OAXACA

PROYECTO:

“DOCUMENTACIÓN CATALOGO DE SERVICIOS DE INFRAESTRUCTURA EN LA UNIVERSIDAD ANAHUAC DE OAXACA”

Índice

1.- Portafolio de Servicios

2.- Catálogo de Servicios

3.- SLA's

4.- Plan de Capacidad

5.- Gestión de servicios de control de seguridad

6.- Manual de Control de Cambios

- 6.1 - RFC's
- 6.2 - Documento de procesos para la gestión de cambios

7.- Validación y prueba de la entrega

- 7.1 - Documento de Memoria Técnica

8.- Operación del Servicio

- 8.1 - Documento de eventos, incidentes y problemas
- 8.2 – Carta de Bienvenida
- 8.3 - Formato de reporte de servicio

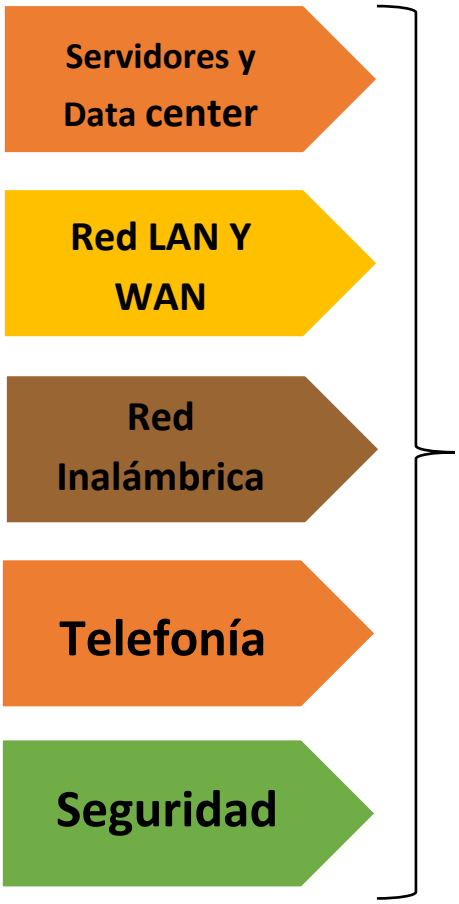
9.- Valor del Servicio

- 9.1 - Diagramas de flujo de eventos y de incidentes
- 9.2 - Proceso de Gestión de Incidentes

10. ejemplo de cómo se documenta un problema (errores conocidos)

- 10.1 perfil del puesto

1.-Portafolio de Servicios



Portafolio de servicios.

Servidores y Data center

Descripción: Servicio basado en la implementación de servidores para las diferentes aplicaciones y servicios que presta el área de servicios de tecnología de la universidad Anahuac Oaxaca.

Propuesta de valor:

- Estabilidad del servicio, que garantiza calidad y rendimiento óptimo del procesamiento, transferencia y almacenaje de la información vital para la universidad.
- Actualización y mantenimiento de los equipos, garantizando el servicio al 100 % los 365 días del año.
- Actualización de los equipos cada 4 años
- Aumento de memorias según las necesidades

Red LAN y WAN

Descripción: El servicio de Red LAN y WAN, garantiza el servicio de internet y telefonía en todas las áreas de la universidad Anahuac.

Propuesta de valor:

- Conexión entre edificios mediante fibra óptica, tomando en cuenta que con ello se garantiza la transmisión.
- Administración, segmentación y mejor rendimiento de los switches de acuerdo a las necesidades de la universidad, por ejemplo, segmentación por vlans dividiendo entre administrativos y salas de computo.
- Diseño e instalación de redes de área local y amplia.
- Certificación del cableado, garantizando el óptimo rendimiento de la misma.

Red Inalámbrica

Descripción: El servicio garantiza la conexión vía inalámbrica en todo el campus.

Propuesta de valor:

- Conexión garantizada durante los horarios de clases.
- Servicio garantizado durante el horario y calendario escolar.
- Mantenimiento y actualización a los equipos, para garantizar la estabilidad del servicio.

Telefonía

Descripción: El servicio de telefonía permite la comunicación de la universidad internamente y externamente, garantizando ahorro en costos.

Propuesta de valor:

- Reducción de costos
- Tecnología actualizada
- Comunicación garantizada entre personal y llamadas externas
- Mantenimiento y actualización del firmware de los equipos para garantizar la estabilidad del servicio.

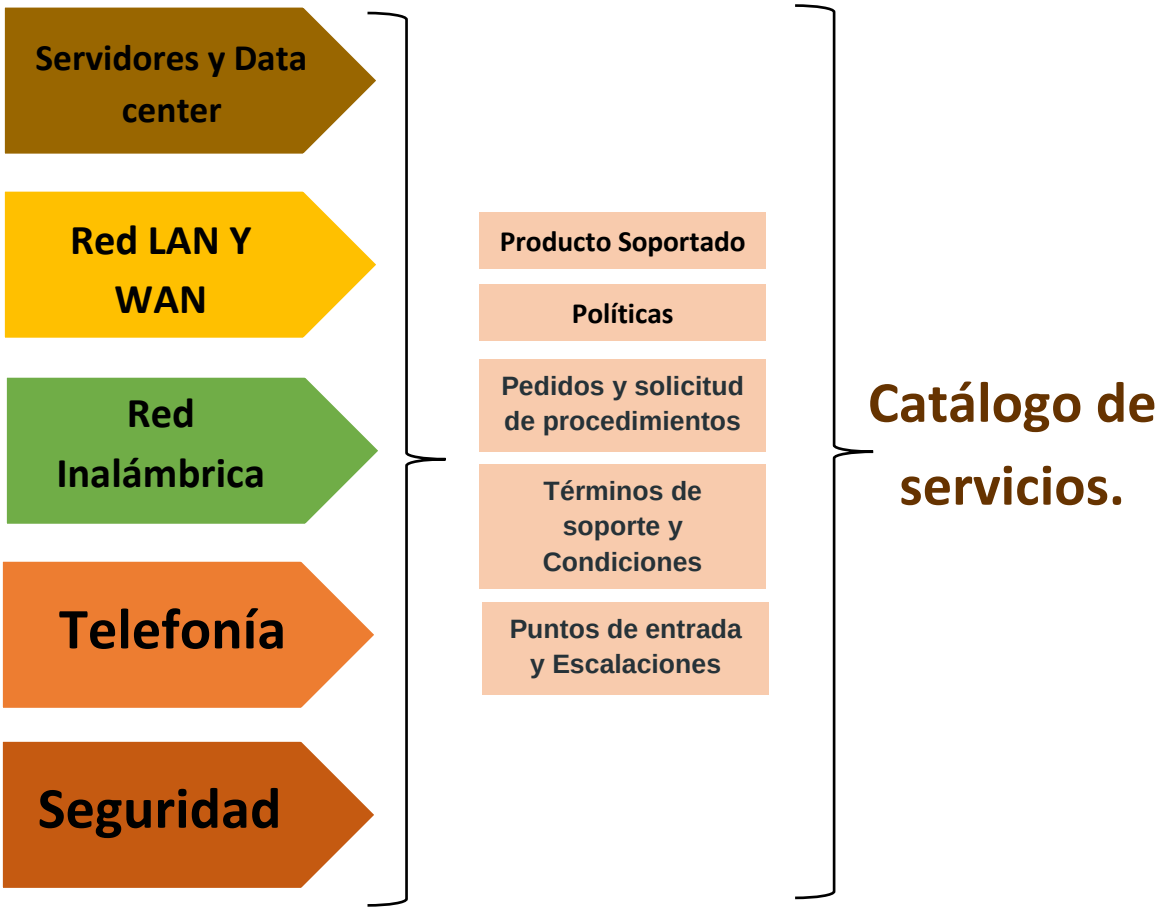
Seguridad

Descripción: El servicio de seguridad de red tiene como objetivo mantener las redes y comunicaciones lo más seguras posibles, así como la definición y manteniendo de las políticas y procedimientos de seguridad.

Propuesta de valor:

- Prevención y medidas de protección ante amenazas a la seguridad de los sistemas y redes, optimizándolas, evitándolas o mitigándolas en la medida de lo posible, minimizando el impacto.

2.-Catálogo de Servicios


Servidores y Data center
Red LAN Y WAN
Red Inalámbrica
Telefonía
Seguridad
Producto Soportado
Políticas
Pedidos y solicitud de procedimientos
Términos de soporte y Condiciones
Puntos de entrada y Escalaciones
Catálogo de servicios.

Servidores y Data center	
Producto Soportado	Servidores marca Dell y Lenovo Virtualización en Vmware y hyperV
Políticas	-Se configuran en la vlan 14 -Deben tener antivirus instalado -Programar actualizaciones mensuales -Programar backups según el servicio almacenado
Pedidos y solicitud de procedimientos	Las solicitudes para instalación de servidores o solicitud de almacenamiento en los mismos se realizan mediante correo electrónico a Jorge.gomez@anahuac.mx, quien autoriza y da fecha de atención
Términos de soporte y Condiciones	
Puntos de entrada y Escalaciones	

Red LAN y WAN	
Producto Soportado	Cableado panduit en categoría 6, switches marca extreme y cisco, conexión entre edificios de Fibra Óptica Multimodo
Políticas	El cableado debe estar estandarizado. Se debe conectar a la vlan que le corresponda según área.
Pedidos y solicitud de procedimientos	-La solicitud de nodos se realiza con 15 días de anticipación para solicitar la cotización y planear el trabajo con la empresa. -Las conexiones de equipos se solicitan con 24 hrs de anticipación, para realizar la configuración del puerto si es necesario.

Términos de soporte y Condiciones	El soporte que se brinda es: -conexión de equipos mediante cables cat 6 y en el nodo correspondiente ya sea de voz o datos - se debe solicitar las conexiones con horas de anticipación

Red Inalámbrica	
Producto Soportado	Switches Cisco Meraki y Ap´s cisco meraki
Políticas	Se cuentas con 3 SSID dependiendo del puesto se realizará la conexión mediante el usuario y contraseña entregado por el área de servicios tecnológicos - UAOProfesores - UAOAlumnos - UAOInvitados Las políticas de navegación están empatadas con las políticas de seguridad de la red LAN, mediante el equipo Fortigate.
Pedidos y solicitud de procedimientos	La solicitud de usuario y contraseña se solicitan con horas de anticipación para poder generarlos en el servidor correspondiente.
Términos de soporte y Condiciones	El apoyo para la conexión de realiza en las áreas de servicios tecnológicos ubicadas en los edificios A y E.
Puntos de entrada y Escalaciones	El servicio no se cobra a los usuarios.

Telefonía	
Producto Soportado	Cisco y Huawei
Políticas	El servicio se presta a todas las áreas según las necesidades, tienen permisos para realizar llamadas internas, locales, nacionales e internacionales según el puesto en el que se encuentren, debido a las necesidades de cada uno de ellos.
Pedidos y solicitud de procedimientos	La solicitud de equipo se hace mediante un correo electrónico a jorge.gomez@anahuac.mx, quien lo comparte con el consejo para su autorización, teniendo la autorización se le asigna extensión según el área y se le asigna el tipo de llamada.
Términos de soporte y Condiciones	Se brinda soporte en el transcurso del día que se reporta la falla, en caso de estar dañado el equipo o puerto se le informa al usuario la gravedad del problema y se le da tiempo de reparación.

