Manual de Normas y Procedimientos
POLÍTICAS DE SEGURIDAD LÓGICA Y FÍSICA ME- DS-DTI-MNP-PMR-10 Versión 01

Aprobado por	Cargo	Fecha	Firma y sello
Ing. Roberto Antonio Malouf Morales	Ministro de Economía	14/06/2021	ROBERTO ANTONIO MALOUF MORALES MINISTRO DE ECONOMÍA MINISTERIO DE ECONOMÍA DESPACHO SUPERIOR REPÚBLICA DE GUATEMALA, C.A.

Actualizado y revisado por	Cargo	Fecha	Firma y sello
Marco Antonio Hernandez	Director de Tecnologías de la Información	18-05-2021	Marco Antonio Hernández Director Dirección de Tecnologías de la Información Ministerio de Economía

Documentado por	Cargo	Fecha	Firma y sello
Lic. Mynor Zúñiga	Director de Desarrollo Institucional	20/04/2021	Lic. Mynor Zúñiga Director de Desarrollo Institucional Ministerio de Economía

Vigente a partir de:	16/06/2021

ÍNDICE

1. OBJETIVO:

El presente manual de normas y procedimientos define las directrices para la correcta protección a nivel lógico y físico de los recursos resguardados en el centro de datos del edificio central del Ministerio de Economía, con la finalidad de prevenir la pérdida total o parcial de la información contenida en los mismos.

2. ALCANCE:

El presente manual de normas y procedimientos debe ser cumplido para llevar a cabo la protección exclusivamente de los recursos informáticos resguardados en el centro de datos del edificio central del Ministerio de Economía. Estas políticas no aplican para los centros de datos que no administra directamente la Dirección de Tecnologías de la Información, aunque se recomienda su uso en dichos casos.

3. DEFINICIONES:

3.1. Dispositivo biométrico:

Es usado en sistemas computarizados de seguridad, principalmente para identificar atributos físicos como rasgos faciales, patrones oculares, huellas digitales, la voz y la escritura.

3.2. Firewall:

También llamado cortafuegos, es un equipo y/o sistema cuya función es prevenir y proteger la red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red.

3.3. VLAN, Virtual Local Area Network:

Una VLAN, acrónimo de virtual LAN (red de área local virtual) es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

3.4. Switch de acceso:

Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3.

3.5. Departamento de seguridad:

Unidad designada para la seguridad física perimetral del del Ministerio de Economía.

4. BASE LEGAL, DOCUMENTOS O DATOS RELACIONADOS:

Base legal, documentos o datos relacionados	
Numero o código del documento o dato	**Descripción del documento o dato**
Acuerdo Gubernativo No. 211-2019	Reglamento Orgánico Interno del Ministerio de Economía.
Acuerdo Ministerial 762-2019	Estructura Orgánica Interna Complementaria a la estructura establecida en el Reglamento Orgánico Interno del Ministerio de Economía.

5. NORMAS:

5.1. Las personas con acceso a la Dirección de Tecnologías de la Información son los empleados debidamente contratados por la Dirección de Recursos Humanos del Ministerio de Economía en cualquiera de los renglones establecidos por la Ley de Compras y Contrataciones del Estado;

5.2. La persona encargada para la administración de los registros de huella en los dispositivos biométricos es el Coordinador de operaciones, éste llevará un registro el cual le será enviado vía correo electrónico debidamente actualizado al director de la Dirección de Tecnologías de la Información cada vez que se realice una actualización en los registros de huella y/o código de acceso;

5.3. Se llevará un control físico ubicado en el ingreso de las oficinas que componen la Dirección de Tecnologías de la Información, a nivel escrito que requiere los datos y la firma de las personas externas a la Dirección de Tecnologías de la Información que ingresen a las instalaciones de esta Dirección en el Edificio central, de igual forma se llevará un control similar para el acceso al centro de datos, en el ingreso a éste, que requiere los datos y la firma de las personas externas al departamento de Operaciones y Seguridad informática. Las hojas de estos controles deberán ser escaneadas cada mes, para su resguardo digital, así como archivadas para contar con un control físico histórico de las visitas efectuadas a la Dirección de Tecnologías de la Información, así como al centro de datos ubicado dentro de ésta;

