INGENIERIA DE SISTEMAS – SPTI 2021-1

LABORATORIO 3:

Análisis de Riesgos de Seguridad de la Información

GERSON DAVID QUINTERO RODRIGUEZ

Autor:

Torres Segura Duck James Alexander

Jimmy Armando Chirivi Nivia

INTRODUCTION

In this laboratory we will learn to identify, analyze and evaluate the risks of interruption that can compromise the provision of critical services in an organization, we will also treat the risks and classify them from a scale where we will see or not affect our assets and we will observe through these scales the impact that it can have on our company and how we can avoid the interruption of the service.

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.

1. SECTION ONE: UNDERSTANDING ORGANIZATIONAL CONTEXT

- 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.

Ilustración 1: Types of process in an organization.

UNIDAD DE NEGOCIO	PROCESO	DESCRIPCIÓN	CRITICO PARA CONTINUIDAD (S/N)	JUSTIFICACION CRITICIDAD
Estratégico	Revisión de objetivos, valores y políticas	Se encarga de analizar y actualizar los objetivos, valores y políticas.	N	La revisión de los objetivos, valores y políticas no generan criticidad ya que su ejecución no es constante pero es algo importante de la empresa lo cual no permite efectos a corto plazo.
Soporte	Gestión de clientes	El área enfocada en prestar una atención respecto al software adquirido.	N	Al no tener disponible la capacidad de responder y acompañar a los clientes durante el desarrollo se afecta la reputación de la empresa.
Estratégico	Gestión de alianzas	Es el proceso encargado de realizar, entablar y controlar todas las alianzas orientadas a la materia prima para la realización de las obras	N	Este puede tener interrupciones en la operación sin afectar la continuidad de una obra o del negocio como tal

Operativo	Gestión de desarrollo de producto	Se encarga de gestionar el desarrollo de nuevos proyectos tecnológicos en la creación de nuevos productos	S	Este proceso no puede tener interrupciones dado que el desarrollo de un producto es fundamental en los ingresos de la empresa.
Operativo	Gestión de infraestructura empresarial	Se encarga de mantener la disponibilidad de los artefactos hardware y software de la empresa	S	El fallo de alguno de los dispositivos hardware causaría un atraso en el proceso de producción de la empresa generando perdidas económicas.
Estratégico	Gestión de proyectos	Es el proceso realizado en planeación, ejecución y financiación del proyecto.	S	Es importante mantener la manera en que se realiza la gestión de proyectos ya que ocurrido un fallo el proceso de ejecución tardaría y con esto la entrega del producto.
Soporte	Gestión Administrativa	Se encarga de revisar los procesos y servicios que permite la gestión de los activos de la compañía.	N	Podría robar información, fraude o realizar espionaje empresarial en los procesos importantes de la empresa causando perdidas monetarias.

Tabla 1: Processes in the organization

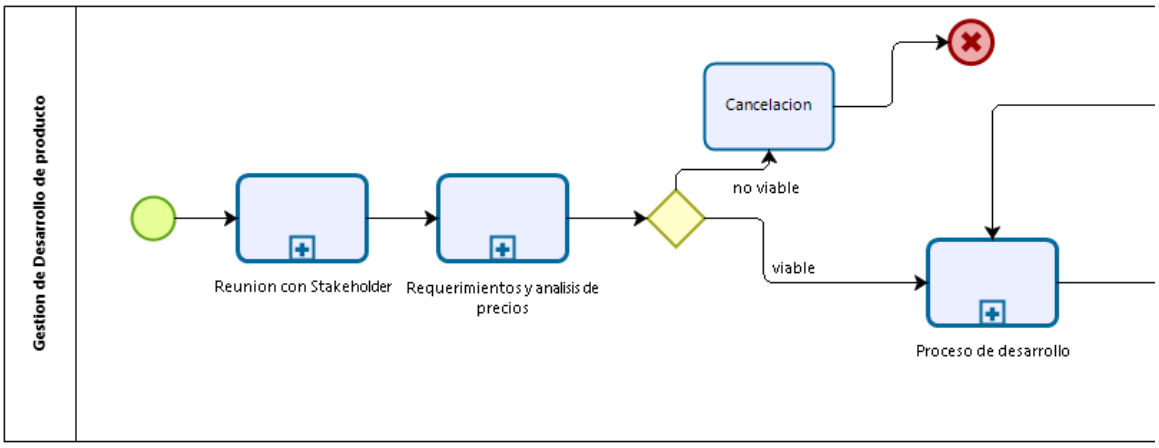
- For a selected critical process, analyze each of the interruption risks scenarios. Complete the existing countermeasures to mitigate each identified risk in table 2.