Seguridad	
Producto Soportado	Forigate 300C
Políticas	Las políticas que se tienen configuradas en el equipo dependen de la vlan a la que estén conectados los equipos: - Vlan administrativos - Vlan Salas de computo - Vlan cámaras - Vlan servidores
Pedidos y solicitud de procedimientos	Las políticas configuradas en el equipo se configuran según las necesidades de las áreas y para cambiarlas o modificarlas se realiza mediante un correo electrónico a

	soporteuao@anahuac.mx mediante el cual se revisa la información y se informa si la solicitud es viable o que opciones se pueden ofrecer.
Términos de soporte y Condiciones	El soporte que se presenta en este servicio es la apertura de páginas o puertos necesarios para algunas aplicaciones o clases específicas y que la red este bloqueando, así como garantizar eventos o conexiones para sesiones remotas.

3.-SLA

Acuerdo de nivel de servicio (SLA) de Telefonía.

Nombre del servicio: Telefonía

Información de autorización: Comité rectoral

- Gestor del nivel de servicio: Jorge Gómez Hernandez
- Cliente: Usuarios de Telefonía de la Universidad Anahuac de Oaxaca

1.- Resumen General

El presente acuerdo de nivel de servicio (SLA) entre el área de servicios de tecnología y el cliente para documentar:

- El servicio de Telefonía
- Los niveles generales de respuesta, disponibilidad y mantenimiento asociado con este servicio.
- Las responsabilidades del Área de Servicios de Tecnología como proveedor de este servicio.
- Las responsabilidades del cliente quien recibe este servicio.

Este acuerdo de nivel de servicio permanecerá vigente durante un año.

2.- Descripción del servicio

Los servicios de TI suministrados por el área de servicios de tecnología son documentados en el catálogo de servicios:

2.1 Alcance del servicio

Asegurar el funcionamiento del servicio de telefonía.

Las funcionalidades del servicio son:

- Permite hacer y recibir llamadas locales y de larga nacional e internacional.
- Permite hacer y recibir llamadas a teléfonos celulares.
- Proveer la capacidad de realizar llamadas en modo conferencias entre 3 usuarios.

- Ofrece la asignación de claves para realizar llamadas.

Adicionalmente, el área de servicios de tecnología brinda, gente y procesos incluyendo:

Instalaciones de infraestructura telefónica

Altas, bajas, cambios, reubicación y atención a fallas de extensiones telefónicas.

Programación de extensiones, facilidades, permisos y troncales telefónicas.

2.2 Desempeño del nivel de servicio

2.2.1 Niveles de servicio especifico

Descripción	Objetivo	Horario	Criterios de medición	Comentarios
Disponibilidad del conmutador	90%	7X24		
Tiempo de atención para el soporte técnico dentro del 1er día	90%	8X5	Mesa de Servicio	Aplica restricciones en días festivos y vacaciones institucionales.

3.- Roles y responsabilidades

Los siguientes propietarios de servicios serán utilizados como la base del acuerdo y representan los principales involucrados con este SLA.

- Por el cliente:

Listado de usuarios que cuentan con equipo telefónico y extensión asignada:

Nombre	Departamento	Ext.
Rodrigo del Val Martín	Rectoría	1101
Patsy Carime Hernández Vásquez	Rectoría	1100
Guillermo Romero Pérez	Finanzas	1201
Faraón España Silva	Finanzas	1205
Adán Esteban Cruz Caballero	Finanzas	1210
Karina Wiyuris Soto	Caja	1200
Alejandro Chávez Bautista	APREU	1515
Elizabeth Félix Acevedo	APREU	1516
Alina Hernández Nieto	APREU	1517
Alicia Galguera Noriega	APREU	1518
Lluvia Itaií Ruiz Ramos	APREU	1519
Alfredo woolrich Bolanos Cacho	APREU	1514
Sarahi Rocio Perez Castro	Desarrollo Institucional	1106
Hortensia Elizabeth Zarate Ocaña	Desarrollo Institucional	1520
Sandra Fabiola Vasquez Perez	Sorteo Anahuac	1521
Guillermo Alfredo Monzón Guzmán	Ext. Y Posgrado	1505
Asesor Posgrado 1	Ext. Y Posgrado	1506
Claudia Ivette Gopar Méndez	Ext. Y Posgrado	1507
Jesús Eduardo Cruz Ortiz	Desarrollo de Negocios	1508
Yoani Paola Rodríguez Villegas	Dirección Académica	1301
Diana Irma Rodríguez Bautista	Dirección Académica	1302
Dalia Alarcón Gonzalez	Dirección Académica	1300
Secretaria Pool	Dirección Académica	1303
Asistente Dirección Académica	Dirección Académica	1304
Irene Osorio Pineda	Dirección Académica	1305
Eduardo Lopez Lopez	Dirección Académica	1306
Luisa Miriam Toledo Ramos	Dirección Académica	1307
Martin Rodriguez Brindis	Investigación	1310
Lorena López Limón	Dirección de Gastronomía y Turismo	1315
Cintya Anali Ruiz Rodriguez	Asistente Dirección de Gastronomía y Turismo	1322
Cocinas Gastronomía	Dirección de Gastronomía y Turismo	1324
Carlos Alberto Diaz Perez	Dirección de Comunicación	1316
Juan Francisco Robles Duran	Centro de Medios	1340

Martin Garnica Hernández	Dirección de Ingeniería	1317
Diego Arroyo Celaya	Dirección de Lenguas	1318
Edgar Cabrera Salazar	Dirección de negocios	1319
Héctor Vásquez Quevedo	Dirección de Derecho	1320
Horacio Guevara Cruz	Dirección de Psicología	1321
Juan Fernando Zamudio Villareal	Dirección de Medicina	1325
Alejandra Aura Perez Olvera	Asistente Dirección de Medicina	1330
Jorge Gómez Hernández	Servicios tecnológicos	1400
Agripino García Cruz	Servicios tecnológicos	1401
Diego Meingüer Cuevas	Servicios tecnológicos	1402
Christian Yesica Méndez Ruiz	Servicios tecnológicos	1403
Arinelly Rojas Alcántara	Servicios Escolares	1410
Luz Estrella Nieto	Servicios Escolares	1411
Arely Amador Geroniimo	Servicios Escolares	1412
Omar Spencer Motes Quiroz	Formación Integral	1110
Sofía Montes Pérez	Formación Integral	1111
Alheli Torres Ramírez	Formación Integral	1112
Jose Berra Pérez	Formación Integral	1109
Erwin Garcia Acevedo	Deportes	1113
Julio Cesar Mendoza Cruz	Biblioteca	1350
Biblioteca Mostrador	Biblioteca	1351
Javier Gutiérrez Cortés	Mantenimiento	1215
	Caseta de Policías	1220

- Por el área de servicios de tecnología

Nombre	Rol	Correo	Teléfono	Puesto
M. Jorge Gómez Hernandez	Administrador de niveles de servicio	jorge.gomez@anahuac.mx	5016250 ext.1400	Jefe del área de servicios de tecnología
Ing. Diego Meinguer	Dueño del proceso	Diego.meinguer@anahuac.mx	5016250 ext.1403	Especialista en infraestructura

Roles y responsabilidades del Área de servicios de tecnología.

Responsabilidades del área de servicios de Tecnología:

- Se proveerá la tecnología, gente y procesos necesarios para el servicio de telefonía, así como:
- Claramente documentar los servicios suministrados en el catálogo de servicios.
- Cumplir con los tiempos de respuesta asociados con la prioridad asignada a incidentes y requerimientos del servicio.
- Generar reportes semestrales sobre el desempeño de los niveles de servicios.
- Generar plan de mejora a partir de los resultados de los reportes de desempeño.
- Notificación apropiada a los usuarios de la telefonía de la universidad para todos los mantenimientos planeados vía calendario de mantenimiento.

Responsabilidades del cliente:

Las responsabilidades y/o requerimientos de este acuerdo incluyen:

- Llevar a cabo el proceso para solicitud de servicio y reportes de incidentes. Utilizando la mesa de servicio del área de tecnología como un canal único de comunicación para la atención de solicitudes y problemáticas sobre la telefonía.
- Contactar al administrador de los niveles de servicios para cualquier adición o modificación en los niveles de servicio.
- Proporcionar la información necesaria para la atención del incidente.
- Cumplir con las políticas emitidas por el área de tecnología.

4.- Solicitar el Servicio

El área de servicios tecnológicos atenderá las solicitudes de los usuarios cada vez que requieran utilizar los servicios ofrecidos.

Así mismo, tratara de restaurar la operación normal de los servicios cuando estos presenten incidentes, con el mínimo impacto a los usuarios de este

servicio dentro de los tiempos de atención y resolución acordados en este documento.

Teléfono: 5016250
Extensiones: 1400 y 1403
Horario de atención: 9:00 a.m. a 6:00 p.m. de lunes a viernes basándonos en el calendario universitario.
Las solicitudes levantadas fuera del horario de atención se mandarán a la cola del siguiente día hábil para ser atendidos en horario de atención.

5.- Horario de Cobertura, tiempos de solución y Escalamiento

La meta del área de tecnología es la de tener a un profesional asignado y con las habilidades adecuadas para resolver las incidencias/requerimientos dentro de los tiempos de solución en este documento, a partir de la recepción de la solicitud.

5.1 Horario de cobertura

- El horario para la disponibilidad del conmutador es proveído las 24 horas del día, 7 días a la semana excepto en los periodos de mantenimiento planeados.
- Las solicitudes son mediante correo electrónico de soporte.uao@anahuac.mx y pueden ser enviadas las 24 horas al día 7 días a la semana y son procesadas durante el siguiente día laboral.

5.2 Incidentes y requerimientos

La meta del área de tecnología es la de tener a un profesional asignado y con las habilidades adecuadas para resolver las incidencias/requerimientos dentro de los tiempos de solución en este documento.

Tiempos de respuesta y solución		
Prioridad	Tiempo de Respuesta	Tiempo de Solución
1	30 min	1 día

2	30 min	3 días
3	30 min	Planeado

Impacto, Urgencia y Prioridad

Matriz de Urgencia		
(Tiempo disponible hasta la resolución)		
Urgencia Alta	Criterios	El servicio está totalmente detenido
Urgencia Media	Criterios	El servicio está parcialmente detenido
Urgencia Baja	Criterios	El usuario puede trabajar

Matriz de Impacto		
(Grado de Severidad del impacto al negocio)		
Impacto (Alto)	Criterios	El servicio está totalmente detenido
Impacto (Medio)	Criterios	Área completa
Impacto (Bajo)	Criterios	Solo Un usuario

Matriz de Impacto / Urgencia				
Urgencia	Impacto			
		Alto	Medio	Bajo
	Alta	1	2	3
	Media	2	3	1
	Baja	3	1	2

5.3 Información

Si los usuarios tienen alguna duda de los acuerdos de niveles de servicio, el punto de contacto será el rol del "Administrador de niveles de servicio".

5.4 Excepciones del servicio para cobertura

Excepción	Parámetro	Cobertura
Días Festivos	Calendario oficial de la UAO	Sin cobertura
Vacaciones Institucionales	Calendario Oficial de la UAO	Sin cobertura
El solicitante no cuenta con la autorización correspondiente	N/A	Sin cobertura
Por causas inherentes a los proveedores de servicios	Falla	Sin cobertura

5.5 Requisitos mínimos para brindar el servicio.

- Ser empleado administrativo vigente y contar con autorización del titular del área, además de contar con el servicio telefónico.

