterior	Detalle de la Modificación Realizada

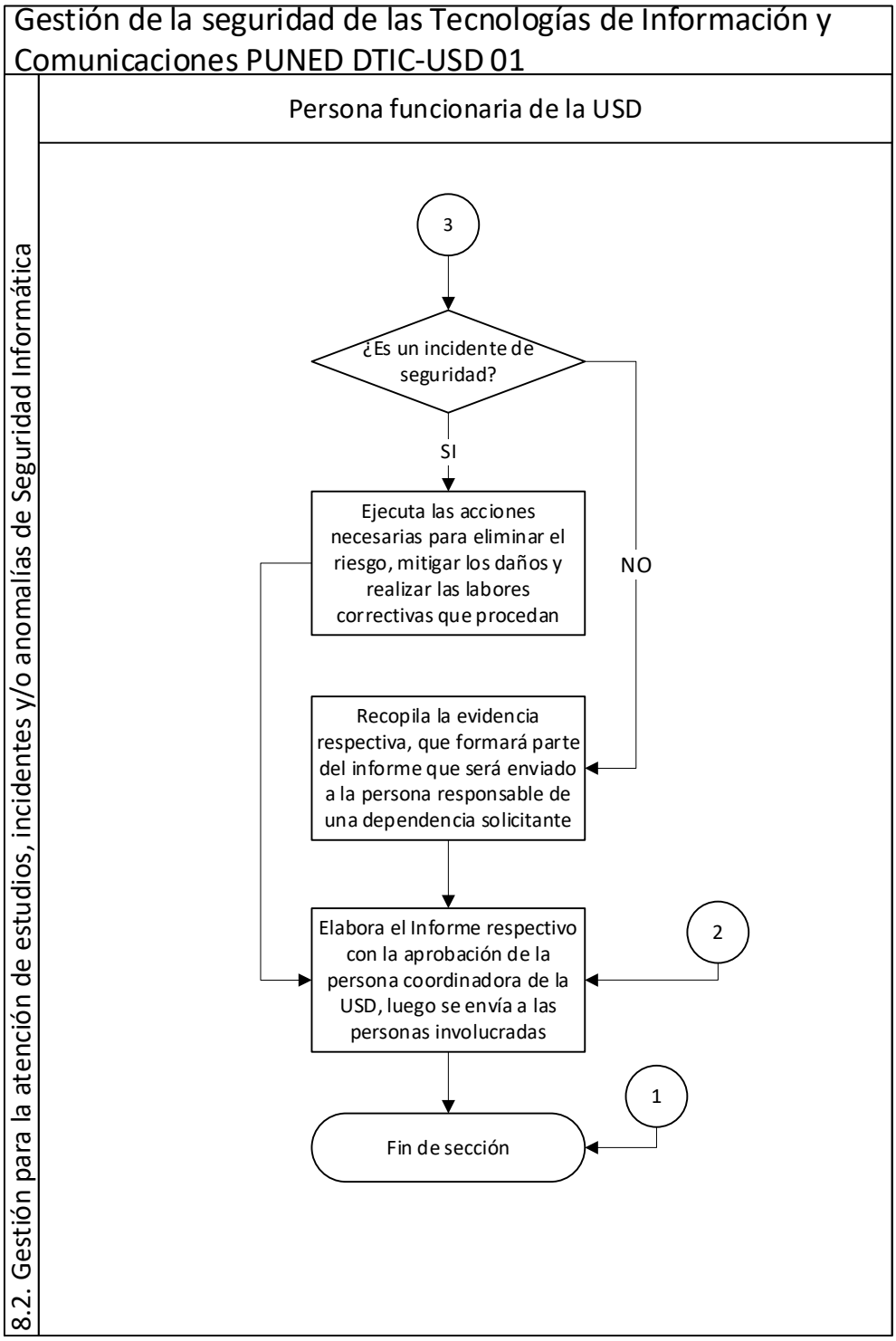
Fin del Procedimiento.