5.4. Se deberá revisar los registros del firewall para evaluar los eventos registrados, este proceso deberá llevarse a cabo en la primera hora laboral de cada día de lunes a viernes, es necesario que por lo menos cada tres (3) meses se evalúen las políticas de seguridad para implementar mejoras y validar su buen funcionamiento, el tiempo puede ser más corto sin embargo debido a que afectan la operación general, es mejor distanciar este tipo de procedimientos, en caso sea necesario aplicar cambios. En casos de extrema necesidad, es factible realizar cambios sin previa calendarización, pero con el visto bueno del Director de Tecnologías de la Información;

5.4.1. En caso de existir anomalías, éstas deberán ser notificadas al Director de Tecnologías de la Información, una vez se cuente con su visto bueno para subsanarlas se procederá de inmediato a aplicar la debida acción correctiva para recuperar la funcionalidad optima y mantener la operación sin contratiempos. Es necesario llevar una bitácora de los incidentes, así como el detalle de la solución aplicada para futuros casos;

5.5. Continuidad de la operación:

5.5.1. Para responder ante una emergencia de manera adecuada y lograr un mínimo impacto en los servicios que presta la institución, se debe contar con el apoyo directo del Departamento de seguridad, perteneciente a la Dirección Administrativa, ya que conforma el primer anillo de seguridad para el acceso al edifico central, por lo que su importancia es relevante respecto a los sucesos que se registren a nivel físico dentro de las instalaciones del edificio central;

5.6. Dispositivos externos de seguridad:

5.6.1. Se deberá contar con cámaras de seguridad, administradas y monitoreadas por el Departamento de seguridad, perteneciente a la Dirección Administrativa.

5.6.2. Toda la información recabada por las cámaras de seguridad deberá estar almacenada por un período no menor a un (1) mes en el dispositivo de grabación desde donde se administran y consolidan los canales de vídeo dados de alta por cada cámara de seguridad.

5.7. Los funcionarios y empleados que intervienen en el numeral "7. PROCEDIMIENTO" del presente Manual de normas y procedimientos, son corresponsables del contenido y cumplimiento del mismo, según corresponda;

5.8. Situaciones no previstas en el presente manual de normas y procedimientos, serán resueltas por el Director de Tecnologías de la Información.

6. RESPONSABILIDADES:

6.1. Despacho Superior es responsable de:

6.1.1. Aprobar, firmar y sellar el presente manual de normas y procedimientos.

6.2. Director de Tecnologías de la Información es responsable de:

6.2.1. Revisar, firmar y sellar el presente manual de normas y procedimientos, garantizando que su contenido responde al proceso que norma y documenta el mismo;

6.2.2. Actualizar o delegar y supervisar la actualización oportuna del presente manual de normas y procedimientos, en coordinación con la Dirección de Desarrollo Institucional;

6.2.3. Cumplir y supervisar en lo que corresponde, el cumplimiento del presente manual de normas y procedimientos;

6.2.4. Otras responsabilidades que correspondan, establecidas en el numeral 7: "PROCEDIMIENTO" del presente manual.

6.3. Técnico asignado para elaborar o actualizar el presente manual de normas y procedimientos es responsable de:

6.3.1. Actualizar oportunamente el presente manual de normas y procedimientos, por instrucciones del Director de Tecnologías de la Información y en coordinación con la Dirección de Desarrollo Institucional;

6.3.2. Firmar y sellar el presente manual de normas y procedimientos, garantizando que su contenido responde al proceso que norma y documente el mismo;

