MEDIDAS DE SEGURIDAD EN DATOS PERSONALES

Continum Datacenter

Abril 2020

Contenido

Introducción

Continum Datacenter cumple con los lineamientos de seguridad lógica y física requeridos por el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) implementando controles para el procesamiento, almacenamiento y/ trasmisión de datos de titulares de tarjetas y/o datos confidenciales de autenticación.

Propósito

El propósito del presente documento es exponer las medidas de seguridad utilizadas en el tratamiento de los datos personales en el proyecto PROTEGER.

Alcance

Este documento presenta las medidas de seguridad a nivel administrativo, físico y lógico utilizadas por Continum Datacenter en el tratamiento de los datos personales.

Responsables

En la siguiente tabla se presentan los datos de los encargados del proyecto PROTEGER en Continum Datacenter:

Nombre	Teléfono de oficina	Teléfono Personal	E-mail
Adrian Lachner Castro	83046262	83046262	adrian.lachner@payfacility.com
Alvaro Fernandez	88842906	88842906	alvaro.fernandez@invenio.org
Pedro Vilalta Chavarría	21051303	8788 5543	pedro.villalta@continumcenter.com

*ver cartas adjuntas de aceptación del cargo y responsabilidades inherentes al mismo.

Medidas de seguridad administrativas para el manejo de datos personales.

Continum Datacenter cuenta con políticas para la seguridad y confidencialidad de la información basadas en el estándar PCI DSS para la industria de tarjetas de pago:

- Cada director de unidad debe notificar a los colaboradores sobre el uso correcto de la información, así como cumplir con las políticas de confidencialidad.
    - Realizar procedimiento de inducción.
    - Cada colaborador debe conocer y comprender las políticas de la empresa.
    - Aplicar auditorías internas.

- Los colaboradores no deben compartir Información Confidencial con terceros, excepto si se le es autorizado previamente.

- Los colaboradores no deberán compartir Información Confidencial con los colaboradores de otras sedes de la empresa, a menos que el(los) empleado(s) tengan motivo para conocer la información y estén obligados por las restricciones de confidencialidad correspondientes.
    - Los colaboradores de otras sedes de la empresa deben firmar el contrato de confidencialidad.

- Los colaboradores deben abstenerse de discutir la Información Confidencial en lugares en donde otros puedan escuchar por casualidad. Esto aplica dentro y fuera de la oficina.

- Los colaboradores deben ejercer cuidado extra al tener conversaciones en lugares públicos como restaurantes, trenes, elevadores, taxis, aviones, etc., y al utilizar teléfonos de manos libres o teléfonos celulares.

- Los colaboradores que participan en llamadas con inversionistas u otros foros, deben estar preparados para respaldar sus análisis sin revelar Información Confidencial.

- Los colaboradores deben utilizar el sistema de correo electrónico de Continum Datacenter (y no su cuenta personal) @continumcenter.com para la transmisión electrónica de información relacionada con sus responsabilidades en la empresa o información importante que pueda ser trasmitida por este medio.
    - Realizar el procedimiento para administración de usuarios.

- El contacto con los clientes para la atención de solicitudes, cambios, atención de averías o transmisión de información importante que pueda ser trasmitida por este medio, se debe realizar por los medios oficiales, noc@continumcenter.com (21051327 / 21051301).
    - Realizar procedimiento para la gestión de solicitudes de servicio.
    - Realizar procedimiento para la gestión de incidentes.
    - Realizar procedimiento para la gestión de problemas.
    - Realizar procedimiento para la gestión de accesos.

- Los empleados no deben entregar parte alguna de un expediente o documento que contenga datos de tarjetas a tercero alguno sin el consentimiento expreso o instrucción del jefe directo correspondiente a su departamento.

- Los documentos, las notas y los demás trabajos analíticos de los colaboradores no se deberán dejar a la vista de visitantes u otras personas no autorizadas.
    - Brindar charlas y capacitación a los colaboradores.

- Se debe aplicar la norma de escritorios limpios y bloqueo de sesión al dejar de usar la computadora personal, para evitar el uso de sesiones abiertas para fines mal intencionados.

- Todo colaborador que maneje datos de titulares debe ingresar únicamente por red de gestión a las infraestructuras tecnológicas o vía VPN (en caso de acceso remoto).