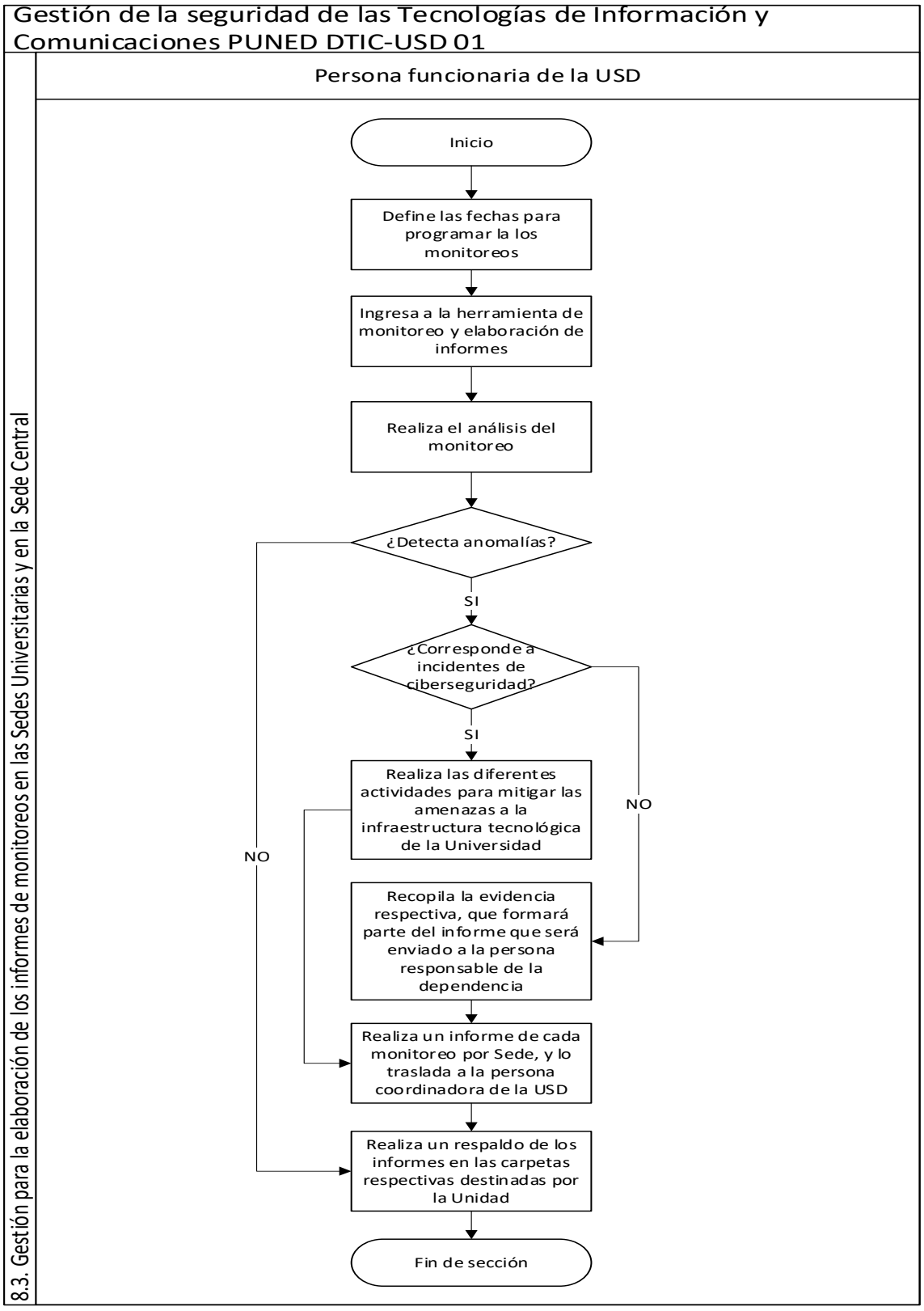
11. Anexos

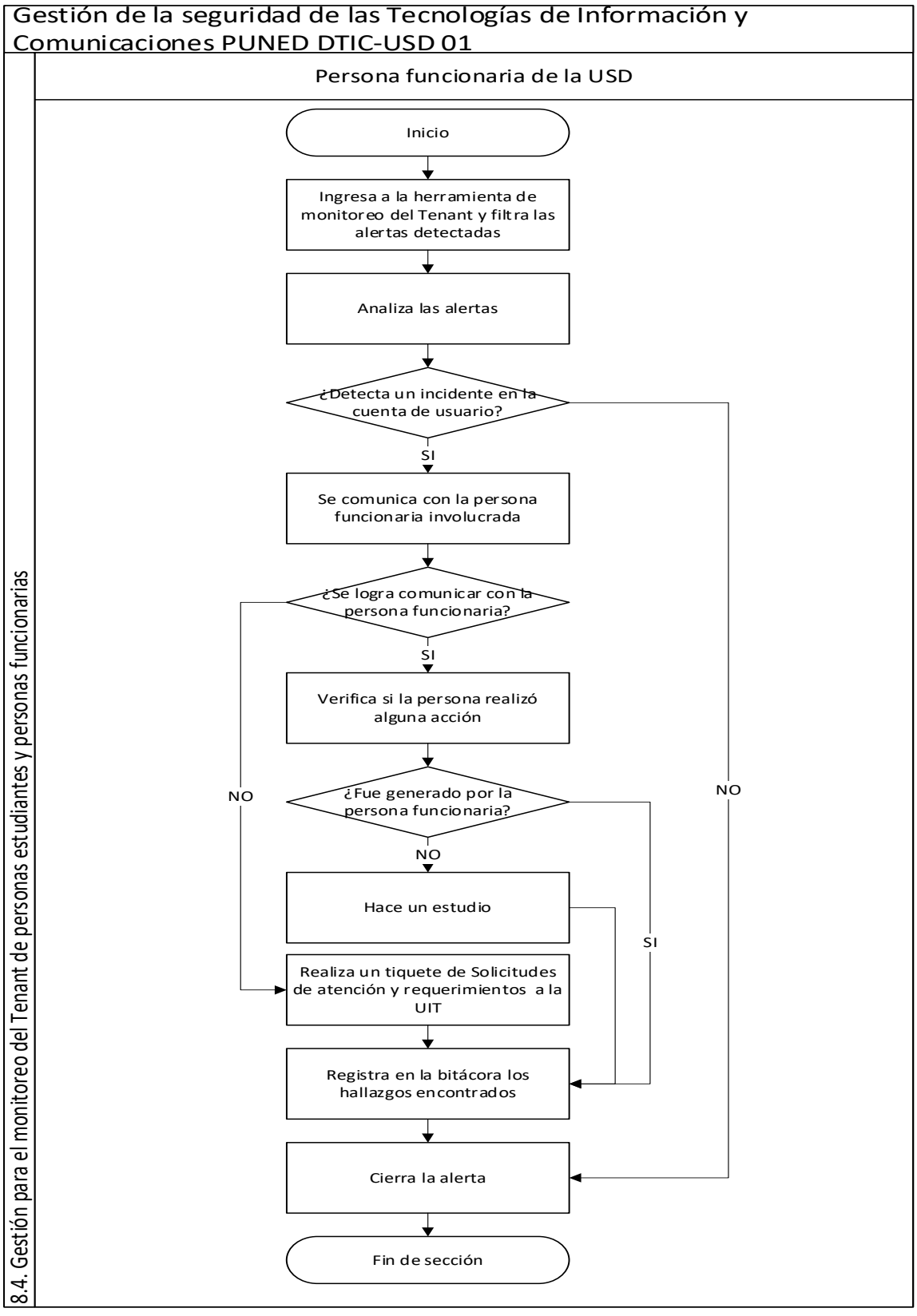
Anexo 1 Diagrama de Flujo.