6.3.3. Cumplir en lo que corresponda con el presente manual de normas y procedimientos;

6.3.4. Otras responsabilidades que correspondan, establecidas en el numeral "7. PROCEDIMIENTO" del presente manual.

7. PROCEDIMIENTO:

7.1. Gestión del acceso a la Dirección de Tecnologías de la Información

Responsable	Actividades	Tiempo
Secretaria del Órgano de Tecnologías de la Información	• Facilita la hoja del formulario, así como un bolígrafo al visitante o visitantes, al momento de su ingreso a la Dirección de Tecnologías de la Información.	1 minuto
Visitante	• Llena formulario identificándose con Nombre completo, DPI, Empresa a la que representa, persona a la que visita y la razón de la visita, hora de ingreso; • Firma de acuerdo para validar los datos escritos.	5 minutos
Secretaria de dirección de Tecnologías de la Información	• Anuncia la visita a la persona que identifican a su ingreso; • Conduce al visitante al lugar de la persona que visitan; El tiempo puede variar, ya que dependerá de la disponibilidad del empleado de la Dirección de Tecnologías de la Información que recibe la visita.	5 minutos
Técnico de la Órgano de Tecnologías de la Información	• Recibe y atiende a la visita; • Es responsable de acompañar a la visita a la puerta de salida de la Dirección de Tecnologías de la Información y corroborar que no extienda su presencia dentro de la Dirección de Tecnologías de la Información. • 60 minutos es el tiempo máximo recomendado para una visita, en algunos casos puede extenderse siempre y cuando haya visto bueno del Director de Tecnologías de la Información.	60 minutos

7.2. Gestión del acceso al centro de datos

Responsable	Actividades	Tiempo
Empleado del Departamento de Operaciones y Seguridad Informática	• Recibe la visita; • Conduce a la visita al centro de datos; • Facilita el formulario de ingreso al centro de datos a la visita.	5 minutos
Visitante	• Llena formulario identificándose con Nombre completo, DPI, Empresa a la que representa, razón del ingreso al centro de datos, hora de ingreso; • Firma de acuerdo para validar los datos escritos.	5 minutos
Empleado del Departamento de Operaciones y Seguridad Informática	• Coloca su huella en el dispositivo biométrico para habilitar el acceso al centro de datos; • Permite el acceso a la vista al centro de datos; • Supervisa las labores de la visita;	60 minutos

Responsable	Actividades	Tiempo
	En caso necesario apoya las labores de la visita cuando sea necesario; 60 minutos es el tiempo máximo recomendado para una visita, en algunos casos puede extenderse siempre y cuando haya visto bueno del Director de Tecnologías de la información. • Finalizado el objetivo de la visita, facilita el formulario de acceso nuevamente a la visita para que escriba la hora de salida; • Es responsable de acompañar a la visita a la puerta de salida de la Dirección de Tecnologías de la Información	

7.3. Gestión del firewall

Responsable	Actividades	Tiempo
Coordinador de Operaciones y Seguridad Informática	• Gestiona las credenciales del firewall principal; • Da de alta nuevos usuarios, así como sus perfiles de uso; Tiene la capacidad de delegar la administración y actualización de políticas, con el debido visto bueno del Director de Tecnologías de la Información.	15 minutos
Técnico de Seguridad informática	• Revisa los eventos todos los días de lunes a viernes en la primera hora laboral; • Guarda la entrada en una bitácora que puede llevar en un archivo de Microsoft Excel, anotando lo evaluado y la calidad del servicio del firewall en el momento de la evaluación, identificando la fecha y la hora de la evaluación. • En caso exista una anomalía procede a reportarla, vía correo electrónico, al Coordinador de Operaciones y Seguridad Informática, así como al Director de Tecnologías de la Información.	75 minutos 5 minutos
Coordinador de Operaciones y Seguridad Informática	• Recibe la notificación; • Evalúa el impacto en la operación; • Propone la solución, tiempo estimado, así como la hora y fecha para proceder a resolver el incidente; • Solicita visto bueno para proceder al Director de Tecnologías de la Información, este proceso puede ser verbal, acompañado de un correo electrónico como respaldo documental.	15 - 20 minutos
Director de dirección de Tecnologías de la Información	• Evalúa lo propuesto; • Si es conveniente emite visto bueno para proceder.	5 – 15 minutos