- Toda comunicación privada y/o sensible debe ser encriptada utilizando VPN Site-to-Site y/o VPN de cliente de acceso remoto.

- Toda computadora portátil de gestión de los técnicos del NOC debe contar con el sistema de antivirus activo, configurado y actualizado.

- La gestión de la red y servidores debe realizarse vía PC de gestión hacia PC virtual de gestión dentro del centro de datos, para que la información laboral no se almacene en equipos personales de los técnicos.

- Todo acceso a la intranet o extranet tiene como intermediario un firewall (proxy).

- Todo acceso a VPN o PC virtual de gestión cuenta con un ID de usuario único y no replicado.

- Toda credencial de gestión se debe cambiar cada 60 días.

Medidas de seguridad lógicas para el manejo de datos personales.

Toda la información obtenida de diferentes medios para las personas que han dado su consentimiento, es almacenada en un Expediente digital, que a su vez se le emite una firma (hash) a cada pieza de datos para garantizar su integridad, toda esta información es almacenada en bases de datos seguras, y se maneja una política de credenciales de seguridad

- Se utiliza firewalling stateful inspection y firewall virtual para separar ambiente de cada cliente, en caso de no compartir un mismo escenario con otros clientes.

- Se utiliza un enrutamiento puntual o específico con tablas de rutas separadas entre sí de la tabla de rutas global, lo que permite no mezclar tráficos (VRF).

- Se utilizan enrutadores virtuales dedicados por cada cliente cuyo servicio debe estar separado de otros tráficos.

- Se utiliza la segmentación de redes.

- Se realiza detección y escaneo de amenazas (threat detection).

- Se realiza revisión diaria de amenazas registradas en el equipo de seguridad, para ver bloqueos y comportamiento del tráfico.
- El sistema encripta claves e información confidencial.
- Se maneja un procedimiento de cambio de credenciales.
- Todo acceso a esta información es por rutas encriptadas. como los VPN, TLS 1.2, HTTPS.
- Todo acceso a la base de datos es solo de servidores locales o vía VPN.
- Todo otro sistema interactúa con la base de datos por medio de WEBSERVICES para asegurar que datos se brindan/o no.
- El sistema de gestión mantiene trazabilidad de los cambios de datos por cada usuario.
- El sistema de gestión tiene seguridad por perfiles, permitiendo a unos usuarios ver temas y a otros restringiéndolos.

Medidas de seguridad físicas para el manejo de datos personales.

Continum cuenta con cuatro capas de seguridad física para asegurar sus instalaciones, personas y activos, así como políticas y procedimientos de seguridad física y de acceso al data center:

La seguridad física de nuestro data center implica proteger la infraestructura crítica de amenazas externas o intrusiones que atenten contra las actividades de la empresa y nuestros clientes. Así como elementos de alto valor y sumamente importantes, tales como servidores, switches y unidades de almacenamiento propios y de nuestros clientes.

Este tipo de seguridad incluye video-vigilancia a través de cámaras, sistemas de control de acceso y seguridad perimetral. Se pronostica que la seguridad física para centros de datos crecerá significativamente durante el periodo 2017-2019.

Las mejores prácticas globales de seguridad física para data centers se segmenta en cuatro niveles en base a las capas de seguridad:

1. Seguridad del perímetro
2. Seguridad de las instalaciones
3. Seguridad de la sala de ordenadores
4. Seguridad a nivel de racks

Seguridad perimetral – primera capa

El principal objetivo de esta capa de protección del data center se basa en las cuatro D's: detener, detectar, demorar y desistir.

Existen varios ejemplos de barreras que pueden ser utilizadas para proteger al data center bajo esta primera capa, desde los elementos más convencionales como bardas o cercas, hasta los métodos más sofisticados como fosas con cocodrilos (si, los animales de verdad). Todo depende del enfoque y el tipo de empresa, por lo general encontraremos métodos más complejos en instituciones bancarias y en compañías que brindan su data center como servicio a terceros.