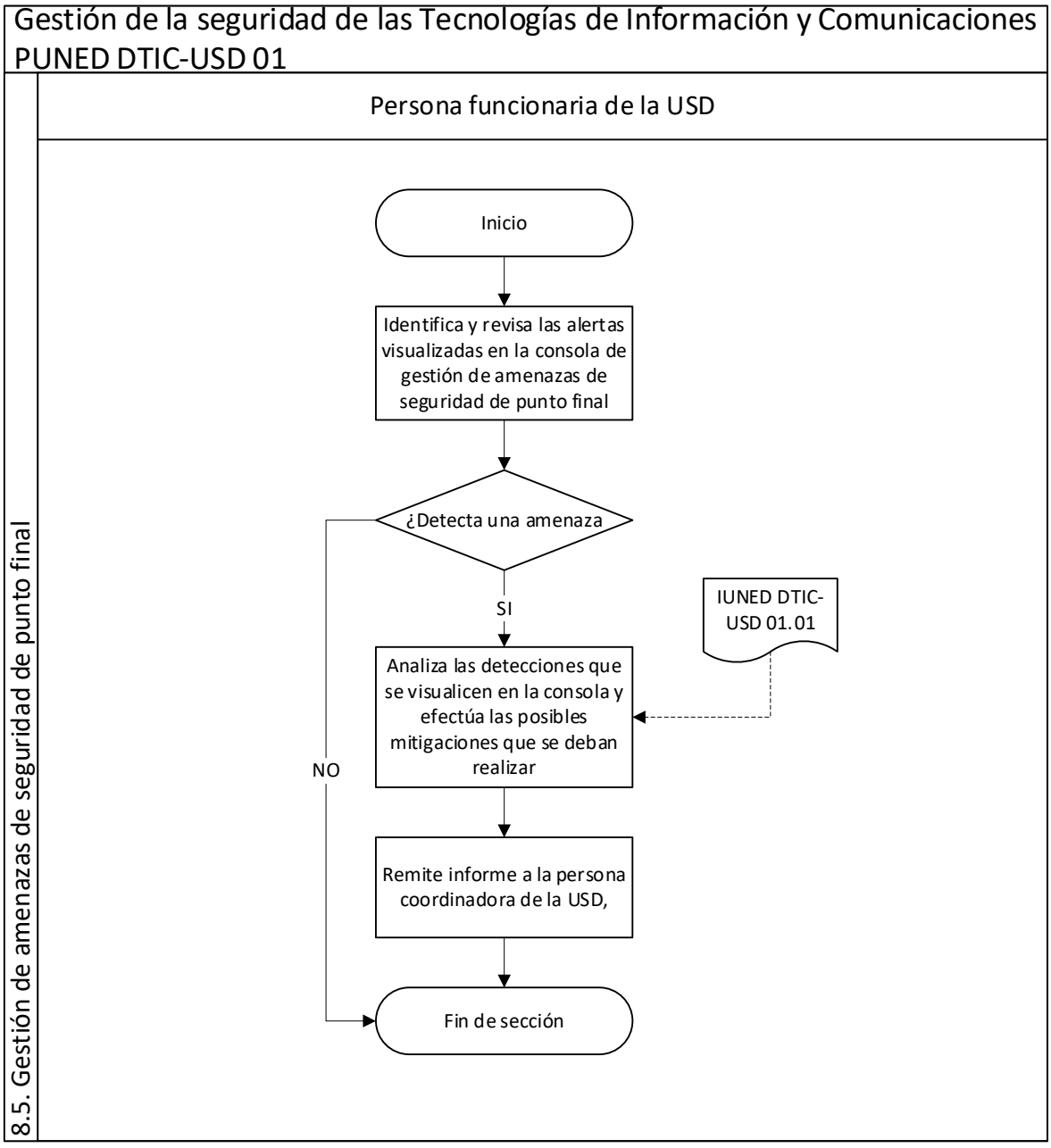


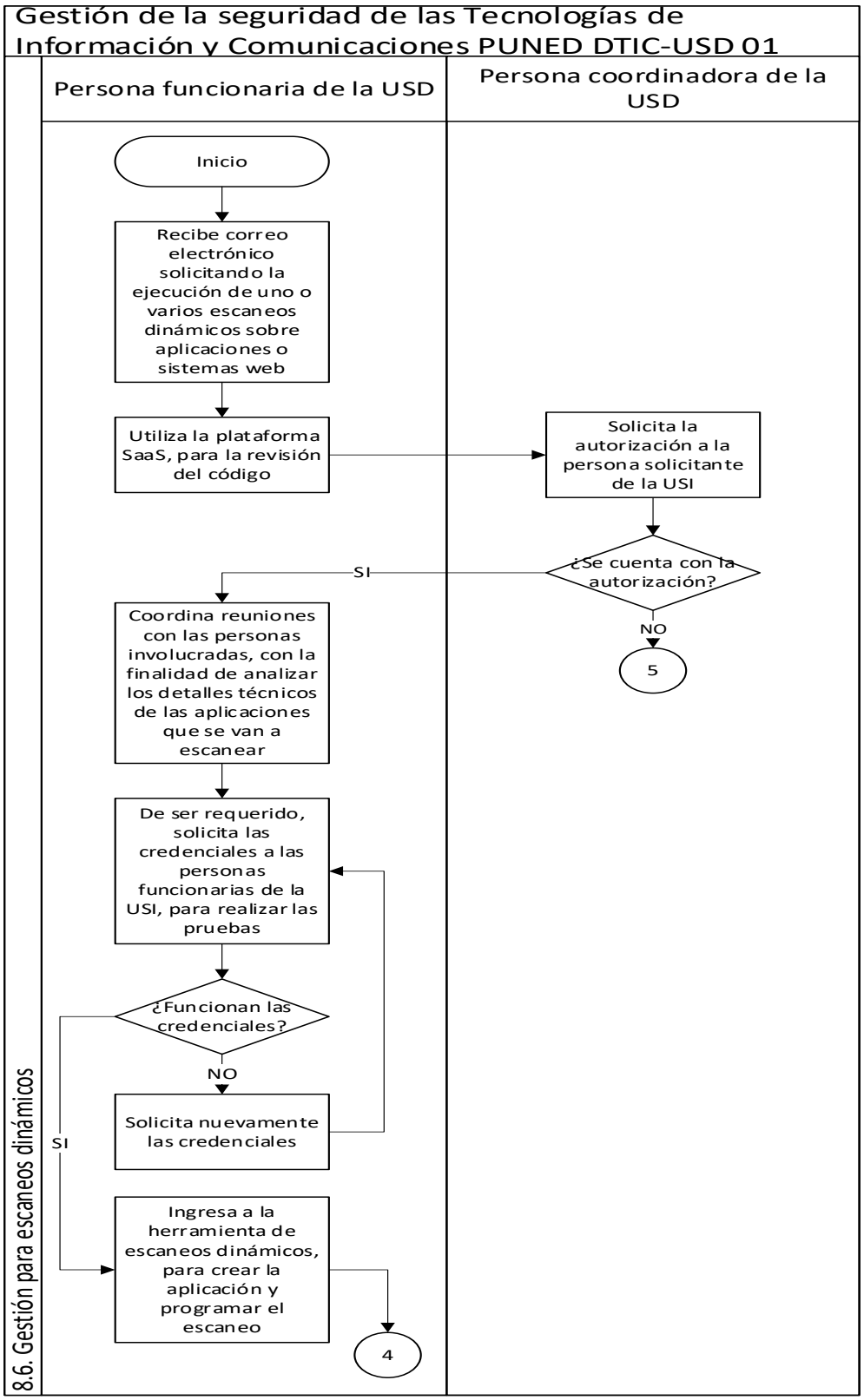

Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
8.2. Gestión para la atención de estudios, incidentes y/o anomalías de Seguridad Informática
Persona responsable de una dependencia solicitante
Persona directora de la DTIC o coordinadora de la USD
Persona funcionaria de la USD
Inicio
FUNED DTIC-USD 01.00.01
MEGAC-PEGAC.03-PR-06
Hace una solicitud de estudio sobre el uso de equipo de cómputo e internet
Analiza la solicitud para realizar el estudio
¿Es aceptada la solicitud?
NO
SI
Remite un oficio con la justificación
1
La persona coordinadora de la USD, designa a una persona responsable de la Unidad para atenderla
Instala software, revisa las últimas actividades realizadas en el equipo de cómputo y ejecuta cualquier otra acción necesaria
Realiza el estudio
¿Se detecta incidentes o anomalías al reglamento?
NO
SI
2
3

