Escuela Colombiana de Ingeniería Julio Garavito
Laboratorio de Seguridad Informática
Laboratorio Nº 3 – Plan de Continuidad de Negocios

OBJECTIVES

GENERAL

- Identify, analyze and evaluate interruption risks that can compromise the delivery of critical services in an organization.

SPECIFIC:

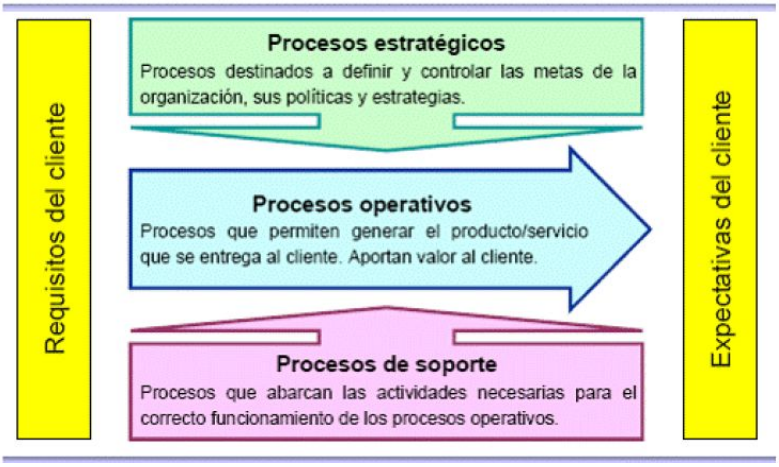
- Identify the critical processes for an organization.
- Make an interruption risk assessment for a critical process identified previously.
- Identify the technological context (inputs, outputs, critical times) where a critical process is involved.
- Identify recovery time objectives (RTO/RPO) for a critical process in the selected organization.
- Propose a recovery strategy to support the Business Continuity Plan for the critical process.

Make groups of <u>three</u> students and answer the following questions:

SECTION ONE – UNDERSTANDING ORGANIZATIONAL CONTEXT

1. According with figure No. 1, identify strategic, operational and support processes in a selected organization, completing table 1. Additional, chose and document one of the critical process creating a flowchart with the activities that composed it.

Figure 1. Types of process in an organization



Escuela Colombiana de Ingeniería Julio Garavito
Laboratorio de Seguridad Informática
Laboratorio Nº 3 – Plan de Continuidad de Negocios

Table 1. Processes in the organization

UNIDAD DE NEGOCIO	PROCESO	DESCRIPCIÓN	CRÍTICO PARA CONTINUIDAD (S/N)	JUSTIFICACIÓN CRITICIDAD
Estratégico	Dirección del restaurante	Planificación y objetivos , finanzas , gestión de calidad y plan operativo	N	Este puede tener interrupciones en la operación sin afectar la continuidad del negocio como tal
Estratégico	Comercialización y marketing	Publicidad y promoción. Precios y control de ventas	N	Este puede tener interrupciones en la operación sin afectar la continuidad del negocio como ta
Soporte	Gestión de compras	Especificaciones , selección de proveedores , compras , recepción y control de inventarios	N	Este puede tener interrupciones en la operación sin afectar la continuidad del negocio como tal
Soporte	Mantenimiento e innovación	Mantenimiento a hornos , estufas , congeladores , equipos de servicio y sistema de operación informático	S	Es indispensable que los elementos de trabajo estén en constante mantenimiento ya que con ellos se preparan los pedidos. Además , los servicios informáticos para tener control de los pedidos pendientes y de los que se realicen de forma remota
Operativo	Compras	Adquisición de materias primas y productos de calidad con las mejores condiciones de precio	S	Mediante este proceso la empresa obtiene la materia prima con la cual va a generar sus ingresos
Operativo	Recepción y entrega de pedidos	Mediante este proceso se reciben y se entregan las peticiones del cliente tanto de aquellos que llegan al establecimiento como de aquellos que utilizan el servicio de domicilios	S	Mediante este proceso se reciben y almacenan en la base de datos del restaurante los pedidos de los clientes que son los que en un futuro generarán los ingresos del restaurante

Escuela Colombiana de Ingeniería Julio Garavito
Laboratorio de Seguridad Informática
Laboratorio Nº 3 – Plan de Continuidad de Negocios

2. For a selected critical process, analyze each of the interruption risks scenarios. Complete the existing countermeasures to mitigate each identified risk in table 2.