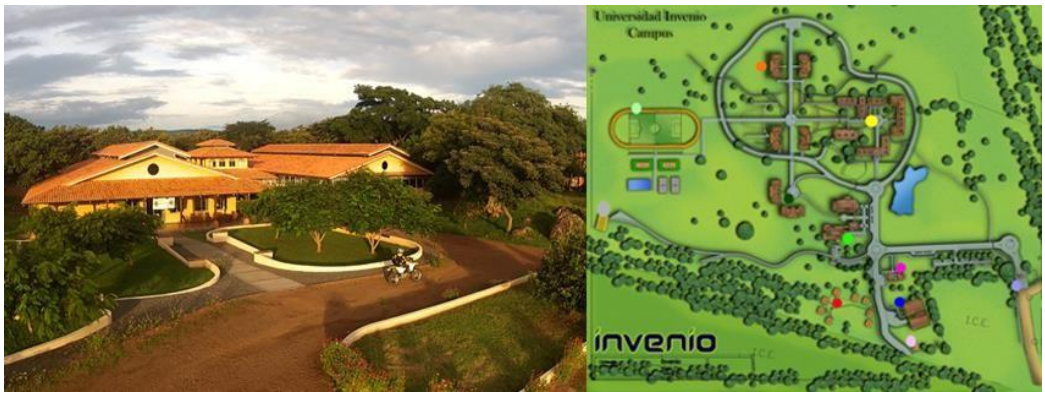
En CDC la seguridad perimetral se aplica al Campus Invenio GML donde se ubican tanto la Universidad Invenio como Continum DC. Se basa, además, en el principio ¿Quién es? ¿Qué tiene? ¿Qué sabe?

El Campus Invenio GML está cercado con alambre de púas (Barbed Wire Fence) que delimita el mismo y que permite aplicar la ley respectiva de invasión de la propiedad privada de la República de Costa Rica. Este perímetro está controlado por personal de seguridad contratado a una empresa privada especializada en esta labor. Esta firma de seguridad aplica un protocolo de seguridad y apoyado por equipo técnico y humano para evitar el ingreso y permanencia de personas no autorizadas, ingreso o permanencia sea a pie o en vehículo.

Un elemento de alto valor es la distancia desde la zona pública hasta las instalaciones, tanto de Universidad como del Data Center que permite cumplir con los principios de detectar y demorar.

El Gobierno de la República de Costa Rica, por medio del ministerio de Comercio Exterior ha autorizado a CDC a funcionar como Zona Franca sin necesidad de malla perimetral interna pues cumple con las condiciones necesarias de seguridad perimetral del Campus donde opera Continum Data Center.

En un plazo no mayor a 2 años, y para superar los requerimientos, CDC reforzará sus instalaciones no solo con malla perimetral interna, sino con un muro de concreto reforzado al frente del Centro de Datos.



Seguridad de las instalaciones – segunda capa

El objetivo de esta segunda capa de protección se centra en restringir el acceso en caso de que se presente una violación en el perímetro. La vigilancia en los interiores, sistemas de identificación y métodos de verificación, son algunos de los elementos esenciales en esta capa de protección física, así como los procedimientos y políticas para el acceso al data center, aplicadas a colaboradores y visitas

El tipo de instalación dictará los niveles necesarios de seguridad en relación al balance que se debe considerar entre la seguridad requerida y la experiencia de las visitas.

Continum Data Center es un edificio tipo Bunker con paredes de concreto reforzadas y que obedece a un diseño aprobado por el UP-Time Institute y conforme a las normas para calificarlo Edificio tipo A que cumple y supera nuestra meta de protección de la segunda capa de seguridad.

Seguridad de la sala de ordenadores – tercera capa

El objetivo de esta tercera capa de seguridad física es restringir el acceso a través de múltiples métodos de verificación, monitorear todos los accesos autorizados y contar con redundancia energética y de comunicaciones.

El acceso a la sala de ordenadores de CDC está restringido a un pequeño grupo de personas seleccionadas según su perfil para la entrega de credenciales mediante el proceso para la gestión de accesos. Existen diversos métodos para restringir el acceso a esta área, y estos pueden ser clasificados en base a su nivel de confiabilidad:

- “Lo que sabe”, esta categoría es la menos confiable y hace referencia principalmente a contraseñas.
- “Lo que tiene”, categoría intermedia la cual engloba dispositivos como tarjetas o llaves de acceso.
- “Lo que es”, esta categoría es el método más confiable y se basa en la autenticación biométrica.