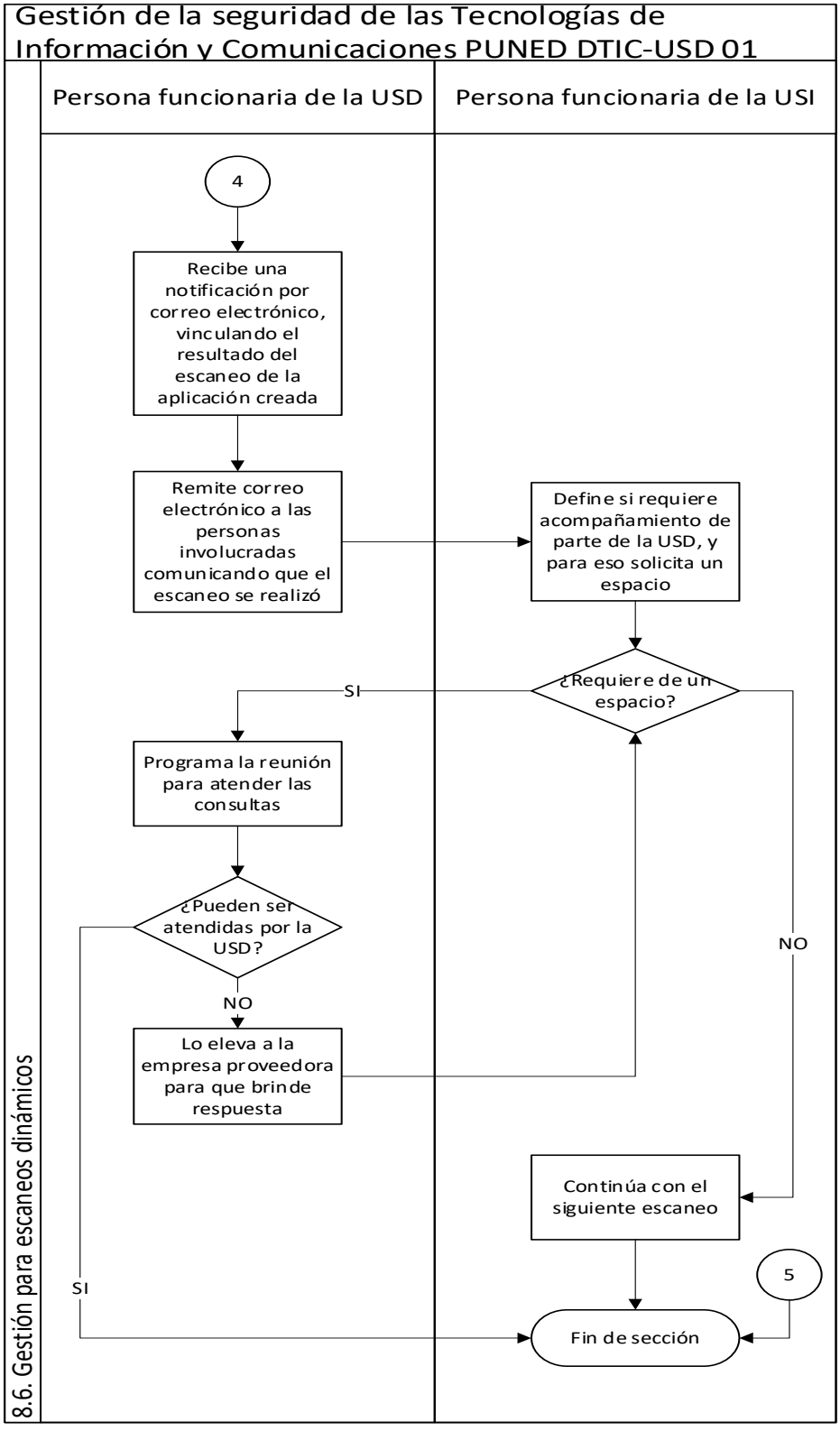

Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
8.2. Gestión para la atención de estudios, incidentes y/o anomalías de Seguridad Informática
Persona funcionaria de la USD
3
¿Es un incidente de seguridad?
SI
NO
Ejecuta las acciones necesarias para eliminar el riesgo, mitigar los daños y realizar las labores correctivas que procedan
Recopila la evidencia respectiva, que formará parte del informe que será enviado a la persona responsable de una dependencia solicitante
Elabora el Informe respectivo con la aprobación de la persona coordinadora de la USD, luego se envía a las personas involucradas
2
1
Fin de sección

