UF1876: Atención a usuarios e instalaciones de aplicaciones cliente

Elaborado por: J. A. Jiménez Toro

Edición: 5.0

EDITORIAL ELEARNING

ISBN: 978-84-16199-14-3

Impreso en España - Printed in Spain

Presentación

Identificación de la unidad formativa:

Bienvenido a la Unidad Formativa **UF1876: Atención a usuarios e instalación de aplicaciones cliente.** Esta Unidad Formativa pertenece al Módulo Formativo **MF0963_3: Administración de servicios de comunicaciones para usuarios**, que forma parte del Certificado de Profesionalidad **IFCM0310: Gestión de redes de voz y datos**. Este contenido se integra en la familia profesional **Informática y comunicaciones**.

Presentación de los contenidos:

La finalidad de esta unidad formativa es enseñar al alumno a atender y gestionar incidencias y reclamaciones de usuarios correspondientes a los servicios de comunicaciones proporcionados, con el fin de garantizar sus prestaciones, y a instalar y configurar aplicaciones en equipos terminales de cliente para proveer servicios específicos de comunicaciones, según especificaciones recibidas y criterios de calidad de la organización.

Objetivos:

– Atender las incidencias producidas en la asignación y uso de los servicios y recursos de comunicaciones, de acuerdo a unas especificaciones dadas.

– Definir procedimientos de instalación de aplicaciones de comunicaciones en equipos terminales de acuerdo a especificaciones técnicas y funcionales.

Índice

UD1

Incidencias producidas en la asignación y uso de los servicios y recursos de comunicaciones

1.1. Alarmas y alertas. Significado
1.2. Herramientas específicas y técnicas de detección de incidencias en sistemas de comunicaciones
1.3. Procedimientos de diagnóstico y reparación de la incidencia
1.4. Tipos de incidencias
    1.4.1. Responsabilidad de la operadora
    1.4.2. Incidencias de usuario
    1.4.3. Incidencias del proveedor del servicio

1.1. Alarmas y alertas. Significado

En todas las redes comunicaciones se producen incidencias de diversa índole que perjudican a los usuarios de la red, este perjuicio puede afectar al rendimiento de los recursos o servicios de la red. Estas incidencias pueden ser divididas en dos tipos:

- **Anomalías:** define un comportamiento extraño o mal funcionamiento que afecta al rendimiento de un componente de la red pero no provoca un fallo en el componente. Las anomalías provocan unas pérdidas de rendimiento en los componentes afectados y el origen es debido a varios factores como puede ser:
    - Mal uso de un componente: los usuarios utilizan un componente de una forma correcta o en un uso para el cual no está diseñado.
    - Seguridad deficiente: las políticas de seguridad utilizadas por los usuarios son ineficaces, pueden provocar accesos no autorizados a un componente y utilizarlo para su provecho.
    - Mala configuración: la configuración de un componente no es óptima, provocando un funcionamiento anómalo.
- **Fallos:** define un error grave que provoca una pérdida de funcionamiento del componente, los factores expuestos anteriormente pueden provocar un fallo, otros factores pueden ser:
    - Fallo hardware: error en el hardware interno del componente provocado por una sobrecarga de tensión, rotura de un componente, golpe físico, incendio, etc.
    - Fallo software: error que provoca que un determinado software deje de funcionar, pueden ser provocados por errores de programación, fallos de diseño en el software, etc.

- Ataques informáticos: en este apartado podemos incluir, virus, troyanos, DDOS, etc., que utilizan algún error de seguridad en el sistema o aprovechan alguna vulnerabilidad, como un Zero Day, en el componente.

Las anomalías de funcionamiento deben ser controladas y resolverlas lo antes posible para que no conviertan un error grave que provoque un fallo y deje de funcionar un determinado recurso o servicio.

Un corte en el funcionamiento de un servicio, puede provocar pérdida económicas en la empresa proveedora. Una correcta monitorización de todos los componentes de la red puede detectar posibles anomalías en el funcionamiento de la red, analizando los datos y realizando las posibles actuaciones para resolver la situación.

Para controlar las posibles anomalías y fallos en la infraestructura de red, requiere una buena monitorización de los componentes de la red que permite realizar un control de su funcionamiento. Para detectar posibles errores en la red tenemos disponibles las alertas y alarmas.

ALERTAS	ALARMAS
Detecta un posible error en el sistema, tomando las medidas necesarias para resolverlo y que no derive en un error de mas gravedad.	Detecta un fallo grave en el sistema que puede provocar un daño grave en el funcionamiento de un componente de la red.

La principal diferencia entre las alertas y las alarmas es la gravedad del evento que ha servido para activarlo. Una alerta conlleva un estado de precaución para vigilar el evento activador, se debe resolver la alerta aunque no lleve una prioridad alta la resolución. En una alarma la acción prioritaria sea resolverla, porque a diferencia de una alerta, el evento que ha provocado la alarma sí está causando un daño en el funcionamiento de la red.

Por ejemplo una excesiva subida en el tráfico de la red a un determinado nivel activará una alerta y cuando se produzca una sobrecarga en la red por el exceso de tráfico activará una alarma.