INSTITUCION: ESCUELA SUPERIOR DE COMERCIO N°43

CARRERA: TECNICO SUPERIOR EN SOPORTE DE INFRAESTRUCTURA DE TECNOLOGIA DE LA INFORMACION

ESPACIO CURRICULAR: Integridad y Migración de Datos

CAMPO DE LA FORMACIÓN: Específica

CURSO: Tercer Año

CICLO LECTIVO: 2019

PROFESOR/A: Pratto Andrea Yanina

ASIGNACION HORARIA: 4 hs.

FORMATO: Taller

REGIMEN DE CURSADO: Anual

PLAN DECRETO: 2120/16

FUNDAMENTACION

El diagnóstico y solución de incidentes es una de las tareas primordiales de un administrador de infraestructuras

OBJETIVOS

CONTENIDOS

Unidad 1: Diagnóstico

Concepto de incidente, diferencia entre incidente y problema. Procedimientos para aislar o realizar cierres controlados de recursos de la infraestructura y su reactivación. Procedimientos de registro de incidentes y de las actividades necesarias para resolverlos. Información sobre disponibilidad y costos de recursos necesarios para el diagnóstico y solución de problemas. Trabajo en grupos "ad- hoc". Concepto de "Service Level Agreement", tiempos admisibles para una solución de problema. Normas ISO 20000 y bibliografía ITIL relacionadas con manejo de incidentes y problemas. Métricas de servicios de soporte.

Unidad 2: Riesgos

Calamidades naturales, accidentes catastróficos, sabotaje o ataques terroristas. Impacto de la interrupción de servicios sobre la organización, categorización de aplicaciones para establecer prioridades de restablecimiento.

Unidad 3: Plan de contingencia

Prioridades, sitios y proveedores alternativos: características, disponibilidad, costos, contratación, personal y suministros, desplazamientos, información a usuarios. Acciones y responsabilidades: recupero de archivos, restablecimiento del servicio, procedimientos adicionales de seguridad, registro de eventos.

Unidad 4: Evaluación de riesgos

Riesgos que afectan a la infraestructura física: incendios, suministro de energía, medios externos de comunicación, intrusos, catástrofes. Riesgos que afectan a la infraestructura lógica.

Unidad 5: Resolver casos de estudio

Prever y analizar riesgos, planificar actividades requeridas, prever los elementos que deban estar disponibles incluyendo los que permitan recuperar situaciones de inicio, diseñar instrumentos para control, preparar y testear plataformas, realizar scripts que automaticen actividades, preparar backups de las aplicaciones migradas, realizar un seguimiento inicial del rendimiento de los sistemas migrados.

ESTRATEGIAS METODOLOGICAS

RECURSOS

MODALIDADES DE CURSADO

EVALUACION

TALLER:

· Sólo admitirán el cursado regular presencial.

· 75% de asistencia a las clases áulicas.

· Aprobar el 100% de las instancias de evaluación previstas en la planificación anual, contemplando una instancia final de integración. La nota será de 6 (seis) o más sin centésimos.

· El estudiante que no haya aprobado podrá presentarse hasta dos turnos consecutivos inmediatos posteriores a la finalización de la cursada (Turno de diciembre y Feb/Marzo; o Julio y Diciembre)

BIBLIOGRAFIA

Normas ISO 20000 link:
https://www.proactivanet.com/images/Blog/ISO20000_GuiaCompletadeAplicacion_LuisMoran.pdf

ITIL

Finalidad Formativa

Esta unidad curricular permite a los estudiantes obtener herramientas que le posibiliten prever situaciones que puedan afectar el normal funcionamiento de la TI y diseñar planes de contingencia.

Práctica Formativa

Como parte de la forma de adquirir estos aprendizajes y demostración práctica de los resultados alcanzados, los estudiantes tienen que realizar en un mínimo del 33%, las siguientes actividades: Práctica de diagnóstico y solución, tanto en forma individual como grupal, en algunos casos asistida por docentes, de diversos tipos de incidentes y problemas de complejidad creciente preparados por docentes, tratando de respetar los tiempos admisibles. Realizar visitas a data centers para tomar conocimiento de sus condiciones y planes de contingencia. Discutir en clase la pertinencia del plan observado y proponer mejoras. En base a un caso de estudio, evaluar riesgos y proponer un plan de contingencia y secuenciar las acciones a realizar, simulando algunas de ellas en laboratorios. Implementar servicios de backup o espejados, respecto a procesos, equipos y datos, que se activen ante la contingencia ocurrida. Redactar instrucciones de procedimiento para planes de contingencia.

FUNCIONES QUE EJERCE EL PROFESIONAL

"Atender incidentes que afecten al Soporte de Jnfraestructura de TI, diagnosticar las causas que los originan y resolverlos o coordinar su solución

Esto implica:

• Identificar el problema que dio lugar al incidente y diagnosticar su origen o 9fl causa ifitima para generar una solución duradera.

• Establecer prioridades Para su solución, tomando en cuenta las posibles consecuencias del problema para la operatoria de la organización, administrando el problema.