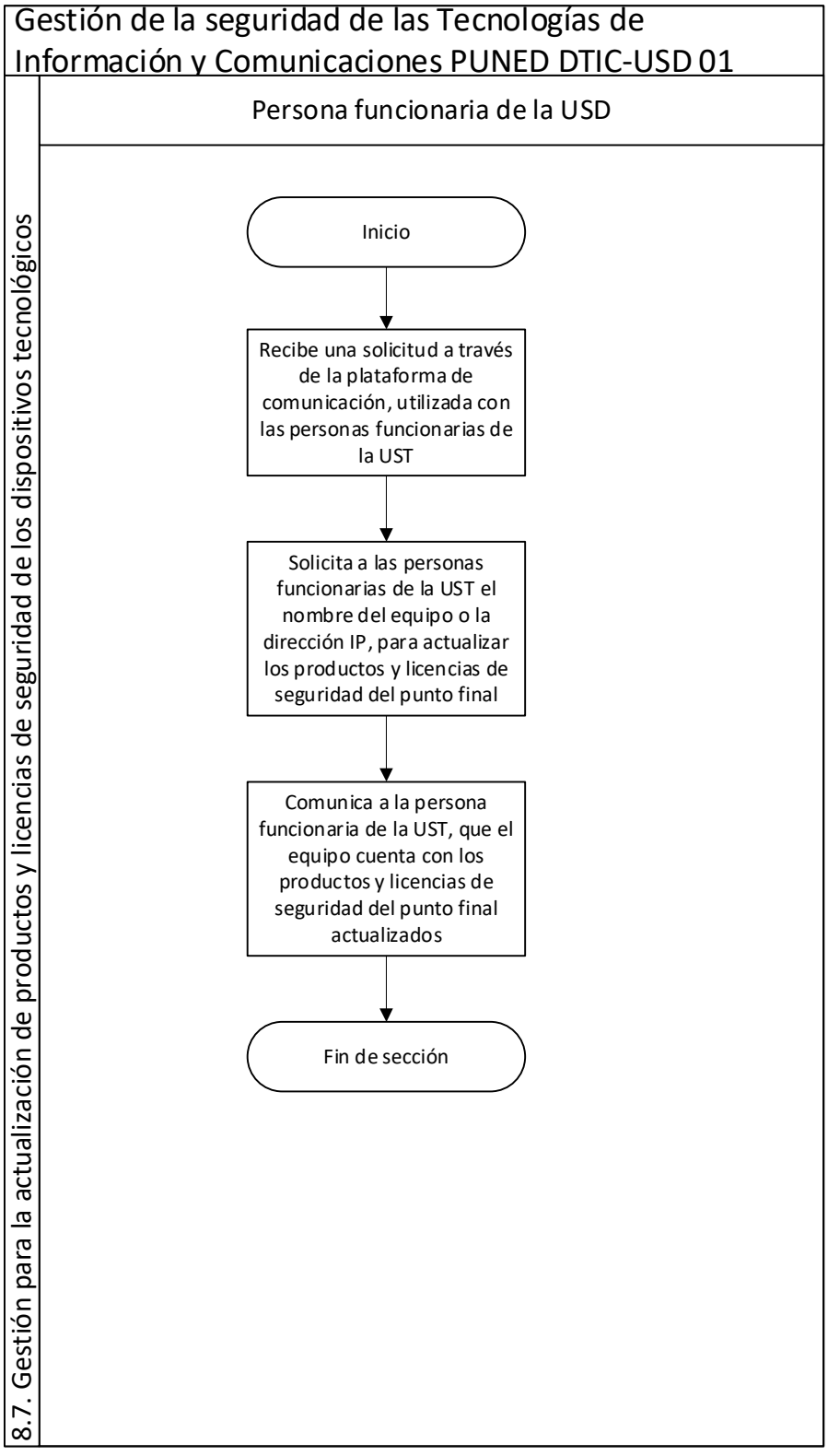

Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
8.3. Gestión para la elaboración de los informes de monitoreos en las Sedes Universitarias y en la Sede Central
Persona funcionaria de la USD
Inicio
Define las fechas para programar la los monitoreos
Ingresa a la herramienta de monitoreo y elaboración de informes
Realiza el análisis del monitoreo
¿Detecta anomalías?
SI
NO
¿Corresponde a incidentes de ciberseguridad?
SI
NO
Realiza las diferentes actividades para mitigar las amenazas a la infraestructura tecnológica de la Universidad
Recopila la evidencia respectiva, que formará parte del informe que será enviado a la persona responsable de la dependencia
Realiza un informe de cada monitoreo por Sede, y lo traslada a la persona coordinadora de la USD
Realiza un respaldo de los informes en las carpetas respectivas destinadas por la Unidad
Fin de sección