Table 2. Existing countermeasures

Riesgo	Amenaza	Controles	Calificación del control	Riesgo residual		
				Probabilidad	Consecuencia	Valoración del riesgo
No acceso a la base de datos de los pedidos.	Falla de suministro eléctrico	No tiene	0	Posible	Moderado	M
	Fallas en el hardware	No tiene	0			
	Fallas en el software	No tiene	0			
	Borrado de información en la base de datos	Backups	4			
Errores en la entrega del pedido	El cliente no informa de la falla	No tiene	0	Probable	Moderado	M
	Falla en el empaque del pedido por parte de los empleados	No tiene	0			
Fallo en la aplicación por la cual se realizan los pedidos	Falla de comunicación entre la aplicación y la base de datos	No tiene	0	Posible	Mayor	M

	Fallas en el sistema que impidan el acceso a la aplicación	Mantenimiento mensual del software y la red que sostienen la aplicación	3			
No acceso a las instalaciones en donde se desarrolla el proceso	Incendio	Herramientas para el control de un incendio (extintores, mangueras)	3	Poco posible	Moderado	N
	Inundación	Motobombas, Baldes	3			
	Temblores, sismos	Botiquín de primeros auxilios	3			

Escuela Colombiana de Ingeniería Julio Garavito
Laboratorio de Seguridad Informática
Laboratorio Nº 3 – Plan de Continuidad de Negocios

3. Evaluate the risk level (consecuencia x probabilidad) for each identified risk scenery using the following risk map and scales proposed in the following tables.

Riesgos :

- **No acceso a la base de datos de los pedidos.**
- **Errores en la entrega del pedido**
- **Fallo en la aplicación por la cual se realizan los pedidos**
- **No acceso a las instalaciones en donde se desarrolla el proceso**

Table 3. Risk map

		CONSECUENCIA				
PROBABILIDAD	IMPACTO X PROBABILIDAD	Insignificante	Menor	Moderado	Mayor	Catastrófico
	Muy Probable	M	M	H	H	MH
	Probable	M	M	M	H	H
	Posible	N	M	M	M	H
	Poco Posible	N	N	M	M	M
	Raro	N	N	N	M	M

Table 4. Risk assessment

Valoración	Color	Descripción
Nulo		Situación adecuada para la organización
Moderado		Los controles son adecuados, sin embargo existen algunas debilidades.
Alto		La organización debe adoptar medidas que minimicen el riesgo de forma rápida y efectiva.
Muy alto		La organización debe adoptar medidas inmediatas.

SECTION TWO – TECHNOLOGICAL CONTEXT

4. Analysis of applications supporting the business critical process: Next, list all applications that support the execution of the chosen process in section one, and estimate the availability time requirement (considering a labor week of 40 hours), and the unavailability percentage for each application. Complete the following table with these information:

Table 5. Applications per critical process

Proceso crítico	Aplicación	Tiempo de disponibilidad	% de indisponibilidad	Justificación
Recepción y entrega de pedidos	Base de datos MySQL	40 horas	10 %	La base de datos es la encargada de almacenar todos los pedidos recibiendolos desde las distintas fuentes (Web o móvil), si este servicio se ve interrumpido no será posible atender las solicitudes de los clientes.
	Programa web y móvil de realización de pedidos	30 horas	30 %	La aplicación de reservas tiene que estár disponible todo el tiempo en el cual el establecimiento permanezca abierto debido a que es una de

				las fuentes de ingresos, además de proporcionar satisfacción según el nivel de atención al cliente
	Aplicación Interna de pedidos a realizar y comunicación entre trabajadores	40 horas	10 %	La aplicación interna se encargará de indicarle a los empleados la correcta preparación de cada una de las solicitudes.