- Contar con los recursos económicos para cubrir los gastos de corrección de la falla.

- contar con correo institucional @anahuac.mx

6.- mantenimiento y cambios al servicio

- Mantenimiento semanal: N/A

- Mantenimientos Planeados: Se le darán 2 mantenimientos preventivos al año. En caso de que el servicio se vaya a suspender se avisara con una semana de anticipación a los usuarios.

- Atención a peticiones de cambio: Toda petición de cambio se debe de realizar a través del correo de soporte.uao@anahuac.mx y será trabajado bajo el proceso de cambios definido en este documento.

7.- Precio

N/A

8.- Revisiones

8.1 Revisiones del SLA

Este acuerdo es válido desde el 1 de enero del 2017 y será revisado anualmente o como se necesite.

El administrador de niveles de servicio es responsable de facilitar recisiones anuales de este documento. El contenido de este documento puede ser actualizado cuando se requiera, siempre y cuando exista un acuerdo mutuo con los principales involucrados y comunicado a todas las partes afectadas. El Administrador de niveles de servicio incorporará todas las revisiones subsecuentes y obtendrá los acuerdos mutuos.

4.-PLAN DE CAPACIDAD

Plan de capacidad del servicio de Telefonía

La administración de la capacidad es la disciplina encargada de asegurar que todos los servicios de TI este soportados por una infraestructura tecnológica con capacidades acordes con las necesidades de la empresa, dentro de costos razonables.

Cuando no se establecen normas y procedimientos de administración de capacidades, existe la tendencia a desaprovechar los recursos disponibles y, peor aún, a realizar inversiones que realmente no son necesarias. También es posible que la ausencia de una buena administración de capacidades impida que una organización de TI prevea sus requerimientos de recursos y caiga en una situación de congestionamiento, que afecte la calidad y la continuidad de los servicios.

Las principales funciones de la administración de la capacidad pueden resumirse de la siguiente forma:

- Asegurar que se cubren las necesidades de capacidad TI tanto presentes, como futuras.
- Controlar el desempeño de la infraestructura TI.
- Desarrollar planes de crecimiento requeridos para cumplir con los niveles de servicio acordados con los usuarios.
- Analizar y armonizar el uso de los recursos de TI (memoria, discos, canales de comunicación, etc.)

Nombre del documento: Formato y recomendaciones de un plan de capacidades y de un plan de compras.

Aprobación del documento

Fecha	Aprobado Por	Rol en el proyecto	Firma
	Yoani Rodriguez	Rectora	

	Guillermo Romero	Dir. Finanzas	
	Jorge Gómez	Jefe de servicios tecnológicos	

Elaboración del documento

Fecha de creación: 02/01/2017

Última modificación: 15/02/2017

Fecha	Aprobado Por	Rol en el proyecto	Firma
02/01/2017	Diego Meinguer	Especialista en Infraestructura	
	Jorge Gómez	Administrador de niveles de servicio	

Plan de capacidades

Plan de Capacidades		
Termino	Descripción	Ejemplo
Unidad Ejecutora	Se refiere a las unidades, departamentos o áreas de la UAO que son responsables de alguno de los procesos críticos	Rectoría Finanzas
	Conjunto de actividades que tendrán que realizarse para entregar los productos y servicios fundamentales que	

Proceso critico	permitan a la UAO cumplir sus objetivos más importantes y sensibles.	Acreditaciones de la institución
Infraestructura de soporte	La tecnología, los recursos humanos y las instalaciones que permiten el procedimiento de las aplicaciones que soportan las actividades críticas de la UAO	Servidores de aplicaciones y bases de datos
Activo	Lo que le da valor a la institución	Software, hardware, documentación
Capacidad técnica	Rendimiento máximo que se puede obtener de un activo en el cumplimiento de los objetivos de nivel de servicio	Numero de Extensiones Capacidad de memoria

5.-Gestión de servicios de control de seguridad

Objetivos

Gestionar adecuadamente los incidentes y eventos de seguridad de la información, mediante el reporte oportuno de los usuarios, y el análisis de la información para reducir la afectación negativa de la seguridad de la información y/o la continuidad de las operaciones de la universidad Anahuac.

Alcance

Inicia con la detección del incidente de seguridad de la información.

Ámbito de Aplicación

Proteger la confidencialidad, integridad y disponibilidad de la información de la Universidad Anahuac Oaxaca

Definiciones

- **Activo de información**: Es cualquier elemento que tenga valor para la organización y, en consecuencia, debe ser protegido.
- **Amenaza:** Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la universidad. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.
- **Autenticidad**: Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.
- **Contención**: Evitar que el incidente siga ocasionando daños.
- **Erradicación**: Eliminar la causa del incidente y todo rastro de los daños.
- **Evento de seguridad:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Gestión de Incidentes**: Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, inclinados a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.
- **Impacto**: Consecuencias que produce un incidente de seguridad sobre la organización.
- **Incidente de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Logs:** Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.
- **Recuperación:** Volver el entorno afectado a su estado natural.
- **Sniffer**: Software que captura los paquetes que viajan por la red para obtener información de la red o del usuario.
- **SSI**: Subsistema de Seguridad de la Información.
- **Validación:** Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.
- **Vulnerabilidad:** Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

Generalidades.

1. Roles que participan en el proceso

- ## Oficial de Seguridad de la Información:

  Orientar y dar adecuado tratamiento a los incidentes de seguridad de la información detectados o reportados.
  Debe hacer un seguimiento periódico a los incidentes de seguridad presentados.

  En caso de no presentarse un número significativo de reportes de incidentes de seguridad revisara los reportes de las herramientas de seguridad para el análisis pertinente y otras fuentes con el propósito de mejorar la gestión de incidentes de seguridad.

- ## Colaboradores y contratistas

  Deben tomar conciencia de su responsabilidad de reportar eventos y debilidades de seguridad de la información tan pronto como sea posible al área de tecnologías de la información.
  Recibir las capacitaciones y participar en las campañas de sensibilización que se realicen al interior de la institución.
  Reportar oportunamente los incidentes o eventos de seguridad de la información y cualquier comportamiento anormal que se presente en la institución o en sus activos de información.

- **Grupo de Recursos Físicos**

  En caso de llegar a requerirse, debe hacer la valoración económica del activo de información involucrado en un evento/incidente de seguridad de la información.

- **El Grupo de Administración y Seguridad de la Información**

  Debe mantener constante capacitación y sensibilización a los colaboradores, contratistas y demás partes interesadas en cuanto al reporte de incidentes de seguridad de la información y vulnerabilidades de los sistemas de información con los que cuenta la institución, debe hacer énfasis en:

  a) Los riesgos de un control de seguridad ineficaz;
  b) Que es la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información.
  c) Los errores humanos.
  d) Las no conformidades con políticas o directrices.
  e) Violaciones de acuerdos de seguridad física.
  f) El mal funcionamiento en el software o hardware.
  g) Las violaciones de acceso.

  Lo anterior con el propósito que los colaboradores, contratistas y demás partes interesadas de la institucón estén en capacidad de reconocer y reportar incidentes de seguridad.

  Debe mantener contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información.

Tipo de Incidentes de seguridad.

Las partes interesadas del Subsistema de Seguridad de la Información deben conocer y saber identificar los incidentes aceptados por la institución:

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Ataques dirigidos y no dirigidos
- Pérdida o robo de la información.
- Modificación no autorizada.
- Información no actualizada.

- Mala gestión del conocimiento.
- Perdida o daño de la documentación.
- Daños sobre Activos de información
- Uso indebido de Activos de información
- Uso Indebido de Software
- Uso Indebido de Usuarios
- Suplantación de Identidad

El grupo responsable debe atender de manera inmediata el incidente de Seguridad de la Información, de acuerdo a los niveles de urgencia del evento / incidente a fin de darle el tratamiento adecuado.

Nivel	Descripción
Alto	Interrumpe seriamente la operación de la entidad, el incidente puede tener velocidad significativa/rápida en su propagación y ocasionar daños de activos. Podría llegar a afectar más de un tipo de activo.
Medio	Interrumpe en un periodo corto de tiempo los procesos generales de la entidad, el incidente/evento compromete un activo importante.
Bajo	No interrumpe los procesos generales de la entidad, el incidente/evento, se detecta y puede controlar fácilmente con recursos existentes en la entidad.

Tabla 1. Niveles de criticidad del evento/incidente

El área encargada de atender el incidente de Seguridad de la Información, debe conocer la siguiente tabla de escalamiento a fin de darle el tratamiento adecuado

Relevancia	Escalamiento
Alto	Se escala a los proveedores pertinentes
Medio	Se escala al Grupo de Administración y Seguridad de la Información, área de servicios tecnológicos y a las áreas involucradas
Bajo	Solo se dirige el caso al área de servicios de tecnología, o se escala al responsable del activo de información involucrado en caso de ser necesario.

Tabla 2. Niveles de escalamiento de evento/incidentes de seguridad de la información

El área de servicios de tecnologia de la información para preservar la Integridad, Disponibilidad y Confidencialidad de los activos de información debe generar las alertas tempranas mediante las herramientas tecnológicas disponibles así:

- Grupo de Infraestructura y soporte: Alertas de la infraestructura de T.I.
- Grupo de Administración y seguridad de la Información: Alertas de activos de Seguridad, Alertas de fuga de información.
- Grupo de Gestión de aplicaciones: Alertas de las plataformas de información.

1. Relación de actividades la Gestión de incidentes de seguridad de la información:

Actividades	Descripción	Responsable
Reportar el incidente de seguridad	Los colaboradores, personal de honorarios y demás partes interesadas con acceso a información de la institución nota que se está presentando un ataque a los activos de la institución, o es conocedor de que alguna persona está violando las políticas de seguridad de la información o conoce de riesgos asociados a la información, debe proceder a reportar esta situación como un evento o incidente de seguridad al área de servicios tecnológicos enviando un correo a ***soporte.uao@anahuac.mx***, llamando a las extensiones ***1400, 1401, 1402 o 1403,*** o informando directamente.	Los funcionarios, personal de honorarios y demás partes interesadas Área de servicios de tecnología
Registrar evento o incidente	El área de servicios tecnológicos toma los datos necesarios y realiza el registro correspondiente categorizando si se trata de incidente o evento, fecha y hora, pequeña descripción de lo ocurrido, si se puede solucionar de inmediato se documenta la solución aplicada entre otros.	Área de servicios de tecnología
	En dado caso que el área de servicios tecnológicos no pueda resolver el evento/incidente se escala al segundo nivel de Seguridad de la Información quien a su vez evaluará que tipo de evento/incidente es el que se presenta, a que activos está afectando, cual es	Segundo Nivel de seguridad