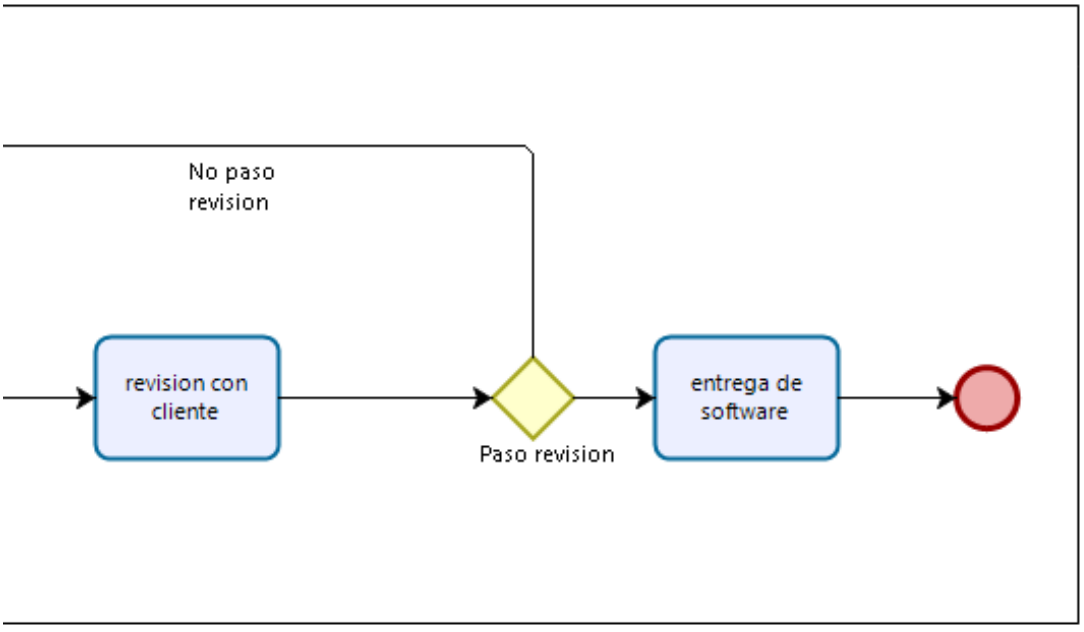
Riesgo	Amenaza	Controles	Calificación del control	Riesgo Residual		
				Probabilidad	Consecuencia	Valoración del riesgo
Indisponibilidad de la tecnología relacionada con el proceso crítico identificado.	Falla de suministro eléctrico	Ej.: Contrato con proveedor 7x24, con repuestos de partes en menos de 24 horas.				
	Fallas en el hardware					
	Fallas en el software					
	Borrado de información de la base de datos.					
No acceso las instalaciones donde se desarrolla el proceso	Actividad terrorista					
	Terremoto					
	Incendio					
Falta de personal critico	Calamidad domestica					
	Pandemias					
Falta de disponibilidad de proveedores críticos	Fallas en el servicio					

Tabla 2: Existing countermeasures

Proceso seleccionado: Gestion de Desarrollo de product

Proceso seleccionado: Gestion de Desarrollo de product





Riesgo	Amenaza	Controles	Calificación del control	Riesgo residual		
				Probabilidad	Consecuencia	Valoración del riesgo
Fallo del uso de servidores, instalaciones y servicios Cloud.	Incendio	Sistema de control temprano de incendios	3	Posible	Moderado	M
	Sismos	Cuarto de computación con protección especial ante terremotos	4			
	Fallo en credenciales de acceso	Backups	4			
	Borrado de información en la base de datos y fallos en servidores Cloud	Backups y controles de archivo	3			
Perdida de data y procesos de desarrollo durante la creación de un producto	Ciberataque	Firewalls, herramientas y personal de control en ciberseguridad y Backups	4	Probable	Mayor	H
	Error personal	Backups, herramientas de versionamientos.	3			
	Acceso administrador a personal no necesario	Auditoria de cuentas y permisos de usuario	3			
	Filtrado de archivos privados	Servidor de archivos privados	4			
Falta del personal critico	Calamidad domestica	Se tienen reemplazos	4	Probable	Insignificante	M
	Pandemia	Se tienen reemplazos	4			
Falta de disponibilidad de servicios	Fallas en el servicio	Backups	4	Posible	Menor	M
	Perdida de acceso	Soporte técnico	3			

Tabla 3: Existing countermeasures

- Evaluate the effectiveness of the countermeasures (Calificación del control), for each identified risk stage. Fill in the corresponding column in table 2, using the values proposed in the following table:

Calificación Cualitativa	Valoración	Descripción
Sin control	0	El control no existe.
Inaceptable	1	El control existe y no se aplica.
Deficiente	2	El control existe, se aplica pero no siempre es eficiente.
Bueno	3	El control existe, pero no se aplica siempre.
Excelente	4	El control existe, es eficiente y siempre lo aplican.