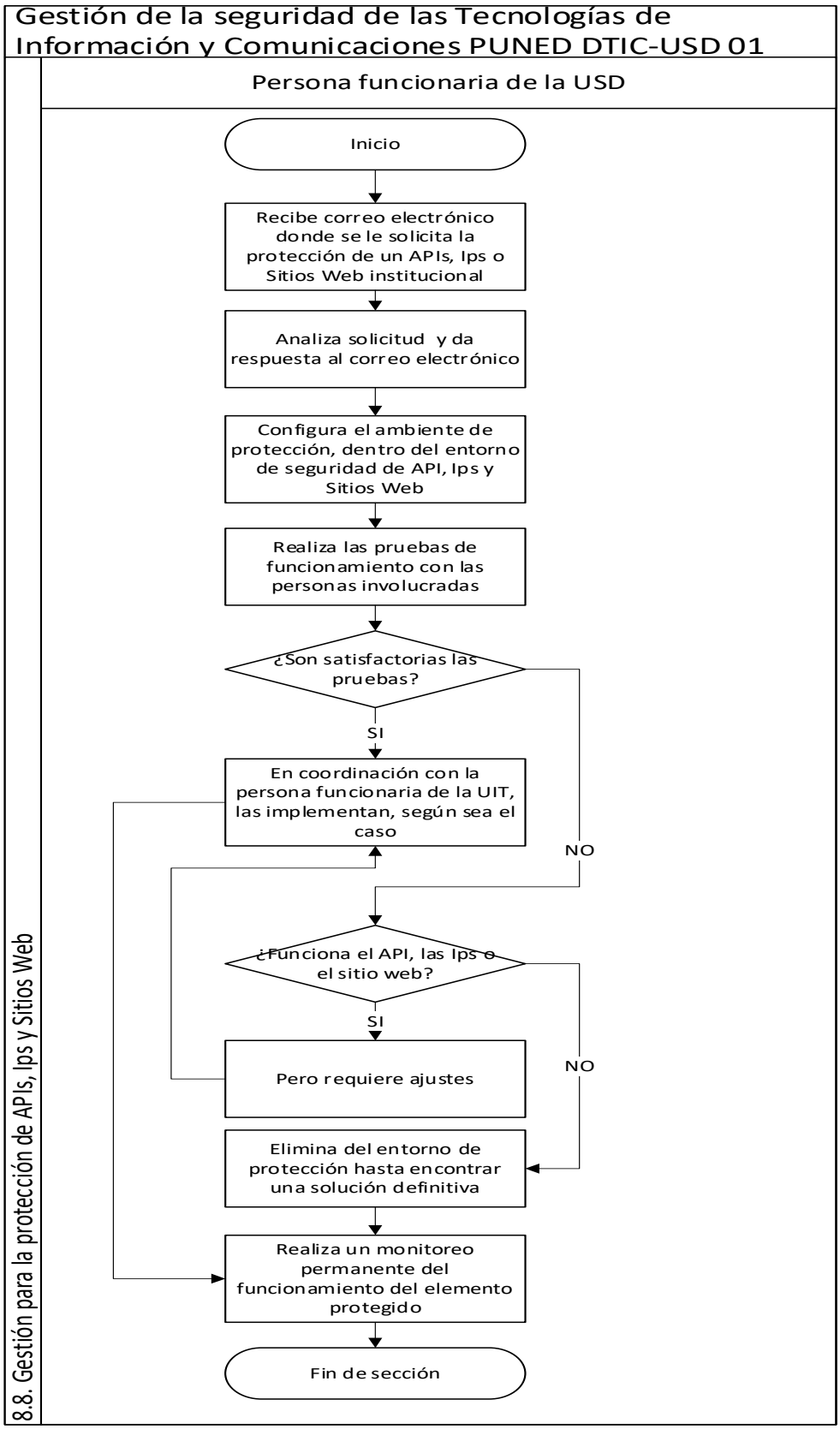

Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
8.4. Gestión para el monitoreo del Tenant de personas estudiantes y personas funcionarias
Persona funcionaria de la USD
Inicio
Ingresa a la herramienta de monitoreo del Tenant y filtra las alertas detectadas
Analiza las alertas
¿Detecta un incidente en la cuenta de usuario?
SI
NO
Se comunica con la persona funcionaria involucrada
¿Se logra comunicar con la persona funcionaria?
SI
NO
Verifica si la persona realizó alguna acción
¿Fue generado por la persona funcionaria?
SI
NO
Hace un estudio
Realiza un tiquete de Solicitudes de atención y requerimientos a la UIT
Registra en la bitácora los hallazgos encontrados
Cierra la alerta
Fin de sección