• Planificar las acciones necesarias para resolver el problema o derivar a otros integrantes o a terceros las acciones necesarias para la soluciOn.

• Realizar las acciones necesarias, ya scan de emergencia o definitivas y coordinarlas con las que tienen que realizar otros integrantes del equipo o terceros.

• Verificar mediante pruebas que la solución implementada haya resuelto el problema. Para realizar esto el técnico analiza bitácoras de incidentes, eventualmente se contacta con quien denuncio el incidente para mejorar la especificacion del mismo y utiliza su capacidad anailtica y de diagnOstico para determinar el componente y condiciones en que se produjo y las causas que le dieran origen. Evaliia el impacto del problema sobre otros componentes de hardware a software y el de su persistencia sobre la operación de los sistemas para fijar prioridades de atención en función de las normas del servicio y su capacidad de negociación. Actüa conjuntamente con otros

integrantes de la organización o prestadores de servicios especializados, trabajando como un equipo, para completar el diagnOstico o dare solución tomando en cuenta la estructura lógica y fIsica de la instalación y las posibles consecuencias de sus acciones sobre otros componentes. En todo momento administra el problema y documenta las decisiones adoptadas, las acciones realizadas y el nuevo estado de la infraestructura a su cargo.

"Migrar o convertir sistemas, aplicaciones o datos tratando de minimizar riesgos para la seguridad y continuidad del servicio ".

Esto implica:

• Analizar todo lo que requiere instalarse, resguardarse, modificarse, trasladarse y recuperarse o poner en marcha, y testear para planificar o intervenir en la planificacion de las tareas a realizar.

• Prever contingencias y realizar ensayos 0 pruebas piloto pan asegurarse que lo planificado es adecuado.

• Acordar con la gerencia y usuarios fechas y condiciones de corte y reanudación para que organicen sus propias actividades.

• Coordinar con otros involucrados]as tareas del plan de migración.

• Desarrollar las acciones necesarias para realizar la migraciOn.

• Verificar el adecuado funcionamiento del sistema migrado antes de liberarlo a sus usuarios. Al realizar esto, el técnico actüa de acuerdo a 10 planificado por los responsables de los sistemas a migrar y el responsable de seguridad, coordinando eventualmente con proveedores de servicios especializados para determinar necesidades de componentes a su cargo y acciones a realizar. Coordina con la gerencia y comunica a los usuarios afectados sobre los momentos en que se afectara el servicio y eventuales consecuencias previsibles para que tomen las precauciones que correspondan. También coordina con la gerencia y el responsable de seguridad la disposición de los archivos de datos reemplazados. PIx-

"Entender en temas de contingencias y riesgos que puedan afectar a! Soporte de Infraestructura de TI"

Esto implica: Evaluar riesgos que puedan afectar a la continuidad del funcionamiento del sistema. Intervenir en la confección de planes de contingencia.

• Verificar mediante pruebas que los planes de contingencia y acciones de recuperación se mantengan válidos.

• Implementar medidas de seguridad lógicas y fisicas respecto a riesgos externos.

• Implementar medidas de seguridad contra riesgos internos o que simulan serb.

• Intervenir en temas de seguridad perimetral. En esto el t6cnico pone en juego su capacidad anticipatoria analizando posibles escenarios que puedan afectar a la continuidad del normal funcionamiento de los servicios y evaluando eventuales consecuencias de los mismos. El técnico tiene que actuar en equipo con los responsables de la seguridad fIsica, electrónica y de los sistemas, realizando las actividades a su cargo y advirtiendo sobre situaciones e incidentes que puedan tener consecuencias para el servicio.

Campo de la Formación Especifica Dedicado a abordar los saberes propios de cada eampo profesional, asI como también la eontextualizacjón de los desarrollados en la formaciOn de fundamento. Los contenidos correspondientes a este campo están agrupados en forma tal que puedan relacionarse fácilmente con las actividades propias del perfil profesional del Técnieo Superior en Soporte de Infraestructura de TecnologIa de la Información. Para poner en perspectiva y seflalar el nivel de Ins contenidos, se Ins acompaña con ejemplos de ejercicios prácticos que contribuyan a la formacion a través de desempenos que u preparen al estudiante para su trabajo futuro, de acuerdo a la Resolucion del CFE / N°107/l0. Anexo II.

Para Rendir	Debe tener Aprobada
Algoritmos y Estructura de Datos	Matemática Lógica y Programación
Bases de Datos	Lógica y Programación
Sistemas Operativos	Arquitectura de las Computadoras
Infraestructura de Redes II	Infraestructura de Redes I
Administración de Bases de Datos	Bases de Datos
Administración de Sistemas Operativos y Redes	Infraestructura de Redes II Sistemas Operativos
Seguridad de los Sistemas	Sistemas Operativos
Integridad y Migración de Datos	Infraestructura de Redes II Administración
Práctica Profesionalizante II	Práctica Profesionalizante I Innovación y Desarrollo Emprendedor