Seguridad a nivel de racks – cuarta capa

Esta última capa de seguridad es particularmente importante y efectiva para minimizar las amenazas internas. La mayoría de los data center enfocan su atención en las primeras tres capas de seguridad, pero la ausencia de control en los racks puede resultar en una costosa fuga de información causada por una persona con malas intenciones.

Algunas consideraciones importantes para esta cuarta capa de seguridad:

- Sistemas de bloqueo físico o electrónico para racks de servidores.
- Sistemas físicos o biométricos para autorizar el acceso a los racks.
- Video-vigilancia para capturar imágenes de la actividad de las personas en los racks.

Continum: Un Data Center Seguro

Los avances tecnológicos en tema de cables y dispositivos electrónicos han elevado la posibilidad de contar con un data center totalmente seguro. Las aplicaciones que aprovechan las redes IP nos brindan la posibilidad de contar con una plataforma integrada para las cuatro capas de seguridad que hemos revisado en este documento, facilitando un sistema eficiente, efectivo y sobre todo inteligente.

En Continum Data Center mantenemos el firme propósito de continuar revisando y mejorando nuestras medidas de seguridad física para garantizar un servicio de excelencia para nuestros clientes internos y externos

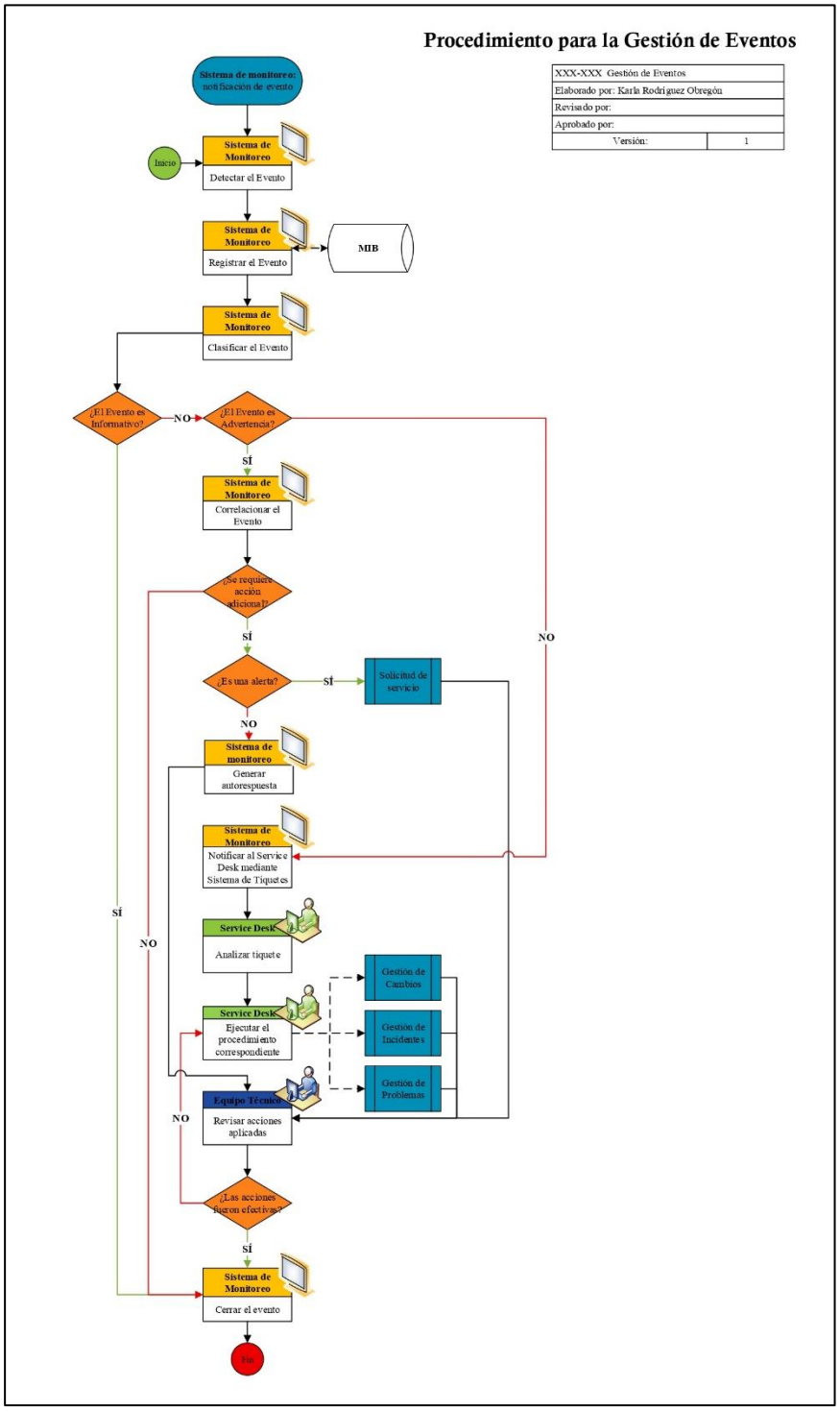
ADRIAN LACHNER CASTRO (FIRMA)