Evaluar el impacto	alcance del mismo, que pronóstico tiene de expansión, así como los daños potenciales o reales que se generen. Para evaluar la severidad de los eventos/incidentes considerará la relevancia de los activos y el nivel del incidente. Cuando exista la convivencia de más de un activo comprometido y/o más de un incidente o evento, todo el conjunto se valorará de acuerdo a los niveles descritos en la Tabla 1 de la presente guía y teniendo en cuenta la relevancia del activo.	
Identificar la relevancia del activo	De acuerdo a la verificación de los riesgos asociados a los activos de información, se establecerá la afectación del activo de información, incluyendo el valor económico y la cantidad información relevante para la Entidad contenida en el mismo.	Encargado de Seguridad de la Información - Grupo de Recursos Físicos – funcionarios, contratistas y demás partes interesadas
Identificar el nivel del incidente	El Encargado de la Seguridad de la Información, deberá identificar el nivel de afectación del incidente de acuerdo a los Niveles de Criticidad del Evento/Incidente descritos en la Tabla 1 del presente documento	Encargado de Seguridad de la Información
Escalar el incidente	Para buscar una solución al incidente el Encargado de Seguridad de la Información debe tener en cuenta los niveles de escalamientos Tabla 2.	Encargado de Seguridad de la Información
Recolectar evidencia	Para hacer una correcta recolección de evidencia el Encargado de Seguridad de la y el área encargada de gestionar el incidente de seguridad, deben tener en cuenta lo siguientes criterios para la recolección de evidencia: • Información basada en la red: logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de servidores de autenticación.	Grupo de Administración y Seguridad de la Información

	• Información Basada en el Equipo: Live data collection: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red. Otra información: Testimonio de colaborador o personal de honorarios que reporta el evento o incidente.	
Manejar la evidencia	El encargado de Seguridad de la Información junto al área encargada de gestionar el incidente de seguridad debe darle un correcto manejo a los datos y evidencias recolectadas, los cuales deben ser almacenados para futuras investigaciones e implementación de controles preventivos o de mejoramiento. La información que debe ser almacenada y custodiada por encargado de Seguridad de la Información incluye: • Cantidad de incidentes presentados y tratados. • Tiempo asignado a los incidentes. • Daños ocasionados. • Vulnerabilidades explotadas. • Cantidad de activos de información involucradas. • Frecuencias de ataques. • Pérdidas. Además, debe cumplir con un control de seguridad que garantice la confidencialidad, integridad y disponibilidad de las evidencias retenidas. El almacenamiento físico seguro de las evidencias estará custodiado por el encargado de Seguridad de la Información y el electrónico se	Grupo de Administración y Seguridad de la Información

	alamacena en el caso generado en la herramienta de gestión de TI.	
Identificar las fuentes de ataque	El área encargada de gestionar el incidente de seguridad, debe tener identificadas las posibles fuentes de ataque posteriormente mencionadas: • Empleados Descontentos. • Baja Concientización. • Crecimiento de Redes. • Falta de Previsión de Contingencias. • Falta de Políticas. • Desastres Naturales. • Inadecuada protección de la Infraestructura. • Confianza creciente en los sistemas • Virus. • Explotación de Vulnerabilidades, tanto a nivel de host, como de arquitectura de red (vulnerabilidades de la seguridad perimetral). • Robo de Información confidencial. • Violación a la privacidad. • Ingeniería social. • Denegación de Servicios. Hacking.	Grupo de Administración y Seguridad de la Información
Establecer la estrategia de Erradicación	El área encargada de gestionar el incidente de seguridad, debe tener en cuenta para definir/decidir las estrategias de erradicación los siguientes factores: •Tiempo y Recursos necesarios para poner en práctica la estrategia. •Efectividad de la Estrategia. •Pérdida económica. •Posibles implicaciones legales. •Relación costo-beneficio de la estrategia. •Experiencias anteriores. •Identificación de los Procedimientos de cada sistema Operativo comprometido.	Grupo de Administración y Seguridad de la Información

	•Identificación de Usuarios o servicios comprometidos para proceder a desactivarlos.	
Aplicar los procedimientos de Recuperación	El área encargada de gestionar el incidente de seguridad, para definir/decidir las estrategias de recuperación debe tener en cuenta los siguientes factores: • Cargar la copia de respaldo actualizada del sistema de información, configuración o base de datos. • Creación nuevamente de la información digital o física, configuración de sistemas operativos, sistemas de información, cargue manual de la información. • Actualización, instalación de parches de seguridad a los sistemas que se vieron comprometidos. Entre otras definidas en el Plan de Recuperación de desastres	Grupo de Administración y Seguridad de la Información
Realizar el análisis Post-Incidentes	El encargado de Seguridad de la Información debe garantizar el correcto manejo de las lecciones aprendidas, de la siguiente manera: • Periódicamente el encargado de Seguridad de la Información reunirá con el área de servicios de tecnología a fin de analizar los eventos e incidentes presentados durante el periodo. Se busca definir esquemas más efectivos para responder ante situaciones que afecten la seguridad de la información en la entidad. Entre las actividades que se realizan está: • Mantener la documentación de los eventos e incidentes de seguridad de la Información.	Grupo de Administración y Seguridad de la Información

	• Mantener actualizada la bases de datos de conocimientos. • Integrar los eventos e Incidentes a la Matriz de Riesgos de los Activos. • Realización de Capacitaciones a los Funcionarios de la entidad en lo relacionado a eventos e incidentes de seguridad de la información. • Analizar los Hechos y tomar decisiones.	

6.-Manual de Control de Cambios

El proceso inicia con la creación de un RFC (Request For Change o Solicitud de Cambio) por parte de una persona o grupo quien planea el cambio y lo somete a revisión técnica. Una vez completo el RFC, se presenta ante el departamento de Gestión de Cambios, el cual establece una valoración y evaluación inicial y decide si acepta, rechaza o solicita cambios al RFC. Los cambios aceptados deben ser aprobados de acuerdo a su clasificación y nivel de impacto. Cuando el RFC ha sido debidamente autorizado, su implementación es planeada, comunicada y ejecutada. Luego, dicha implementación es evaluada por el solicitante, que establece si esta fue exitosa o no. Las acciones necesarias para remediar efectos no esperados o no deseados, se ejecutan de ser necesario. Finalmente, el administrador de cambios revisa el desarrollo del cambio y cierra el RFC.

7.1 RFC´s

FORMULARIO DE CONTROL DE CAMBIOS

AÑO: 2017	FOLIO

1. Identificación Confección del documento	
Fecha de solicitud	
Nombre Solicitante	
Área o departamento	
Cargo	
E-mail	
Responsable del área	
Servicio	
Responsable del Cambio	

2. Tipo de Cambio	
□ Cambio Programado	□ Cambio no Programado

3. Objetivo del Cambio

4. Evaluación de Impacto	
	Severidad: □ Baja □ Media □ Alta Baja (No implica bajar el servicio) Media (Bajar el servicio de 1 hora) Alta (Bajar el servicio más de una hora)

5. Cronograma de Actividades

Nodo	Detalle Actividades	Responsable	Fecha	Tiempo estimado	Hora	
					Inicio	Fin

Observaciones
Si durante cualquier punto del cronograma de actividades se presentaran problemas la actividad será cancelada y todos los esfuerzos se centrarán en resolver los problemas.

6.- Escalamiento		
Nombre	Empresa	Teléfonos

7.- Severidad del cambio	
Fecha de disponibilidad	
Existe plan de retorno	
Recuperación de ultimo respaldo	
Puede existir perdida en la performance durante o después del cambio	

8.- Cronograma de Actividades del plan de Retorno				
Detalle actividades		Responsable	Hora	
			Inicio	Termino
Observaciones				

6.2 Documento de Procesos para la gestión de cambios

	Proceso	Servicios Tecnológicos
	Procedimiento	Gestión de incidentes

Elaboro Christian Méndez	Reviso Jorge Gómez	Aprobó Jorge Gómez
Objetivo	Atender, asegurar y resolver todos los incidentes de TI, mediante la utilización de mesa de servicios y bajo los parámetros de tiempo de respuesta acordados en los niveles de servicio, con el fin de restaurar y optimizar el servicio con un mínimo de impacto en la operación de la entidad.	
Alcance	Inicia con el registro de la solicitud ya sea por correo electrónico o vía telefónica, con todos los detalles que han ocurrido (hora, descripción, sistemas afectados y/o usuario que lo reporta), continua con el diagnóstico, análisis y la asignación de prioridad del incidente y finaliza la restauración, solución, monitoreo y seguimiento al incidente del servicio.	
Ámbito de Aplicación	Este procedimiento aplica a toda la operación de la universidad.	

Definiciones

ANS: Acuerdos de niveles de servicio de TI: Acuerdos de niveles de servicio – Es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

ALO: Acuerdos de niveles de operación – Se trata de un acuerdo entre el área de tecnologías y área solicitante. Brinda apoyo en la prestación de servicios al solicitante por parte del área de tecnologías de la información, define los bienes y servicios que se proveen y las responsabilidades de ambas partes.

Base de Datos de Conocimiento. Base de datos que contiene los conocimientos de la entidad, tales como manuales, procedimientos, políticas, entre otros. Por medio de esta base de datos se analizan, almacenan y se comparte la información al interior de

la entidad, con el fin de mejorar la eficiencia en algunos procesos y reducir la necesidad de redescubrir la información

Base de Datos de Errores Conocidos: Esta base de datos es administrada por la Gestión del Problemas y utilizada por Gestión del Incidente para la solución de incidentes repetitivos.

Ciclo de vida del Incidente: Fases detalladas en el ciclo de vida de un Incidente. Las fases son detección, diagnóstico, reparación, recuperación y restauración

Detección de Incidentes: La detección de incidentes es una etapa en el ciclo de vida del incidente, lleva a conocer el incidente al proveedor de servicios. La detección puede ser automática, o puede ser resultado de un incidente comunicado por un usuario.

Diagnóstico de Incidentes: Etapa en el ciclo de vida de un incidente. El propósito de diagnóstico es identificar una Alternativa para dar solución a un Incidente.

Prioridad: Categoría empleada para identificar la importancia relativa de un incidente. La Prioridad se basa en el Impacto y la Urgencia, y es utilizada para identificar los plazos requeridos para la realización de las diferentes acciones. Por ejemplo, un ANS de TI podría indicar que los Incidentes de Prioridad 2 deben ser resueltos en menos de 12 horas

Requerimiento: Un requerimiento es una descripción de una condición o capacidad que debe cumplir un sistema, ya sea derivada de una necesidad de tal manera que le sea útil a los funcionarios o a los usuarios finales.
Restauración del servicio: La restauración del servicio, es la toma de acción para restaurar un servicio de TI a los usuarios tras reparar y recuperarse de un incidente

Soporte Técnico: El soporte técnico se define como todas las actividades humanas que se deben realizar para corregir una o más fallas técnicas que los equipos puedan presentar con relación al hardware, software y sistemas de información cuando son operados por los usuarios.
TI: Tecnología de la Información

Nivel 1: Servicio prestado por un técnico de mesa de servicios, los cuales se basan en un conjunto de recursos técnicos y humano que permitirán dar soporte a diferentes usuarios informativos de la entidad. Estos servicios pueden ser prestados personalmente, telefónico o remotamente.

Nivel 2: La prestación del servicio es ofrecido por un analista, técnico o profesional especializado en un tema específico por la oficina de tecnologías de la información.

Nivel 3: Son los incidentes que la mesa de servicios ni por la Oficina de Tecnologías de la Información pueden solucionarlos, ya que son servicios categorizados por garantías.

Plataforma web CA: Software web para reportar los incidentes o servicios que requieran los usuarios de la Superintendencia Nacional de Salud.
Prioridad: Categoría empleada para identificar la importancia relativa de un incidente. La Prioridad se basa en el Impacto y la Urgencia, y es utilizada para identificar los plazos requeridos para la realización de las diferentes acciones. Por ejemplo, el un ANS podría indicar que los Incidentes de Prioridad 2 deben ser resueltos en menos de 12 horas.
Requerimiento: Un requerimiento es una descripción de una condición o capacidad que debe cumplir un sistema, ya sea derivada de una necesidad de tal manera que le sea útil a los funcionarios o a los usuarios finales.
Restauración del servicio: La restauración del servicio, es la toma de acción para restaurar un servicio de TI a los usuarios tras reparar y recuperarse de un incidente.
Solución Exitosa: es la gestión que realiza los analistas, técnicos y/o profesional resolviendo un incidente, cumpliendo los acuerdos de niveles de servicio y restaurando el servicio.
Soporte en sitio: es la solución personalizada del incidente en cada sitio de trabajo.