5. List all business units and external entities of which the selected critical process receives inputs. Additional, list the process outputs, complete all this information in the table below:

Table 6. Process inputs

Entradas			
Interna/ Externa	**Unidad de negocio/ Entidad**	**Descripción de la(s) Entrada(s)**	**Medio de envío**
Interno	Recursos humanos	Personal para atender al cliente	Físico
Externa	Codensa	Energía para la operación del negocio	Físico
Externa	Procables S.A.S (Cable UTP)	Cables UTP para realizar la conexión de los computadores	Físico
Externa	MySQL	Base de datos dónde se almacenarán los pedidos.	Digital
Externa	Cisco	Infraestructura de red necesaria para montar la aplicación.	Físico
Interna	DELL	Equipos usados para soportar el funcionamiento	Físico, Digital

Table 7. Process outputs

Outputs					
Interna / Externa	**Unidad de negocio / Entidad**	**Ente regulatorio**	**Descripción de la(s) salida(s)**	**Medio de envío**	**Periodicidad de entrega**
Externa	Cliente	N	Pedido entregado	Físico	Al finalizar un pedido
Interna	Gerente de compras	S	Ganancias obtenidas por los pedidos	N/A	Cada semana
Interna	Analista de pedidos	S	Pedido empacado	Físico	Al empacar un pedido

6. For the selected critical process, describe the most critical operations periods of the year and justify the reason, additional, include the most critical day schedule with its justification. Complete these information in the table below.

Table 8. Critical operation periods and schedules

Proceso Crítico	**Periodos de mayor criticidad en el año**	**Horarios de mayor criticidad en el día**
Recepción y entrega de pedidos	Día de las madres	Desde las 11 am hasta 5 pm
Recepción y entrega de pedidos	Entre noviembre y diciembre (Es cuando empieza la temporada de fin de año)	Medio día, específicamente la hora de almuerzo es cuando más pedidos se reciben.

7. Consider that a high impact incident has just happened and the critical process is interrupted, define the Recovery time objective (RTO), maximum time to recover the process without negatives impacts to the organization. Specify the recovery point objective (RPO), maximum information loss that the critical process could support. Complete these information in the table below:

Table 9. Critical process RTO and RPO

Proceso crítico	Rto	Justificación Rto	Rpo	Justificación Rpo
Recepción y entrega de pedidos	1 día	La recepción y entrega de pedidos es el proceso que genera mayores ingresos para la empresa. Es por esto que no puede estar mucho tiempo indisponible porque implicaría una gran perdida de dinero para la empresa y obligaría a volver a coordinar las fechas de los pedidos recibidos y a reconfirmar los pedidos entregados por lo menos en la última semana.	10 % de los pedidos que se realizan al día por fallo en la aplicación del cliente.	Si un cliente realiza un pedido y le muestra una confirmación exitosa, pero esta no es procesada, es casi inmediata la pérdida de dicho cliente.

Recovery strategies

8. List functional teams required to operate the critical process. Each person should have a Backup in case the main person couldn't attend the operation. Complete the table below with the team, critical process, role in the process, position, name, office location, business telephone, cellphone and home telephone. Use the tables below:

Table 10. Functional team of the process

Nombre del equipo funcional: Order recovery team			**Proceso crítico: Recepción y Entrega de pedidos**		
Composición inicial del equipo funcional					
Rol dentro del equipo	**Cargo**	**Nombre**	**Ubicación oficina**	**Teléfono oficina**	**Teléfono celular**
Líder del equipo	Líder de proyecto	Nicolás Aguilera	Wework	4889596	3103257786
Miembro del equipo	Administrador de base de datos	Diego Puerto	Remoto	4889596	311836666
Miembro del equipo	Arquitecto de redes	Juan Mejía	Wework	4889596	3002182530
Miembro del equipo	Administrador de la aplicación de pedidos	Andrés Rocha	Wework	435345	3102986675

9. Minimum operation resources: assume that an incident affecting the location where all your team is operating the critical process has occurred, and the mobilization of people is required to an alternate operation location, where critical operations could be recovered. Having into account the situation proposed above, complete the following tables with the minimum resources to operate and vital registers required in the alternate operate location:

Tabla 11. Minimum resources

Equipo funcional					
Recursos mínimos					
# Funcionarios actuales que atienden el proceso	**# mínimo de funcionarios requeridos en contingencia**	**Hardware**	**Software**	**Conexiones especiales**	**Útiles especiales de escritorio (ej. Papelería específica, etc)**
Líder del proyecto, administrador de la base de datos , administrador de las aplicaciones y el arquitecto de red , meseros , cocineros y domiciliarios.	los 4 miembros del equipo del proyecto más algunos cocineros y domiciliarios.	1 computador : Para tener acceso a la base de datos de los pedidos realizados y entregados.	- Sistema operativo: Requerimiento básico para que la aplicación pueda operar hacia los clientes y recibir sus solicitudes - MySQL: para que se pueda llevar control del registro de	-A MySQL -B Alquiler de servicio de cocina.	Ninguna

			los pedidos momentáneamente		

Tabla 12. Vital registers

Registros vitales (archivos locales)						
Registros vitales	**Frecuencia del respaldo**	**Ubicación del respaldo**	**Medio**	**Criticidad (Muy crítico medianamente crítica)**	**Requerimiento Regulatorio. S/N**	**Descripción**
El menú del restaurante	Mensualmente	Oficina y correo electrónico	Físico y digital	Muy crítico	N	El menú es la base de los pedidos de los clientes, es determinado por la administración y se actualiza cada mes según la oferta agrícola y se envía la actualización vía correo electrónico o de manera física en la oficina

Base de datos	Diariamente	En la nube	Dígital	Muy crítico	N	La base de datos es el lugar que guarda todos los pedidos que debe realizar la empresa para cumplir con su objetivo básico financiero.

SECTION THREE- RECOVERY STRATEGY

10. Define some recommendation to mitigate the identified interrupción risk in section one that have moderate and high values. Complete the tables below with the information:

Escuela Colombiana de Ingeniería Julio Garavito
Laboratorio de Seguridad Informática
Laboratorio Nº 3 – Plan de Continuidad de Negocios

1. No acceso a la base de datos de los pedidos

Riesgo	Amenaza	Controles	Calificación del control	Riesgo residual			Recomendaciones sobre los controles	Recomendaciones generales
				Probabilidad	Consecuencia	Valoración del riesgo		
No acceso a la base de datos de los pedidos.	Falla de suministro eléctrico	No tiene	0	Posible	Moderado	M	Planta eléctrica para autonomía en caso de un fallo de suministro eléctrico	La planta eléctrica debe estar siempre cargada y lista para operar en caso de una emergencia Debe estar ubicada en un lugar seguro y accesible solo por personal autorizado Ubicada en un lugar lo más lejano posible a el resto de los activos
	Fallas en el hardware	No tiene	0				Siempre debe estar un computador Un computador disponible en caso de fallo de hardware	Siempre debe estar un computador disponible con todo el software requerido para la operación en caso de falla de hardware para ser asignado al residente de obra Se debe tener listo el equipo para operar y ser enviado Ubicado bajo condiciones de seguridad y alejado del resto de equipos
	Fallas en el software	No tiene	0				Disco de respaldo con el software requerido	El disco de respaldo debe contener el software listo para instalar, incluidas las licencia y manuales de usuario El personal que

Escuela Colombiana de Ingeniería Julio Garavito
Laboratorio de Seguridad Informática
Laboratorio Nº 3 – Plan de Continuidad de Negocios

								usa el disco no debe modificar el disco, solo debe usarlo Contar con un registro de logs sobre dicha información
	Borrado de información en la base de datos	Backups	4				Menor tiempo entre backups y centralización	Que sean más seguidos y se manejen en un ambiente compartido como la nube Con único acceso del servidor principal y el de contingencoa

2. Errores en la entrega del pedido

Riesgo	Amenaza	Controles	Calificación del control	Riesgo residual			Recomendaciones sobre los controles	Recomendaciones generales
				Probabilidad	Consecuencia	Valoración del riesgo		
Errores en la entrega del pedid	El cliente no informa de la falla	No tiene	0	Probable	Moderado	M	Controles telefónicos o por medio de la aplicación que permitan saber si el cliente recibió el pedido esperado	Además de los controles realizados al cliente , realizar un inventario por cada día de lo que se tenía y lo que se gastó para de esta manera reconfirmar la correcta entrega de los pedidos.
	Falla en el empaque del pedido por parte de los empleados	No tiene	0				Establecer un nuevo rol que se encargue de analizar los pedidos después de empacados antes de ser enviado	Ese rol debe recibir una capacitación para que tenga el conocimiento de qué requerimientos debe cumplir cada pedido