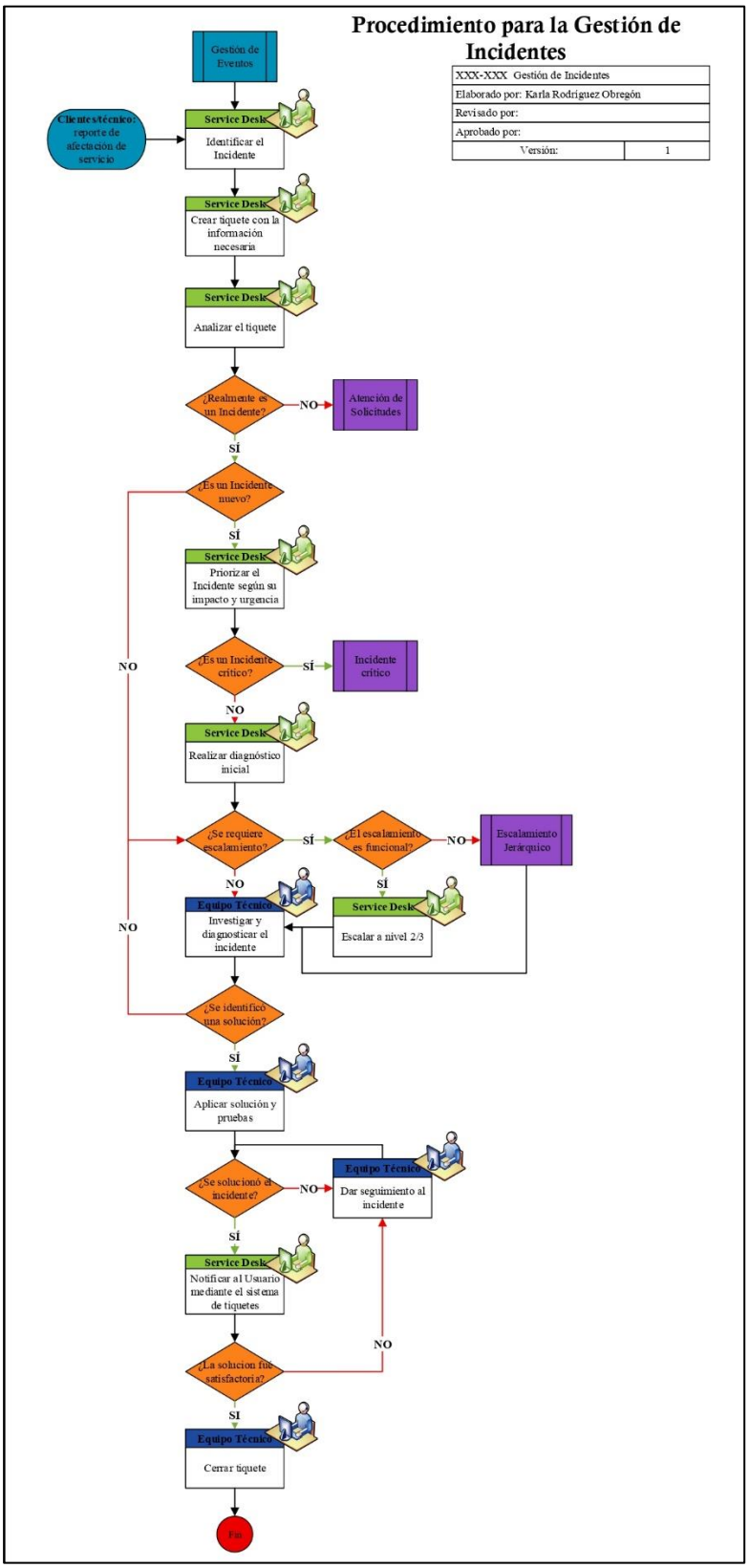
Digitally signed by ADRIAN LACHNER CASTRO (FIRMA)
Date: 2020.05.13 18:06:09 -06'00'