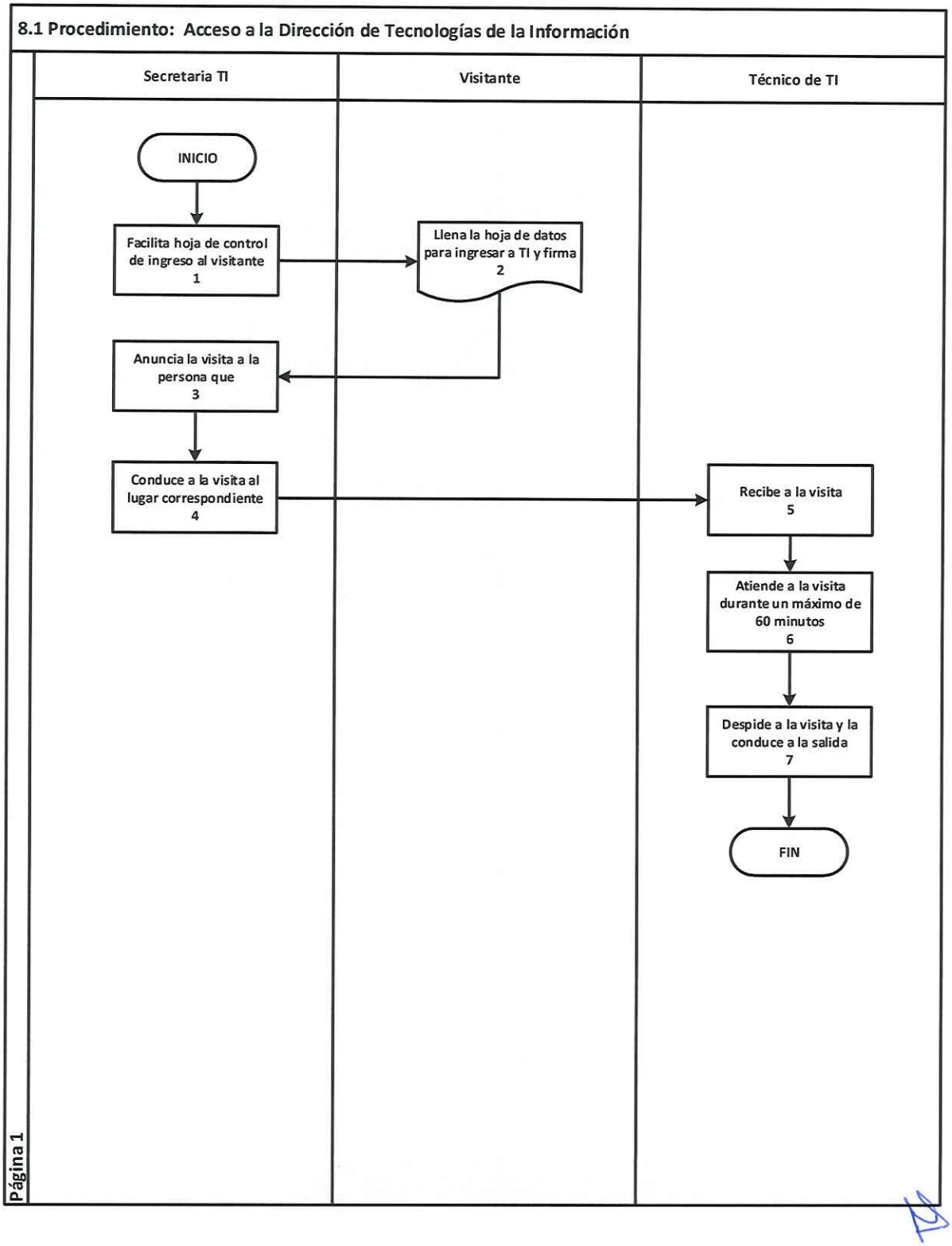
Responsable	Actividades	Tiempo
Coordinador de Operaciones y Seguridad Informática	• Recibe el visto bueno del Director de Tecnologías de la Información; • Da el visto bueno al Técnico de Seguridad informática para que proceda, este proceso puede ser verbal, acompañado de un correo electrónico como respaldo documental.	5 minutos
Técnico de seguridad informática Técnico de Seguridad informática	• Recibe el visto bueno del Coordinador de Operaciones y Seguridad informática; • Procede a implementar la solución; • Documenta lo realizado para futuros usos; 60 minutos es el tiempo estándar para resolver un incidente, incluyendo las pruebas, en algunos casos puede extenderse siempre y cuando haya notificación a Dirección, así como visto bueno del Director de Tecnologías de la información. • Traslada al Coordinador de Operaciones de Seguridad informática, con copia al Director de Tecnologías de la Información.	60 minutos 60 – 180 minutos
Coordinador de Operaciones y Seguridad Informática	• Recibe el proceso y finaliza.	5 minutos