Escuela Colombiana de Ingeniería Julio Garavito
Laboratorio de Seguridad Informática
Laboratorio Nº 3 – Plan de Continuidad de Negocios

3. Fallo en la aplicación por la cual se realizan los pedidos

Riesgo	Amenaza	Controles	Calificación del control	Riesgo residual			Recomendaciones sobre los controles	Recomendaciones generales
				Probabilidad	Consecuencia	Valoración del riesgo		
Fallo en la aplicación por la cual se realizan los pedidos	Falla de comunicación entre la aplicación y la base de datos	No tiene	0	Posible	Mayor	M	Contratar a una persona que se encargue de realizar la auditoría de las conexiones entre las aplicaciones y la base de datos.	Mejorar el desarrollo de pruebas de dichas conexiones considerando casos poco probables o interrupciones inesperadas
	Fallas en el sistema que impidan el acceso a la aplicación	Mantenimiento mensual del software y la red que sostienen la aplicación	3				Poseer un backup de respaldo que permita restaurar la última versión de la aplicación que funcionó	Implementar practicas de desarrollo continuo que faciliten la implementación de cambios que puedan afectar la aplicación de forma drástica.

4. No acceso a las instalaciones en donde se desarrolla el proceso

Riesgo	Amenaza	Controles	Calificación del control	Riesgo residual			Recomendaciones sobre los controles	Recomendaciones generales
				Probabilidad	Consecuencia	Valoración del riesgo		
No acceso a las instalaciones en donde se desarrolla el proceso	Incendio	Herramientas para el control de un incendio (extintores, mangueras)	3	Poco posible	Moderado	N	Cambio del químico contra incendios anualmente y revisión de las instalaciones	Las áreas con mangueras y extintores deben estar marcados y
	Inundación	Motobombas, Baldes	3				Deben ser revisadas para comprobar su funcionamiento y que los baldes no tengan agujeros	Siempre debe estar en un lugar de fácil acceso y resaltado para fácil detección
	Temblores, sismos	Botiquín de primeros auxilios	3				Medicamentos no vencidos y reponer cualquier elemento que se gaste	Debe ubicarse en un área visible y no estar bloqueado por otros objetos o puertas

---

11. Elaborate a PowerPoint, maximum 13 slides which contain:

    - ✔ 1-2 slides with the description of the organization and its processes based on table 1.
    - ✔ 1-2 slides with the analysis of interruption risks (*Calificación del control, probabilidad, consecuencia, riesgo*) for the selected critical process based on table 2.
    - ✔ 1-2 slides explaining the applications that support the selected critical process based on table 8.
    - ✔ 1-2 slides explaining the input/output of the selected critical process and the most critical periods, based on table 9, 10 and 11.
    - ✔ 1 slide defining the RTO and RPO for the critical process based on table 12.
    - ✔ 1 slide explaining the current functional team of the critical process based on table 13.
    - ✔ 1 slide explaining the minimum resources and vital registers of the critical process based on table 15 and 16.
    - ✔ 1-2 slides explaining your recommendations over the controls based on table 17, which help to meet the RTO/RPO defined previously for the critical process. Justify the recommendations based on a cost/benefit analysis. Define the actions to follow to implement the recommendations. You can use graphs, tables, figures or any other element that you believe can help to explain your recommendations to the manager.

Prepare the following two documents to deliver:

1. Word or excel document which includes the tables of responses for the present Laboratory.
2. Power point presentation related with point 11.

The files must be named in the following way:

- **Lab3-AndresRochaDiegoPuertoJuanMejiaNicolasAguilera.pdf**
- **Presentation-AndresRochaDiegoPuertoJuanMejiaNicolasAguilera.ppt**