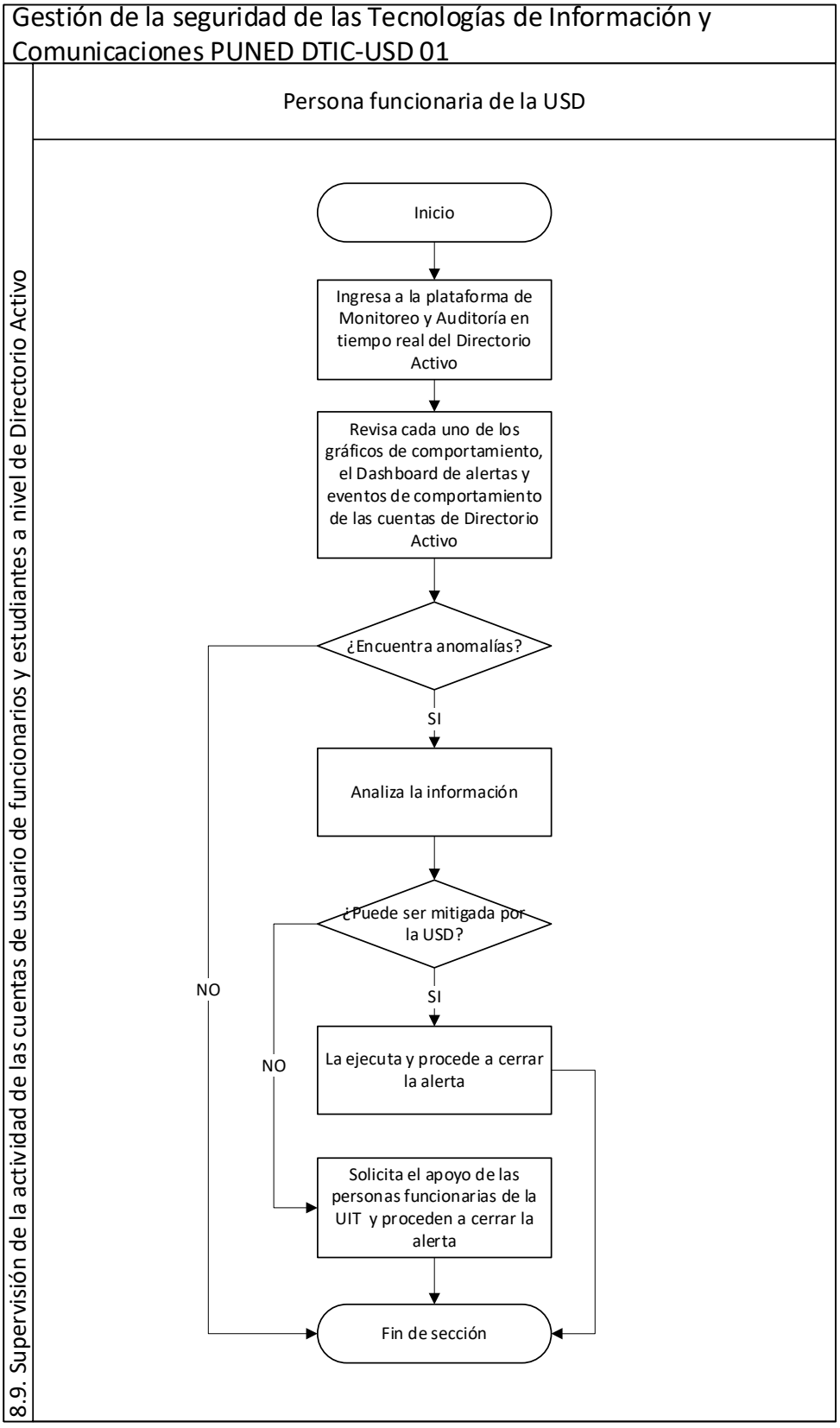

Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
8.5. Gestión de amenazas de seguridad de punto final
Persona funcionaria de la USD
Inicio
Identifica y revisa las alertas visualizadas en la consola de gestión de amenazas de seguridad de punto final
¿Detecta una amenaza
SI
NO
IUNED DTIC-USD 01.01
Analiza las detecciones que se visualicen en la consola y efectúa las posibles mitigaciones que se deban realizar
Remite informe a la persona coordinadora de la USD,
Fin de sección


Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
Persona funcionaria de la USD
Persona coordinadora de la USD
8.6. Gestión para escaneos dinámicos
Inicio
Recibe correo electrónico solicitando la ejecución de uno o varios escaneos dinámicos sobre aplicaciones o sistemas web
Utiliza la plataforma SaaS, para la revisión del código
Solicita la autorización a la persona solicitante de la USI
¿Se cuenta con la autorización?
SI
NO
5
Coordina reuniones con las personas involucradas, con la finalidad de analizar los detalles técnicos de las aplicaciones que se van a escanear
De ser requerido, solicita las credenciales a las personas funcionarias de la USI, para realizar las pruebas
¿Funcionan las credenciales?
NO
SI
Solicita nuevamente las credenciales
Ingresa a la herramienta de escaneos dinámicos, para crear la aplicación y programar el escaneo
4


Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
Persona funcionaria de la USD
Persona funcionaria de la USI
8.6. Gestión para escaneos dinámicos
4
Recibe una notificación por correo electrónico, vinculando el resultado del escaneo de la aplicación creada
Remite correo electrónico a las personas involucradas comunicando que el escaneo se realizó
Define si requiere acompañamiento de parte de la USD, y para eso solicita un espacio
¿Requiere de un espacio?
SI
NO
Programa la reunión para atender las consultas
¿Pueden ser atendidas por la USD?
NO
SI
Lo eleva a la empresa proveedora para que brinde respuesta
Continúa con el siguiente escaneo
5
Fin de sección


Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
8.7. Gestión para la actualización de productos y licencias de seguridad de los dispositivos tecnológicos
Persona funcionaria de la USD
Inicio
Recibe una solicitud a través de la plataforma de comunicación, utilizada con las personas funcionarias de la UST
Solicita a las personas funcionarias de la UST el nombre del equipo o la dirección IP, para actualizar los productos y licencias de seguridad del punto final