7.4. Gestión de switches de acceso y Access points

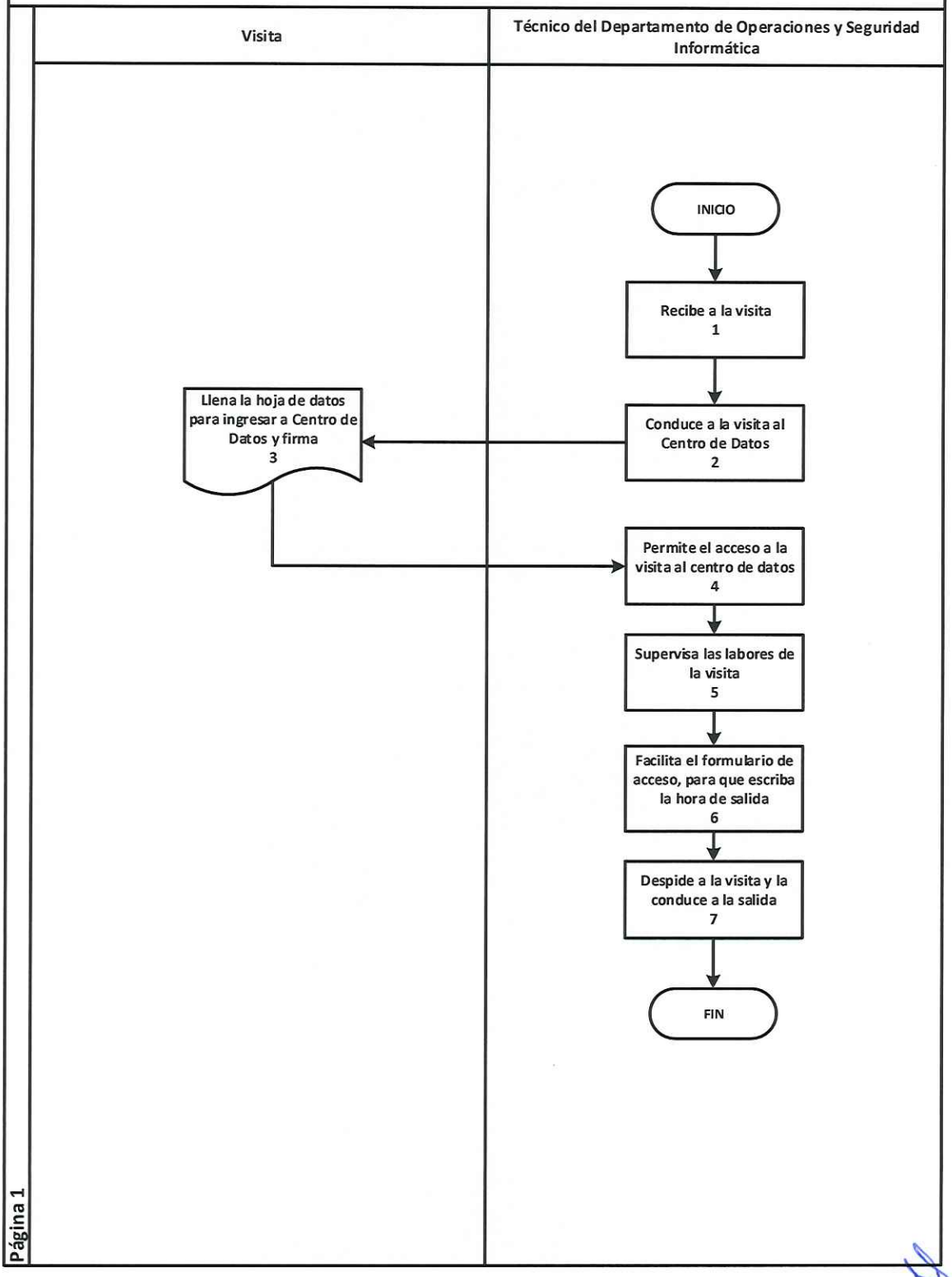
Responsable	Actividades	Tiempo
Técnico de seguridad informática	• Gestiona las credenciales de los switches de acceso y Access points, vLAN y otras configuraciones necesarias para el uso seguro de la red local; • Da de alta nuevas configuraciones de acuerdo con lo requerido por el Director de Tecnologías de la Información o el Coordinador de Operaciones y Seguridad informática; • Revisa semanalmente el estado físico de los switches; • Guarda en una bitácora el estado que presentan los switches el día de la revisión, este proceso se lleva a cabo cada lunes en las primeras horas del día. • En caso exista una anomalía procede a reportarla, vía correo electrónico, al Coordinador de Operaciones y Seguridad Informática, así como al Director de Tecnologías de la Información; • En caso no exista anomalía, informa a Coordinador de Operaciones.	60 - 120 minutos 120 minutos 5 minutos