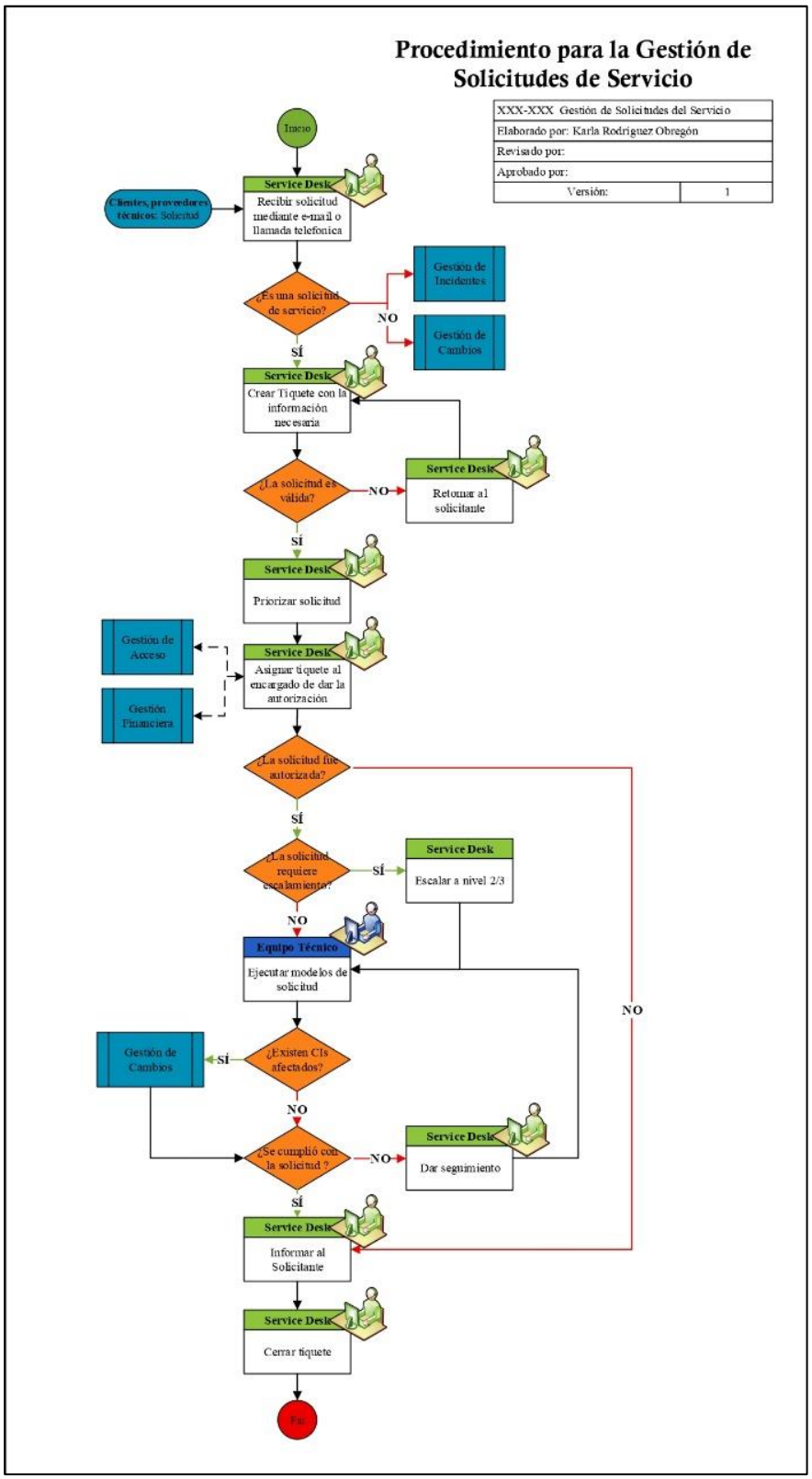
Adrián Lachner Castro
105940313

Anexos

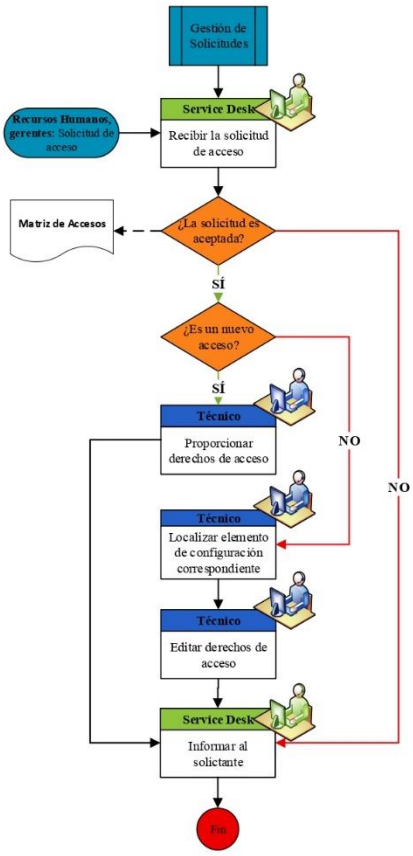
Anexo A: Protocolos mínimos de actuación




Procedimiento para la Gestión de Incidentes
XXX-XXX Gestión de Incidentes
Elaborado por: Karla Rodríguez Obregón
Revisado por:
Aprobado por:
Versión: 1
Gestión de Eventos
Clientes/técnicos reporte de afectación de servicio
Service Desk
Identificar el Incidente
Service Desk
Crear tiquete con la información necesaria
Service Desk
Analizar el tiquete
¿Realmente es un Incidente?
NO
Atención de Solicitudes
SÍ
¿Es un Incidente nuevo?
SÍ
Service Desk
Priorizar el Incidente según su impacto y urgencia
¿Es un Incidente crítico?
SÍ
Incidente crítico
NO
Service Desk
Realizar diagnóstico inicial
¿Se requiere escalamiento?
SÍ
¿El escalamiento es funcional?
NO
Escalamiento Jerárquico
SÍ
Service Desk
Escalar a nivel 2/3
NO
Equipo Técnico
Investigar y diagnosticar el incidente
NO
NO
¿Se identificó una solución?
SÍ
Equipo Técnico
Aplicar solución y pruebas
¿Se solucionó el incidente?
NO
Equipo Técnico
Dar seguimiento al incidente
SÍ
Service Desk
Notificar al Usuario mediante el sistema de tiquetes
NO