Comunica a la persona funcionaria de la UST, que el equipo cuenta con los productos y licencias de seguridad del punto final actualizados
Fin de sección


Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
Persona funcionaria de la USD
8.8. Gestión para la protección de APIs, Ips y Sitios Web
Inicio
Recibe correo electrónico donde se le solicita la protección de un APIs, Ips o Sitios Web institucional
Analiza solicitud y da respuesta al correo electrónico
Configura el ambiente de protección, dentro del entorno de seguridad de API, Ips y Sitios Web
Realiza las pruebas de funcionamiento con las personas involucradas
¿Son satisfactorias las pruebas?
SI
NO
En coordinación con la persona funcionaria de la UIT, las implementan, según sea el caso
¿Funciona el API, las Ips o el sitio web?
SI
NO
Pero requiere ajustes
Elimina del entorno de protección hasta encontrar una solución definitiva
Realiza un monitoreo permanente del funcionamiento del elemento protegido
Fin de sección


Gestión de la seguridad de las Tecnologías de Información y Comunicaciones PUNED DTIC-USD 01
8.9. Supervisión de la actividad de las cuentas de usuario de funcionarios y estudiantes a nivel de Directorio Activo
Persona funcionaria de la USD
Inicio
Ingresa a la plataforma de Monitoreo y Auditoría en tiempo real del Directorio Activo
Revisa cada uno de los gráficos de comportamiento, el Dashboard de alertas y eventos de comportamiento de las cuentas de Directorio Activo
¿Encuentra anomalías?
SI
NO
Analiza la información
¿Puede ser mitigada por la USD?
SI
NO
La ejecuta y procede a cerrar la alerta
Solicita el apoyo de las personas funcionarias de la UIT y proceden a cerrar la alerta
Fin de sección

Anexo 2. Actividades de monitoreo.

En la herramienta de monitoreo y elaboración de informes, en el apartado de Reportes se ingresa a la opción de los monitoreos mensuales, posteriormente se accede a la plantilla del reporte en la pestaña de ajustes, se ingresa el nombre del informe a realizar, se establecen las fechas según la planificación anual de la USD, se selecciona el dispositivo donde se va a ejecutar el monitoreo y se aplican los cambios.

- En la pestaña de ver reporte se ejecuta el mismo.
- En el apartado de Reportes en la sección de Generar Reportes se muestran los reportes generados.
- Una vez generado el reporte en formato PDF, el mismo es descargado y almacenado en la carpeta de monitoreo destinada para dicho fin.
- Se programa el siguiente reporte.
- Al obtener los 5 reportes, se procede con la elaboración del informe del monitoreo correspondiente el cual es almacenado en la carpeta destinada para dicho fin.