Políticas de operación

1. El área de servicios de tecnología es el punto único de contacto para el usuario, mediante el cual se atienden y solucionan los incidentes de servicios de Tecnologías de la Información (TI).
2. Tiempo de atención: EI tiempo de atención debe ser máximo de dos horas, desde el momento en que se registra la solicitud. La respuesta se entiende como el diagnóstico de la falla a través de la presencia directa por parte del analista y/o profesional en el sitio donde se encuentre el equipo.
3. Tiempo de solución: Es el tiempo determinado para solucionar el requerimiento y restaurar el servicio.
4. Si la solución del incidente no es favorable, la mesa de servicios debe proveer un equipo de iguales o superiores características en calidad de préstamo, hasta el momento en que se subsane el daño o se reemplace definitivamente el equipo.
5. Si dentro de los diez (10) días calendario siguientes a la prestación del servicio la herramienta tecnológica no se ha podido ser reparada, se deberá reemplazarla definitivamente por otro equipo de iguales o superiores características, éste deberá ser aprobado por el responsable del inventario de la infraestructura tecnológica de la entidad.
6. Cuando algún componente de hardware de la herramienta tecnológica haya sido reparado por la misma causa en tres (3) oportunidades dentro de un periodo de dos (2) meses, la herramienta tecnológica debe ser reemplazada definitivamente.

7. La prestación del servicio de soporte técnico por parte del área de tecnologías se dará solo en lo referente a cuestiones técnicas de herramientas tecnológicas utilizadas para el desarrollo de las actividades diarias.
8. Los colaboradores deberán asegurarse de comunicar de forma oportuna la realización de copias de respaldo o backups a la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.
9. El colaborador deberá reportar de forma inmediata a la Oficina de Tecnologías de la Información cuando se detecte riesgo alguno real o potencial sobre las herramientas tecnológicas utilizadas, tales como, comportamientos anormales del sistema, derrames de agua, choques eléctricos, caídas o golpes o peligro de incendio.
10. Los colaboradores tienen la obligación de proteger las herramientas tecnológicas que se encuentren bajo su responsabilidad, aun cuando no se utilicen.
11. Los colaboradores no deben mover o reubicar las herramientas tecnológicas asignadas, instalar o desinstalar dispositivos, ni retirar sellos de los mismos, sin la autorización de la Oficina de Tecnologías de la Información, en caso de requerir este servicio deberá solicitarlo.
12. Las herramientas tecnológicas asignadas, deberán ser para uso exclusivo del ejercicio de las funciones asignadas a los colaboradores o personal de honorarios de la universidad Anahuac Oaxaca.
13. No se deberán consumir alimentos o ingerir líquidos mientras se operan las herramientas tecnológicas asignadas.
14. El colaborador debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos. En caso de que no se cumpla, solicitar el ordenamiento de cables con el personal de la Oficina de Tecnologías de la Información.
15. Se prohíbe que un colaborador distinto al personal de la Oficina de Tecnologías de la Información abra, destape o manipule las herramientas tecnológicas que sufran daños.
16. Todos los colaboradores que hagan uso de equipos de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.
17. Los requerimientos de servicios e incidentes de TI deberán ser escalados por la Mesa de Servicio al profesional especializado de la Oficina de Tecnología de la Información, de acuerdo a las políticas que se definan al respecto.
18. Los suministros serán instalados sobre la base de canje (se retira el elemento dañado y se reemplaza por otro en perfectas condiciones). Por ningún motivo puede retirarse un equipo o parte de él sin que se deje su respectivo reemplazo. Manejando un soporte sistematizado de control de las partes o equipos

cambiados donde quede registrado el historial de los ajustes realizados a la máquina.

19. El área de servicios de tecnología prestara los servicios técnicos de lunes a viernes de 7:30 am a 6:00 p.m. y sábados de 9:00 am a 2:00 pm.

DESCRIPCIÓN DEL PROCEDIMIENTO						
#	ACTIVIDAD / TAREA ¿QUÉ?	DESCRIPCIÓN ¿CÓMO?	ÁREA RESPONSABLE	CARGO	ÁREA PARTICIPANTE	REGISTRO
1	Registrar el incidente	Al recibir la solicitud, el técnico o el profesional asignado registra y analizada por tipo de caso dentro de los tiempos establecidos en las políticas de operación del presente procedimiento, dicha solicitud se registra, para su correcta gestión y control.	Área de servicios tecnológicos	Técnico y/o Profesional	Todas las áreas de la universidad	Bitácora de incidentes
2	Identificar incidente	Punto de entrega del incidente reportado, el Analista y/o Profesional de nivel 1 analiza el incidente basado en los lineamientos de coherencia, claridad y completitud de incidentes.	Área de servicios tecnológicos	Técnico y/o Profesional	Todas las áreas de la universidad	
3	Registrar y Validar incidente	Se recibe el incidente validado, para registrar la información básica necesaria para el procesamiento del incidente como: hora, descripción, sistema afectado y usuario que lo reporta. En los casos en que sea un incidente proveniente de otros procesos, la información relacionada al requerimiento debe ser incluida en el incidente.	Área de servicios tecnológicos	Técnico y/o Profesional	Todas las áreas de la universidad	

4	Diagnosticar y asignar nivel de prioridad	Se realiza un diagnostico al incidente registrado, en el que se determina si es un incidente mayor basado en el impacto que representa para el funcionamiento del área afectada. En el momento que se presente un incidente mayor, el soporte técnico deberá escalarlo al profesional para realizar un tratamiento especial. En los casos en que el diagnostico indique que el incidente no representa un alto riesgo, se deberá validar si el incidente puede ser atendido en nivel 1 o si por el contrario el incidente deber ser escalado a un segundo nivel de servicio. Para realizar de forma acertada el diagnóstico y análisis del incidente el profesional deberá emplear el documento guía Prestación Del Servicio.	Área de servicios tecnológicos	Técnico y/o Profesional	Oficina de Tecnología de la Información	
5	Resolver incidente en nivel 1	Se realizan las actividades requeridas para dar solución al incidente en un primer nivel de servicio incluyendo el soporte en sitio, lo anterior, se puede consultar en la Base de Datos de conocimiento que se encuentra ubicada en la carpeta del servidor Z de la universidad.	Área de servicios tecnológicos	Técnico y/o Profesional		
6	Realizar cierre de incidente	Se debe documentar la solución del incidente y la solución brindada, así como se debe alimentar la Base de Datos de Conocimiento en la carpeta del servicio correspondiente en el servidor Z.	Área de servicios tecnológicos	Técnico y/o Profesional		

7	Verificar satisfacción del usuario	Se debe notificar mediante un correo electrónico la solución del incidente al usuario, este debe notificar por el mismo medio su aceptación a la solución del incidente reportado o su inconformidad con el servicio. Si el usuario no manifiesta su aceptación en 48 horas posteriores a la solución del caso, se cerrará automáticamente el caso.	Área de servicios tecnológicos	Técnico y/o Profesional	Todas las áreas de la Universidad	Correo electrónico institucional
8	Escalar incidentes mayor	Dado el impacto económico técnico y funcional que representa un incidente mayor para la universidad, técnico o profesional escalará el incidente y seguirá los lineamientos establecidos en procedimiento de Gestión de Problemas, para que allí sea atendido por un grupo especializado y se tramite su solución.	Área de servicios tecnológicos	Analista y/o Profesional		
9	Escalar incidente a nivel 2	Los incidentes que no puedan ser resueltos por el primer nivel de servicio por agotamiento del tiempo de respuesta o por solución fuera de alcance del analista, deberán ser escalados a nivel 2 de servicio para recibir atención de un profesional especializado. El escalamiento de incidentes debe ser informado al analista o profesional, para su monitoreo continuo hasta el cierre del mismo o tomar acciones si se requiere un escalamiento a un nivel superior.	Área de servicios tecnológicos	Analista y/o Profesional		

10	Realizar investigación del incidente nivel 2	Se debe realizar una investigación de las causas que generaron el incidente, asignar el grupo de soporte especializado para los temas relacionados con el incidente y determinar sus tiempos de respuesta. Para los incidentes que requiera atención de diferentes especialistas, se debe generar una orden de trabajo (Clasificación y distribución del incidente) por medio de la cual se involucren otras áreas operativas y así disponer de los recursos que demande el incidente.	Área de servicios tecnológicos	Analista y/o Profesional		
11	Planear solución	Se define del plan de acción para la solución de incidentes escalados a segundo nivel de servicio, identificando los grupos especializados que deben intervenir para la solución del incidente. Dentro del plan de acción se debe realizar la definición de actividades con roles claves para la ejecución del plan de acción. En caso de no encontrar una solución para el incidente se debe realizar una evaluación en la que se determine si es necesario escalar el incidente al fabricante o si debe emplearse los lineamientos establecidos en el procedimiento de Gestión.	Área de servicios tecnológicos	Analista y/o Profesional		Plan de acción.

12	Notificar incidente al fabricante	En el momento que se determine que el incidente no puede ser atendido por el profesional asignado, se remite al fabricante para buscar y solucionar el incidente.	Área de servicios tecnológicos	Analista y/o Profesional		
13	Resolver incidentes en nivel 3	Se realizan las actividades por parte del proveedor para dar solución al incidente, en este nivel de servicio el proveedor con el apoyo de los profesionales asignado, se encarga de resolver el incidente y posteriormente se notifica, mediante correo electrónico institucional para las gestiones de cierre del incidente.	Área de servicios tecnológicos	Analista y/o Profesional		Correo Electrónico institucional
14	Escalar incidentes a gestión de problemas	En caso que el proveedor/fabricante no encuentre una solución para el incidente, este deberá ser escalado y seguirse los lineamientos del procedimiento Gestión de Problemas para investigar en conjunto con especialistas del nivel 2 y el proveedor/fabricantes una solución al problema.	Área de servicios tecnológicos	Analista y/o Profesional - Fabricante		
15	Monitoreo de incidentes	Para el monitoreo de incidentes se debe recorrer el histórico de incidentes y los incidentes activos, verificando sus diferentes acuerdos de nivel de servicio de TI, colas de incidentes de los diferentes asesores y su contenido para definir si se requiere o no realizar un escalamiento o reasignación	Área de servicios tecnológicos	Analista y/o profesional		

PUNTOS DE CONTROL					
ID	**NOMBRE DE LA ACTIVIDAD / TAREA**	**MÉTODO DE CONTROL**	**FRECUENCIA**	**RESPONSABLE**	**REGISTRO**
1	Registrar y actualizar la información	Cada movimiento que se lleva a cabo durante el inicio de la solicitud, los avances, los desarrollos, los seguimientos y la solución del requerimiento deben ser registrados en la carpeta del servicio correspondiente en el servidor Z.	Cada vez que se requiera	Encargado del servicio	
2	Verificar satisfacción del usuario	Se debe notificar mediante un correo electrónico la solución del incidente al usuario, este debe notificar por medio del correo institucional su aceptación a la solución del incidente reportado o su inconformidad con el servicio. Si el usuario no manifiesta su aceptación en 48 horas posteriores a la solución del caso, se cerrará automáticamente el caso.	Cada vez que se requiera	Todos los colaboradores de las diferentes áreas	

7.-Validación y prueba de la entrega.

