INSTITUCIÓN: ESCUELA SUPERIOR DE COMERCIO N°43

CARRERA: TÉCNICO SUPERIOR EN SOPORTE DE INFRAESTRUCTURA DE TECNOLOGÍA DE LA INFORMACIÓN

ESPACIO CURRICULAR: Integridad y Migración de Datos

CAMPO DE LA FORMACIÓN: Específica

CURSO: Tercer Año

CICLO LECTIVO: 2022

PROFESOR/A: Pratto, Andrea Yanina

ASIGNACIÓN HORARIA: 4 hs.

FORMATO: Taller

RÉGIMEN DE CURSADO: Anual

PLAN DECRETO: 2120/16

FUNDAMENTACIÓN

El diagnóstico y solución de incidentes es una de las tareas primordiales de un administrador de infraestructuras. La gestión de datos debe ser considerada como un proceso en sí mismo y no como algo subsidiario a cada proceso operativo. Debe enfocarse en todo el ciclo de vida del dato, desde su generación, pasando por su selección, representación, almacenaje, recuperación, distribución y uso. Independientemente del formato o medio en el que hayan sido registrados, procesados, archivados, utilizados o retirados.

La información es un activo esencial para cualquier organización y el potencial de su valor reside en garantizar la integridad y migración de los datos, ello permite trabajar con información fiable, procesos seguros y realizar la transferencia de datos de un sistema a otro en momentos de transición provocados por la llegada de una nueva aplicación, un cambio en el modo o medio de almacenamiento o las necesidades que impone el mantenimiento de la base de datos corporativa.

Estos procesos permiten conocer el estado del cumplimiento de la integridad de datos en los procesos críticos de negocio, abarcando tanto la gestión manual como informatizada para determinar los principales puntos de riesgos a subsanar y proponer acciones correctoras concretas.

Este espacio les permite a los estudiantes obtener herramientas que le posibiliten prever situaciones que puedan afectar el normal funcionamiento de las Tecnologías de la información y diseñar planes de contingencias.

PROPÓSITOS

- Atender incidentes que afecten al Soporte de infraestructura de TI, diagnosticar las causas que los originan y resolverlos o coordinar su solución.
- Elaborar Planes de contingencias para los distintos riesgos que puedan afectar al Soporte de Infraestructura de TI.

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 METODOLÓGICAS

- ❖Búsqueda de información en Web.
- ❖ Ejercitación en procedimientos de registro de incidentes y de las actividades necesarias para resolverlos.
- ❖ Lectura, análisis y soluciones.
- ❖ Elaboración y presentación de informes.
- ❖ Trabajos colaborativos con diferentes aplicaciones.
- ❖ Realizar visitas a data centers para tomar conocimiento de sus condiciones y planes de contingencias.

RECURSOS

- ❖ Computadoras/Celulares. Internet. Distintas aplicaciones. Proyector.
- ❖ Fotocopias, documentos digitales.
- ❖ Plataforma Classroom

MODALIDAD DE CURSADO

El taller de Integridad y Migración de Datos sólo admite el cursado regular presencial

EVALUACIÓN

La evaluación es continua, acompañada por un seguimiento exhaustivo del trabajo de cada estudiante. Se tienen en cuenta diferentes factores que hacen al conocimiento del docente respecto del desempeño personal de los estudiantes.

Instrumentos de evaluación:

❖ Trabajos prácticos.

❖ Elaboración de informes.

❖ Exposición y puesta en común de diferentes actividades.

Criterios de evaluación:

❖ Entrega en tiempo y forma de los trabajos prácticos en formato digital y papel. ❖ Respeto por el trabajo y las opiniones del resto de los compañeros. ❖ Asistencia a clases y a las actividades extra-áulicas organizada por el espacio curricular. ❖ Compromiso y responsabilidad en el desarrollo de los trabajos.

Regularización del taller:

a) Sólo admitirán el cursado regular presencial.

b) 75% de asistencia a las clases áulicas.

c) Aprobar el 100% de las instancias de evaluación previstas en la planificación anual.

Al cumplir con los requisitos a – b – c tiene derecho a una instancia final de integración que para aprobar deberá obtener nota de 6 (seis) o más sin centésimos.

El estudiante que no haya aprobado la instancia final de integración, podrá presentarse hasta dos turnos de exámenes consecutivos inmediatos posteriores a la finalización de la cursada.

Observación:

Debe tener **APROBADA** Infraestructura de Redes II y Administración.

BIBLIOGRAFÍA

· Normas ISO 20000 link:

https://www.proactivanet.com/images/Blog/ISO20000_GuiaCompletadeAplicacion_L uisMoran.pdf

· Roa Buendia, J. (2013). Seguridad informática. Madrid: Mc GrawHill.