¿La solucion fue satisfactoria?
SI
Equipo Técnico
Cerrar tiquete
Fin


Procedimiento para la Gestión de Solicitudes de Servicio
XXX-XXX Gestión de Solicitudes del Servicio
Elaborado por: Karla Rodriguez Obregón
Revisado por:
Aprobado por:
Versión: 1
Inicio
Clientes, proveedores técnicos: Solicitud
Service Desk
Recibir solicitud mediante e-mail o llamada telefonica
¿Es una solicitud de servicio?
NO
Gestión de Incidentes
Gestión de Cambios
SÍ
Service Desk
Crear Tiquete con la información necesaria
¿La solicitud es válida?
NO
Service Desk
Retomar al solicitante
SÍ
Service Desk
Priorizar solicitud
Gestión de Acceso
Gestión Financiera
Service Desk
Asignar tiquete al encargado de dar la autorización
¿La solicitud fue autorizada?
NO
SÍ
¿La solicitud requiere escalamiento?
SÍ
Service Desk
Escalar a nivel 2/3
NO
Equipo Técnico
Ejecutar modelos de solicitud
Gestión de Cambios
SÍ
¿Existen CIs afectados?
NO
¿Se cumplió con la solicitud ?
NO
Service Desk
Dar seguimiento
SÍ
Service Desk
Informar al Solicitante
Service Desk
Cerrar tiquete
Fin

Procedimiento para la Gestión de Accesos



XXX-XXX Gestión de Acceso	
Elaborado por: Karla Rodríguez Obregón	
Revisado por:	
Aprobado por:	
Versión:	1