7.1 Memoria técnica

Se encuentra en el documento adjunto en esta carpeta.

7.2 Definición de la fase de transición del servicio (ST)

Introducción

Por medio de la fase de transición del servicio se asegura que: en el ciclo de vida del servicio, toda la modificación cumpla con las expectativas del negocio. Este significa: que los servicios ya sean nuevos, modificados, o bien, retirados, deben cumplir con las expectativas del negocio y las del usuario/cliente que se han descrito en la fase de diseño. Con base a lo anterior se requiere:

- Una excelente administración de los conocimientos adquiridos.
- Una cultura organizacional.
- Una mentalidad de transición ante las circunstancias adversas.
- La búsqueda de beneficios competitivos.
- Mejores innovaciones del mercado, de agilidad. Objetivos
- Identificar los fundamentos de la fase de transición del servicio para generar una perspectiva general.
- Identificar los fundamentos de la fase de transición del servicio para generar una perspectiva general de su desarrollo.

Definición de la fase de transición del servicio (ST)

La fase de transición del servicio (ST) es una etapa en el ciclo de vida de un servicio, incluye una serie de procesos que son la guía para el desarrollo y la mejora de las capacidades para hacer la transición de servicios nuevos o modificados en ambientes que tienen soporte. Y se asegura que los servicios nuevos, modificados o retirados satisfagan las expectativas del negocio, tal como se documenta en las etapas de estrategia y diseño del servicio dentro de su ciclo de vida. La transición de servicio incluye los siguientes procesos: planificación y soporte a la transición, gestión del cambio, gestión de activos y servicios y configuración, gestión de liberación e implementación, validación y pruebas de servicio, y evaluación de cambios. Con base a lo anterior es importante mencionar que: aunque estos procesos están asociados con la transición del servicio, la mayoría de ellos tienen actividades que se desarrollan en varias etapas del ciclo de vida del servicio.

Guía para el desarrollo y la mejora de las capacidades para hacer la transición de servicios nuevos o modificados en ambientes que tienen soporte.

Propósito Asegurar que los servicios nuevos, modificados o retirados, cumplan con las expectativas del negocio tal y como fueron documentados en las fases de estrategia del servicio y de diseño del servicio. Objetivos

- Planear y gestionar los cambios del servicio de manera eficiente y efectiva.
- Gestionar los riesgos relacionados con los servicios nuevos, cambios y retiros de servicios.
- Implementar con éxito versiones dentro de los ambientes soportados.
- Establecer expectativas correctas del desempeño y del uso de servicios nuevos o modificados.
- Asegurar que los cambios de servicios creen el valor esperado en el negocio.
- Proporcionar una buena calidad del conocimiento e información acerca de los servicios y activos del servicio.

Alcance

Proporcionan la guía para desarrollar e implementar capacidades para la transición de nuevos servicios y cambios de servicios en sus ambientes de operación, incluye la planeación del despliegue, creación, pruebas, evaluación y entrega.

Valor del negocio

- Permite estimar costos, tiempos, requerimientos de recursos y riesgos asociados a transición del servicio.
- Volúmenes más altos de cambios exitosos.
- Facilita la adopción y seguimiento.
- Permite compartir y reutilizar los activos de la transición del servicio.
- Reduce retrasos en conflictos y dependencias.
- Reduce esfuerzos en gestionar la prueba de transición del servicio y pilotos.
- Mejora el establecimiento de expectativas para todo interesado.
- Aumenta la confianza en la entrega del servicio nuevo o cambio en el servicio, sin afectar otros servicios o interesados.
- Asegura que el servicio nuevo o cambio en el servicio sea fácil de mantener y rentable.
- Mejora el control de activos de servicio y configuración.

Roles

– Propietario del servicio

– Gerente de transición del servicio

– Dueño y gerente del proceso de:

- Planificación de la transición y soporte.
- Gestión de cambios.
- Gestión de activos de servicio y configuración.

- Gestión de liberación e implementación.
- Validación y pruebas del servicio.
- Evaluación de cambio.
- Gestión del conocimiento.

Alcance

- La gestión de ciclo de vida de cada elemento de configuración.
- Las relaciones con proveedores de servicio interno y externo.

Actividades

- Gestión y planeación.
- Identificación de configuración.
- Control de configuración.
- Contabilización e informe de estado.
- Verificación e informe de auditoria

8.- Operación del Servicio.

Gestión de incidentes

Objetivo

El Objetivo del presente documento es proporcionar información detallada sobre el proceso de gestión de incidentes que desarrolla el área de servicios de Tecnología de la Universidad Anahuac Oaxaca para todas las áreas que la integran.

- El Objetivo del presente documento es proporcionar información detallada sobre el proceso de gestión de incidentes que desarrolla el área de servicios de Tecnología
- El proceso en sí, nos permitirá restaurar la operación normal de los servicios y sistemas en producción, reduciendo al mínimo el impacto adverso en las operaciones del negocio, asegurando su continuidad y manteniendo los niveles acordados de calidad y disponibilidad del servicio.

Alcance

- El presente documento cubre todo incidente relacionado con los servicios brindados por el área servicios de Tecnología de la Información desde el registro de la ocurrencia hasta su solución y cierre definitivo.

Procesos Descritos

El presente documento contiene la descripción del Proceso de Gestión de Incidentes, que contiene a los siguientes subprocesos:

ST01Registro y Clasificación

ST02 Investigación y Diagnóstico

ST03 Solución, Recuperación y Documentación

ST04 Validación y Cierre

ST05 Seguimiento y Verificación del proceso

Políticas

- El área de Servicios de tecnología será el único punto de contacto con los usuarios para la recepción de reportes de incidentes.
- Todo incidente tendrá un dueño, siendo el personal del área de servicios tecnológicos quienes recibirán el incidente y le darán seguimiento hasta su solución y cierre.
- El Gestor de Problemas es quien hace seguimiento a los problemas generados en este proceso.
- El Gestor de Cambios hará seguimiento de los RFCs generados en este proceso.

Todo incidente debe ser revisado e informado desde su registro hasta su solución definitiva por el área de servicios de tecnología pretendiendo al mínimo el impacto adverso en las operaciones del negocio, asegurando su continuidad y manteniendo los niveles acordados de calidad y disponibilidad del servicio.

Procesos de gestión de incidentes

Los procesos definen conjuntos de actividades que son realizadas por parte del área de servicios de tecnología independientemente de que se esté respondiendo a un incidente o no. Los procesos que la política deberá definir comprenderán al menos los siguientes aspectos:

Proceso de planificación y preparación para enfrentar incidentes de seguridad El proceso de preparación incluye todas aquellas actividades de tipo proactivo que puedan llevarse a cabo para estar mejor preparado para responder y enfrentar incidentes.

Estas actividades incluyen items como:

• Análisis de alertas y amenazas

• Actividades de sensibilización

• Actividades de entrenamiento

• Ensayos y evaluaciones de seguridad

• Definición de procedimientos

• Análisis y mejora continua del proceso

Proceso de atención a incidentes

El proceso de atención a incidentes agrupa todas las actividades de tipo reactivo que se realizan como parte de la respuesta a un incidente concreto.

Este proceso incluirá items como:

• Recepción de reportes de incidentes

• Clasificación y valoración de impacto

• Elaboración de un plan de respuesta al incidente con medidas de contención y mitigación recomendadas.

• Elaboración de un informe final de cierre

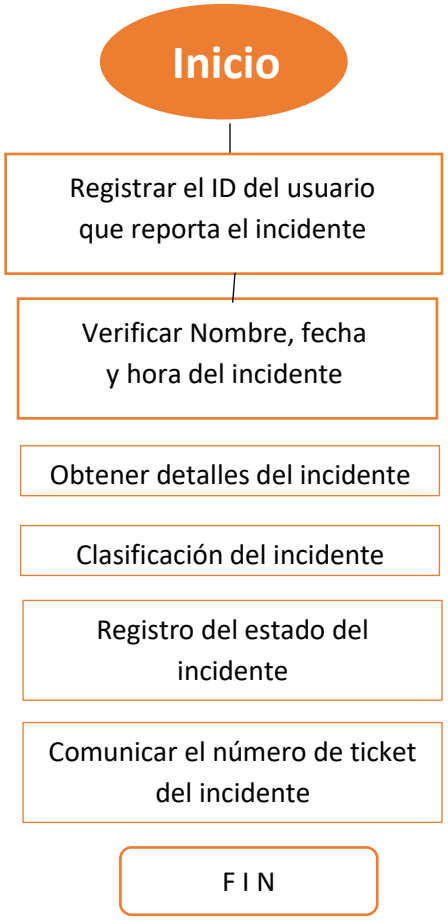


Diagrama del subproceso de registro y clasificación

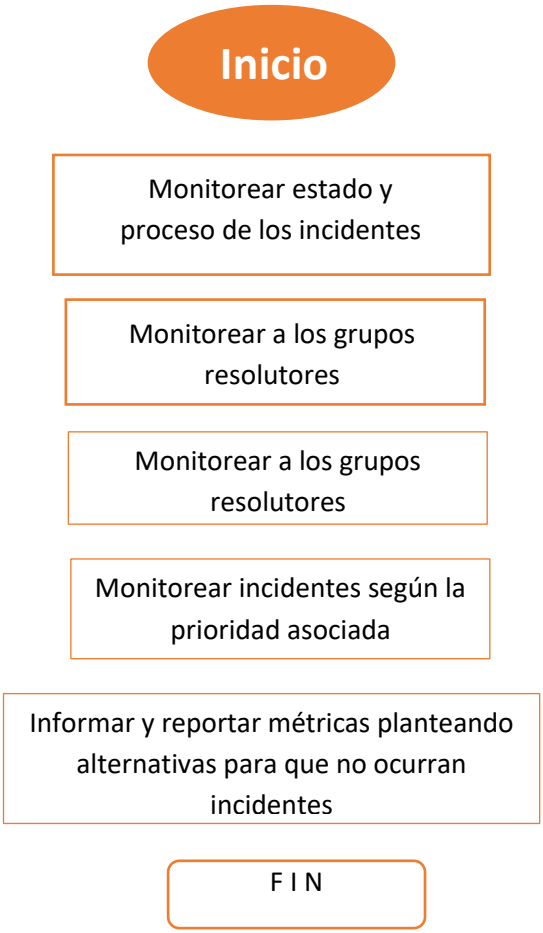


Diagrama del subproceso de seguimiento y verificación del proceso

Proceso de mejora continua para enfrentar futuros incidentes

El proceso de mejora continua agrupa todas las actividades que serán realizadas por parte la entidad afectada por el incidente para mejorar su postura de seguridad para enfrentar futuros incidentes. La experiencia adquirida en la atención al incidente, así como toda la información obtenida durante el curso de la acción podrá permitir la elaboración de un plan de acciones de mejora a implementar por la entidad afectada. El objetivo de este plan de acciones no deberá ser en ningún caso un objetivo de auditoría o de búsqueda de responsables si no que el objetivo deberá ser el de fortalecer a la organización para evitar la repetición de incidentes similares en el futuro.