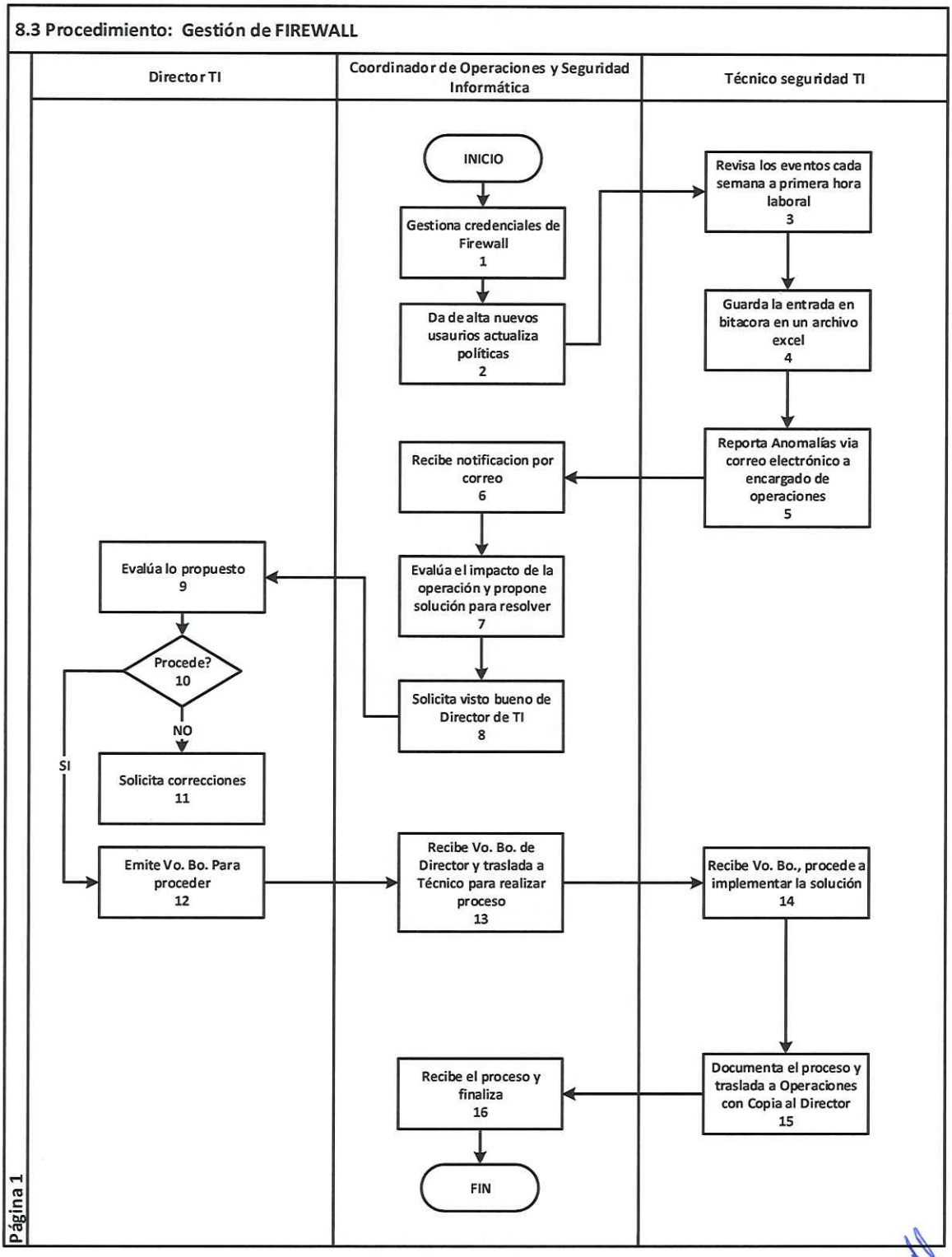
Responsable	Actividades	Tiempo
Coordinador de Operaciones y Seguridad Informática	• Recibe la notificación; • Evalúa el impacto en la operación; • Propone la solución, tiempo estimado, así como la hora y fecha para proceder a resolver el incidente; • Solicita visto bueno para proceder al Director de Tecnologías de la Información, este proceso puede ser verbal, acompañado de un correo electrónico como respaldo documental.	15 - 20 minutos
Director de Tecnologías de la Información	• Recibe la propuesta; • Evalúa la propuesta; • Emite el visto bueno, en caso proceda la propuesta.	24 – 48 horas
Coordinador de Operaciones y Seguridad Informática	• Recibe la propuesta aprobada; • Traslada la propuesta al Técnico de seguridad informática.	15 minutos
Técnico de seguridad informática	• Recibe e implementa la propuesta aprobada; • Documenta el proceso y lo traslada al Coordinador de Operaciones de Seguridad informática, con copia al Director de Tecnologías de la Información.	60 – 180 minutos