Métricas del Proceso

Para este proceso se considerarán las siguientes métricas por cada periodo:

a. Número total de incidentes clasificados por tipo de prioridad reportados.
b. Número de incidentes asignados a grupos de soporte clasificados por tipo de prioridad.
c. Porcentaje de incidentes solucionados de acuerdo al SLA por tipo de prioridad.

Welcome kit

Ing.

P r e s e n t e

Estimado Ingeniero

Antes que nada agradecemos la oportunidad que nos brindan de hacerles llegar la presente propuesta de **"Meraki"** con la que buscamos ayudar a implementar las mejores prácticas en redes y los equipos Cisco Meraki les permitan mantener en óptimo funcionamiento la red Inalámbrica de **UNIVERSIDAD ANAHUAC** asegurando con esto un rápido retorno en la inversión de la infraestructura Cisco.

La solución propuesta tiene la finalidad de cubrir el requerimiento de **UNIVERSIDAD ANAHUAC** permitiendo con ello brindar cobertura inalámbrica a los usuarios que desempeñaran sus tareas con dispositivos móviles o Laptops, asegurando un mejor desempeño en sus actividades.

Hoy en día, en esta nueva era de la información, resulta de gran importancia mantener las comunicaciones y la eficiencia del negocio ante los retos externos y las cambiantes condiciones del mercado. Esto obedece a que precisamente las presiones por ser más competitivo, productivo son cada vez mayores y que estas mejoras operativas se traducen en dinero para la empresa, ya sea en mayores ingresos o en menores gastos. Ya sea por protección de activos ante imponderables o por la continua búsqueda de mejoras operativas, apreciamos la oportunidad que nos brindas de trabajar con usted y queremos reiterar nuestro interés en ser sus socios tecnológicos para la ejecución e incluso definición de las estrategias de **UNIVERSIDAD ANAHUAC** en el presente y futuro.

Ing. Alan Alvarado Valero

CISCO SYSTEM ENGINEER

Formato de Reporte de servicio

Fecha: _____

Hora: _____

Nombre de quien reporta:
Área:
Puesto:

Tipo de Reporte

Computadora	Impresora	Red de Voz	Red local	Correo electrónico	Windows	Office	Otro

Describa brevemente la solicitud del servicio

¿Se había solicitado con anterioridad este servicio?

NO			
SI		FECHA	

Solución y observaciones

Acepta como terminado el servicio: SI NO

Fecha de la finalización del reporte: _____

Servicio realizado por: _____

Firma del solicitante de conformidad: _____

9.-Valor del Servicio

Gestión de Incidentes

Introducción

Objetivo del documento

El presente forma parte del Sistema de Gestión de Servicios del área de servicios de tecnología, y se ubica dentro de los procesos de operación. Específicamente en este documento encontrara la descripción detallada del proceso de Gestión de Incidentes, con el objetivo de estandarizar la atención hacia los clientes que en este caso son el personal administrativo, alumnos y profesores, estableciendo modelos de atención apegados a las mejores prácticas.

Definición del Proceso

Misión

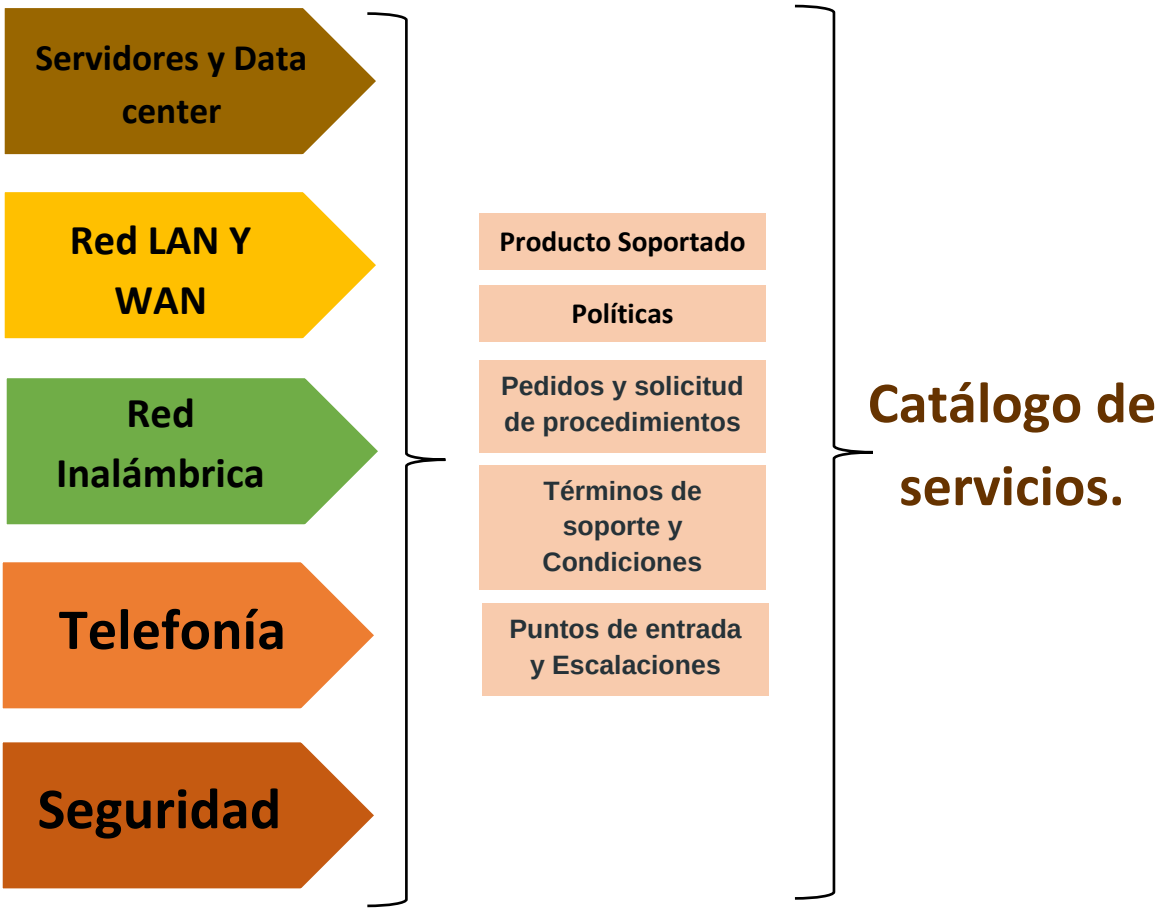
Actuar apegados a los lineamientos establecidos dentro de las políticas del área de servicios de tecnología para dar solución inmediata a los incidentes presentados durante la operación del servicio, manteniendo los niveles más altos en los indicadores de atención al cliente y superando las expectativas a cubrir por los acuerdos de niveles de servicio.

Objetivo

El objetivo principal de la gestión de incidentes se basa en restaurar el servicio a normal lo más rápido posible con la menor afectación a nuestros clientes y responder eficientemente a las peticiones de servicio.

Alcance

Este procedimiento cubre la atención de incidentes de los servicios definidos en el catálogo de servicios;



La atención de incidentes se da conforme a los puntos establecidos dentro de los Acuerdos de Niveles de Servicio.

Conceptos Clave

Incidente. - Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio.

SLA (Service Level Agreement).- Acuerdo de Nivel de Servicio, es un acuerdo entre un proveedor de servicios de TI y un cliente, el SLA describe el servicio de TI, documenta los objetivos del nivel de servicio y especifica las responsabilidades del proveedor de servicios de TI y el Cliente, un único SLA puede cubrir múltiples servicios de TI o varios clientes

RMA (Return Merchandise Authorization).- Autorización de devolución de mercancía, usado en distribuidores o corporaciones, para la transacción por el retorno de un producto por defectos para luego repararlo o reemplazarlo o hacer una nota de crédito para la compra de otro producto. Algunos distribuidores contratan a empresas privadas para realizar esta tarea.

Problema. - Una causa de uno o más incidentes. La causa suele no ser conocida en el momento de que un registro de problema se crea, el proceso de gestión de problemas es el responsable de una investigación más profunda.

Prioridad. - Una categoría utilizada para identificar la importancia relativa de un Incidente, Problema o Cambio. La prioridad se basa en el impacto y urgencia, y se utiliza para identificar las horas necesarias para las acciones que deban tomarse. Por ejemplo, el SLA puede afirmar que la prioridad 2 incidentes deben ser resueltos dentro de las 12 horas.

Impacto. - Una medida del efecto de un incidente, problema o cambio en los procesos del negocio. Impacto a menudo se basa en cómo los niveles de servicio se verán afectados. Impacto y urgencia son usados para asignar prioridad.

Urgencia. - Una medida de cuánto tiempo pasará hasta que un incidente, problema o cambio tenga un impacto significativo en el negocio. Por ejemplo, un incidente de alto impacto puede tener una urgencia baja, si el impacto no afectará el negocio hasta el final del ejercicio. Impacto y urgencia se utilizan para asignar prioridad.

Escalación. - Una actividad que obtiene recursos adicionales cuando éstos son necesarios para cumplir con objetivos de nivel de servicio o las expectativas del cliente. La escalación puede ser necesaria en cualquier proceso de gestión de servicios TI, pero es más comúnmente asociada con la Gestión de Incidentes, Gestión de Problemas y la gestión de quejas de los clientes. Hay dos tipos de escalación, escalación funcional y escalación jerárquica.

Petición. - Petición que hace un usuario solicitando información, asesoramiento, un cambio estándar o acceso a un servicio de TI.

CMDB. - Base de datos de la gestión de la configuración la cual es usada para almacenar los registros de configuración durante todo su ciclo de vida. Esta CMDB debe contener los atributos de CIs y relaciones con otros CIs.

Incidentes graves. - es la categoría más alta de impacto para un incidente. Un incidente grave tiene como consecuencia una interrupción importante en el negocio.

Tiempos de resolución. - Tiempo empleado en la resolución de los incidentes y que sirve para revisar el cumplimiento de los SLA.

Error conocido. - Problema que posee una causa raíz documentada y una solución temporal. Los errores conocidos son creados y gestionados a través de su ciclo de vida por la gestión de problemas. Los errores conocidos pueden ser identificados también por desarrollo o suministradores.

Ticket. - Registro de una solicitud o reporte de incidente el cual es identificado por un único ID asignado en manera consecutiva por nuestra herramienta de gestión de incidentes.

RFC. - Propuesta formal para que se realice un cambio. Un RFC incluye detalles del cambio propuesto, y puede registrarse en papel o electrónicamente. El termino RFC se suele confundir con registro del cambio, o con el cambio en sí.

Entradas del proceso

Las principales entradas en el proceso de atención de incidentes son las siguientes: En primer término, las que son de contacto directo con el usuario, para lo cual se cuenta con los medios que a continuación se listan:

Medio	Datos	Detalles
Vía telefónica	5016250 ext. 1400, 1401, 1402 y 1403	Estas extensiones pertenecen a los integrantes del equipo de servicios de tecnología de la universidad Anahuac
Vía correo electrónico	Jorge.gomez@anahuac.mx diego.meinguer@anahuac.mx	Las direcciones de correos electrónicos que

	Isaac.ramos@anahuac.mx Agripino.garcia@anahuac.mx	se muestran son de atención directa y están siendo supervisados permanentemente

Base de datos de incidentes. - La base de datos de incidentes tiene la finalidad de almacenar el proceso completo por el que cada incidente ha pasado, verificar que no exista duplicidad en la creación de algún incidente, es también un apoyo para la identificación de incidentes similares creados con anterioridad y la solución aplicada.

Base de datos de problemas. - En la atención de incidentes resulta de vital importancia que esta información se encuentre disponible, ya que ayudará para poder identificar si el incidente que se está atendiendo es provocado por un error conocido, de resultar positivo el grupo de atención de primer nivel tiene la oportunidad de saber la forma de solucionarlo sin recurrir a la atención de personal de los grupos especializados, esto reducirá considerablemente el tiempo de atención.

Memoria Técnica. Es el documento que se genera por los departamentos de ingeniería de redes e ingeniería de infraestructura, resultado de la implementación o fase final del proyecto. En este se describen con detalle las especificaciones técnicas, de configuración, de equipo, inventarios, direccionamiento, pruebas y todos los puntos acordados con el cliente. Este documento es entregado en copia al departamento de tecnologías y sirve como referencia para la administración de las configuraciones realizadas en la implantación de la solución.

Comunicación al usuario del incidente resuelto. - Información de salida hacia el usuario para mantener informado sobre el estado del incidente o bien al final para confirmar su resolución.

Base de datos de incidentes. - Se obtiene como salida una base de datos con los incidentes registrados y tratamiento realizado.

Roles y sus responsabilidades

Roles	Responsabilidades
Gestor de incidentes	Responsable de que los incidentes de usuarios se atiendan de manera eficiente y dentro de los márgenes de tiempo establecidos en los acuerdos de nivel de servicio — Seguimiento a todas las actividades del proceso — Seguimiento a las métricas del proceso — Coordinación de las actividades del grupo de soporte — Funge como enlace para escalado de incidentes — Monitorizar el proceso y hacer recomendaciones para la mejora — Elaborar la información de gestión del proceso
Teleoperador	Atención y registro de incidentes recibidos a través de los medios de contacto con el usuario (vía telefónica o vía email), generación del ticket para su atención — Resolución de consultas sencillas — Clasificación de incidentes — Tramita peticiones o solicitudes de servicio de los usuarios y los mantiene informados — Realiza un escalado funcional a la siguiente línea de soporte de los incidentes que no puede resolver — Resuelve o escala de manera funcional loe eventos
Analistas	Forman el grupo de especialistas de 1er. Nivel — Responsable de realizar 1er análisis, diagnóstico y resolución de incidentes. — Escalar la incidencia al siguiente nivel de soporte cuando no pueda resolver
Especialistas de soporte	Resolver la incidencia escalada del segundo nivel de soporte — Encargados de la resolución en sitio de incidencia que no pueden resolverse de forma remota — Encargados de resolver de forma personal las solicitudes de servicio de usuarios de nivel directivo — Incluidos en este nivel distribuidores y fabricantes a quienes podría ser escalado un incidente
Administración y soporte al proceso del incidente	— Impulsar el trabajo en conjunto de los equipos ante la aparición de una incidencia crítica verificando que se cumplan los acuerdos de nivel de servicio — En caso de ser necesario coordina la escalación de incidentes entre los grupos

Matriz RACI

Las matrices de asignación de responsabilidad, o RACI, son así denominadas por las cuatro letras con las que se codifica el tipo de relación con un proceso que tiene cada agente:

- R: Responsable. Es el que se encarga de hacer la tarea o actividad.
- A: Persona a cargo. Es la persona que es responsable de que la tarea esté hecha. No es lo mismo que la R, ya que no tiene porqué ser quien realiza la tarea, puede delegarlo en otros. Sin embargo, si es quien debe asegurarse de que la tarea sea haga, y se haga bien.
- C: Consultar. Los recursos con este rol son las personas con las que hay consultar datos o decisiones con respecto a la actividad o proceso que se define.
- I: Informar. A estas personas se las informa de las decisiones que se toman, resultados que se producen, estados del servicio, grados de ejecución.

Actividades	Gestor de Incidentes	Teleoperador	Analistas	Especialistas de Soporte	Admón. y soporte al proceso del incidente
Recepción y validación de Información para alta de cliente	I				CA
Solicitud de información faltante para alta de cliente, en caso de ser necesario	I				CA
Aceptación de cliente y fecha de liberación.	I				CA
Generación de cuenta de administración de incidentes para cliente	A	I	I		
Captura datos cliente en sistema de administración de procesos e inventarios.	I	I	R		
Alta de equipos a sistemas de monitoreo, en caso de aplicar	I	I	R		
Registro de SLA y configuración para ser utilizadas para el cliente.	CA	I	I		

Proporcionar información de administración y direccionamiento a analistas de atención	CA	I	I		
Realizar explicación de proyecto a todos los involucrados	CA	II	I		R
Informar a áreas solicitantes el alta del cliente y liberación	CA		I		I
Definir los criterios para la creación de un incidente mayor	A	I	I		C
Autorizar escalado jerárquico	A				C
Actualización de información por cambios realizados durante la operación	C				
Proporcionar información a cliente para la administración de incidentes y sitio de almacenaje de reportes.	C				I
Recepción, clasificación, priorización y registro de incidentes recibidos a través de llamadas telefónicas, e-mail, y mensajería		R			
Asignación de incidentes		R			
Realizar el primer diagnóstico de incidentes recibidos					
Solución de Incidentes de primer nivel					
Dar solución a consultas sencillas	C	R			
Dar trámite a solicitudes o peticiones de servicio	C	R			
Realizar cierre de incidente	C				
Realizar escalado del tipo funcional	A				
Solicitar escalado de tipo jerárquico	A				I
Asistir a reuniones con la áreas internas y externas involucradas en el proceso	A				C
Revisión de los informes obtenidos y realización de una comparativa contra SLA					

Realizar un informe sobre la gestión o administración del proceso	R				I
Supervisión de la atención de incidentes	CA				I
Informar al siguiente nivel jerárquico sobre el seguimiento, pérdida o degradación de los servicios comprometidos	A				C
Realizar informes sobre, desviaciones, incumplimiento o tendencias relacionadas con los SLA	A				IC
Realizar los informes basados en los resultados obtenidos de la operación	A				
Atención de incidentes escalados de manera funcional	C				
Diagnóstico, resolución y comprobación de incidentes escalados a 2º nivel	C			C	
Seguimiento a incidentes escalados de manera funcional	A			R	C
Atención en sitio a incidentes de clientes que no pudieron ser resueltos de forma remota				R	I
Atención personalizada de usuarios de primer nivel de los clientes registrados				R	I
Respuesta al CSS sobre la solución implementada usando los mecanismos, formatos o formas establecidos					
Alimentación de la base de conocimientos					
Actualización de cambios relacionados con los activos del cliente	I				C
Presentar informes a cliente en la primera entrega de resultados	I				I

Actualización de cambios relacionados con los activos de la empresa	C				

Métricas del proceso

Las métricas definidas para la medición de la atención de incidentes y solicitudes de servicio son:

1	Nombre	Número de incidentes por día, lapsos de una semana de operación
	Área de éxito	Atención de incidentes
	Factor crítico de éxito	Cantidad de incidentes generados por día
	Objetivo	Mostrar el número de casos registrados por el CSS en la herramienta de gestión de incidentes.
	Descripción	Esta resulta del conteo simple de incidentes registrados por día en la bitacora de gestión de incidentes.
	Origen de datos	Los datos serán obtenidos directamente de la bitácora de gestión de incidentes.
2	**Nombre**	**Origen de incidentes(Medio de recepción)**
	Área de éxito	Atención de incidentes
	Factor crítico de éxito	Cantidad de incidentes generados medio de contacto
	Objetivo	Establecer mayor énfasis en los medios con mayor utilización.
	Descripción	Esta resulta del conteo simple de incidentes registrados en la herramienta de gestión de incidente.
	Origen de datos	Los datos serán obtenidos directamente de la bitácora de gestión de incidentes.
	Metas	Verificar cuales son los medios de comunicación con mayor recurrencia por los clientes al comunicarse al área de servicios de tecnología, para poder reforzar los recursos asignados a ese medio con la finalidad de proporcionar un servicio de mayor calidad al cliente.
3	**Nombre**	**Origen de incidentes (cerrados/en espera/abiertos)**
	Área de éxito	Atención de incidentes
	Factor crítico de éxito	Cantidad de incidentes cerrados en tiempo y forma
	Objetivo	Lograr el mayor número de incidentes resueltos en soporte de primera línea.

	Descripción	Esta resulta del conteo simple de incidentes registrados en la herramienta de gestión de incidente.
	Origen de datos	Los datos serán obtenidos directamente de la bitácora de gestión de incidentes.
	Metas	Verificar la correcta clasificación de los incidentes logrando así información verídica a la toma de decisiones.

Políticas

- Todos los incidentes deberán ser registrados.
- El cliente debe ser informado de en todo momento del seguimiento de sus solicitudes o incidentes reportados.
- Emprender actividad post-incidentes, como hacer mejoras al proceso y asegurar la retención de evidencias.
- Asignar y dar autoridad necesaria al encargado del inocente del proceso para asegurar que el proceso de Incidentes se mantenga a lo acordado.
- Todo el personal del área de servicios de tecnología tiene que cumplir con el seguimiento al proceso.
- Se debe mantener respaldo de toda la evidencia.
- Todo incidente o solicitud deberá cerrarse hasta el momento en el que el cliente confirme la autorización del caso.

Procedimiento Alta de incidente

El presente procedimiento tiene el objetivo de establecer los pasos a seguir para realizar el registro de un incidente o solicitud en la herramienta de gestión de incidentes y solicitudes.

1. Las solicitudes se aran enviando un correo a la cuenta soporte.uao@anahuac.mx desde sus correos institucionales proporcionados anteriormente o llamando a las extensiones 1400,1401, 1402 y 1403.
2. Si la solicitud se realiza vía correo electrónico deberá indicar cuál es el problema, tiempo que lleva con el problema y si es necesario una captura de pantalla o documento del problema.

10.-
Documentación de un problema

Perfil de Puesto "Especialista en Infraestructura"

- **Habilidades Técnicas**
  - Conocimiento en redes
    - Configuración de switches marca extreme, cisco y 3com
    - Cableado estructurado
    - Mantenimiento y actualización de equipos en sites
  - Conocimiento en servidores DELL y LENOVO
    - Instalación e implementación
  - Conocimiento SQL Server
  - Conocimiento de paquetería de Microsoft Office
  - Conocimientos básicos en seguridad
    - Definición de políticas
  - Administración de proyectos
  - Control de cambios
  - Conocimientos de Virtualización VMware y HyperV
  - Mantenimiento y Supervisión de video vigilancia
  - Conocimiento y funcionamiento de Firewall Fortinet
  - Mantenimiento y supervisión de Servidores de Directorio Activo, DHCP y DNS
  - Generación y revisión de reportes de los servicios de impresión y telefonía
  - Conocimientos básicos de telefonía Huawei
    - Configuración de extensiones
  - Conocimiento de Datacenter
    -

- **Habilidades No Técnicas**
  - Trabajo en equipo
  - Disponibilidad de horario

Métricas

- Tiempo de resolución en la primera línea
  - Soporte técnico 30 min – 1 hora
- Tiempo de solución del ticket
  - De acuerdo a los SLA comprometidos
- Tiempo que tarda en escalar un ticket
  - 24 horas
- Costo promedio de un ticket
  -
- Cuantos clientes caen en SLA
- Tiempo
- Número de llamadas que no son exitosas en un centro de soporte