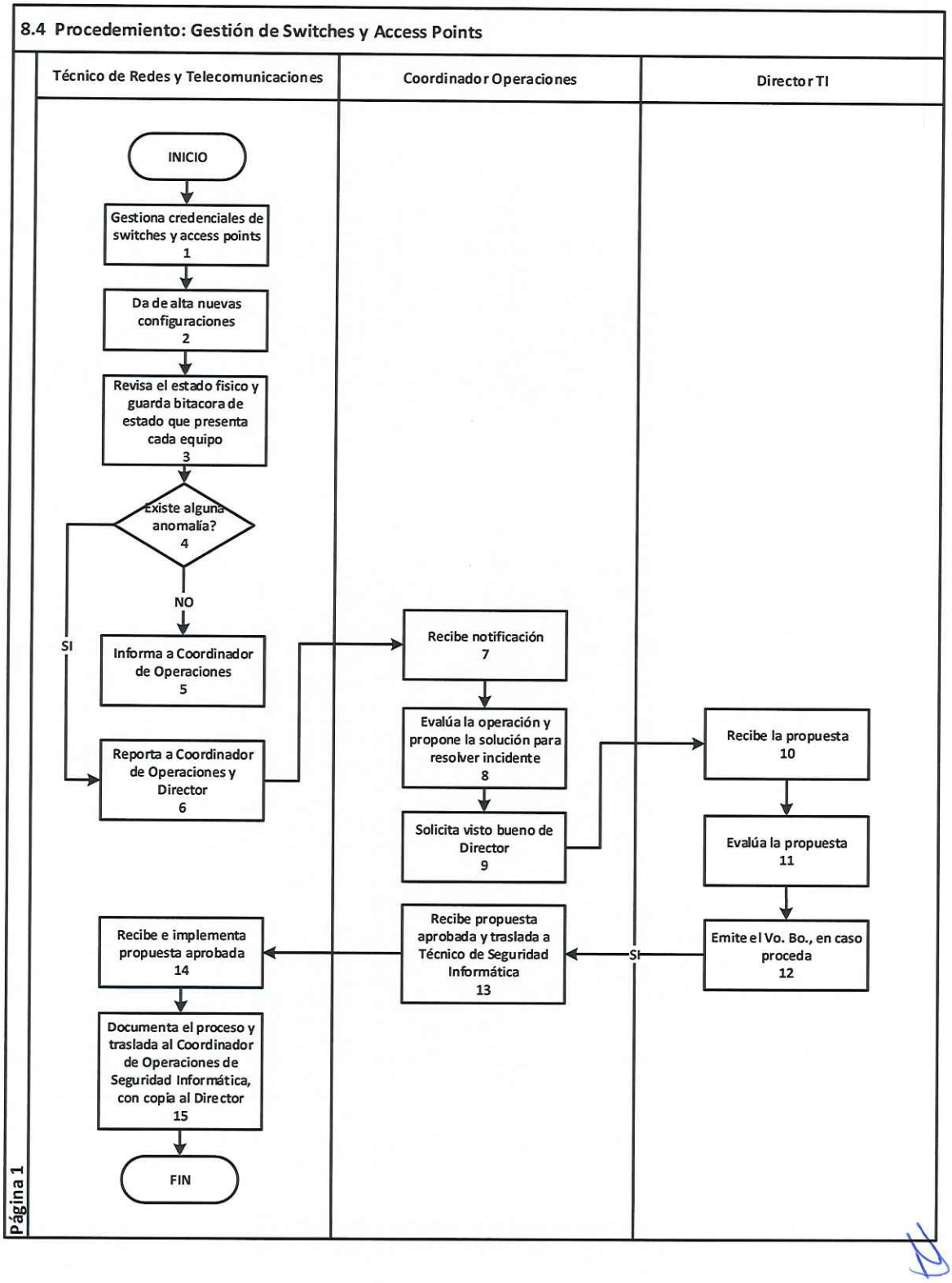
8. FLUJOGRAMAS:



8.2 Procedimiento: Gestión de acceso al Centro de Datos




8.3 Procedimiento: Gestión de FIREWALL
Director TI
Coordinador de Operaciones y Seguridad Informática
Técnico seguridad TI
INICIO
Gestiona credenciales de Firewall 1
Da de alta nuevos usaurios actualiza políticas 2
Revisa los eventos cada semana a primera hora laboral 3
Guarda la entrada en bitacora en un archivo excel 4
Reporta Anomalías via correo electrónico a encargado de operaciones 5
Recibe notificacion por correo 6
Evalúa el impacto de la operación y propone solución para resolver 7
Solicita visto bueno de Director de TI 8
Evalúa lo propuesto 9
Procede? 10
NO
SI
Solicita correcciones 11
Emite Vo. Bo. Para proceder 12
Recibe Vo. Bo. de Director y traslada a Técnico para realizar proceso 13
Recibe Vo. Bo., procede a implementar la solución 14
Documenta el proceso y traslada a Operaciones con Copia al Director 15
Recibe el proceso y finaliza 16
FIN
Página 1


8.4 Procedemiento: Gestión de Switches y Access Points
Técnico de Redes y Telecomunicaciones
Coordinador Operaciones
Director TI
INICIO
Gestiona credenciales de switches y access points 1
Da de alta nuevas configuraciones 2
Revisa el estado fisico y guarda bitacora de estado que presenta cada equipo 3
Existe alguna anomalía? 4
NO
SI
Informa a Coordinador de Operaciones 5
Reporta a Coordinador de Operaciones y Director 6
Recibe notificación 7
Evalúa la operación y propone la solución para resolver incidente 8
Solicita visto bueno de Director 9
Recibe la propuesta 10
Evalúa la propuesta 11
Emite el Vo. Bo., en caso proceda 12
SI
Recibe propuesta aprobada y traslada a Técnico de Seguridad Informática 13
Recibe e implementa propuesta aprobada 14
Documenta el proceso y traslada al Coordinador de Operaciones de Seguridad Informática, con copia al Director 15
FIN
Página 1

9. ANEXOS:

(NO APLICA)