Tabla 4: Countermeasures rating scale

- Assess the probability of occurrence (Probabilidad cualitativa) and the impact (Nivel de consecuencia) in the corresponding column in table 2. Take into account the values proposed in the following table:

Probabilidad Cualitativa	Probabilidad Cuantitativo	Descripción
Muy Probable	Más de 30 veces en el año	Se espera que su ocurrencia sea muy frecuente.
Probable	Entre 11 y 20 veces en un año	Es factible que se presente el hecho dadas las condiciones del ambiente interno y externo de la organización.
Posible	Entre 4 y 10 veces en un año	Puede ocurrir en cualquier momento. La amenaza existe y hace parte de la realidad y del día a día, pero no se ha identificado como una amenaza o problema.
Poco probable	Entre 1 y 3 veces en un año	La amenaza existe pero no es normal o común, considerando las condiciones y el ambiente interno y externo de la organización. Puede convertirse en problema en ocasiones y situaciones específicas.
Raro	1 Vez en más de un año	Es difícil que ocurra.

Tabla 5: Probability of occurrence

Nivel de Consecuencia	Escala numérica	Descripción
Insignificante	0 – 100 Millones	Las consecuencias presentan pérdidas mínimas
Menor	101 -300 millones	Se presentan pérdidas bajas pero su tratamiento y control es rápido y focalizado
Moderado	301- 449 millones	Se presentan pérdidas medias, su tratamiento es intensivo y focalizado
Mayor	450 – 1049 millones	Sus consecuencias presentan perjuicios extensivos con pérdidas altas
Catastrófico	1050 – 1500 millones	Las consecuencias amenazan la supervivencia de la Corporación, perjuicios graves.

Tabla 6: Impact level

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

		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
	Nulo	N	N	N	M	M

Tabla 7: Risk map

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.

Tabla 8: Risk assessment

2. SECTION TWO: TECHNOLOGICAL CONTEXT

- 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:

PROCESO CRÍTICO	APLICACIÓN	%	TIEMPO	JUSTIFICACIÓN
<Digite el proceso crítico por áreas de negocio>	<Digite el nombre de la aplicación que soporta el proceso del negocio>	<Digite el porcentaje de afectación de la aplicación antes descrita>	<Digite el tiempo estimado que transcurriría para esta afectación>	<Diligencie una pequeña justificación del tiempo estimado para la aplicación en afectación>

Tabla 9: Applications per critical process

Proceso crítico	Aplicación	Tiempo de disponibilidad	% de indisponibilidad	Justificación
Gestión de desarrollo de producto	Github	12 horas	30 %	La herramienta de control de versiones es fundamental durante el desarrollo de productos software, ya que se trabaja de manera eficiente y coordinada.
	IDE (Visual Studio)	32 horas	25 %	El IDE es la herramienta mas importante para el desarrollo de productos software.
	Canales de Comunicación (Teams ,correo)	15 horas	10 %	La comunicación entre integrantes del equipo es fundamental para la asignación de actividades y plan de desarrollo.
	Trello o Taiga	12 horas	20 %	Dado que se poseen los requerimientos del proyecto se debe organizar los Sprint de desarrollo.

Tabla 10: Applications per critical process

- 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:

ENTRADAS			
INTERNA / EXTERNA	**UNIDAD DE NEGOCIO / ENTIDAD**	**DESCRIPCIÓN DE LA(S) ENTRADA(S)**	**MEDIO DE ENVÍO**
<Digite las entidades externas/internas del cual se reciben entradas>	<Digite las unidades de negocio que se está evaluando>	<Realice una pequeña descripción de las entradas que soporta el proceso crítico>	<Correo electrónico, físico directo, físico mensajería, usb, cd, transmisión electrónica ,fax>

Tabla 11: Process inputs

Entradas			
Interna/ Externa	**Unidad de negocio/ Entidad**	**Descripción de la(s) Entrada(s)**	**Medio de envío**
Interno	Recursos humanos	Personal para la ejecución del desarrollo del producto.	Físico, Digital
Externa	Stakeholder	Determina los requerimientos para el desarrollo del producto.	Físico, Digital
Externa	AWS	Empresa proveedora de servicios Cloud.	Digital.
Externa	Empresa proveedora de servicios de red (IPS)	Empresa proveedora de servicios de internet.	Físico, Digital
Externa	Cisco	Proveedores de herramientas hardware.	Físico, Digital

Tabla 12: Process inputs

SALIDAS					
Interna / Externa	Unidad de negocio / Entidad	ENTE REGULATORIO? S/N	DESCRIPCIÓN DE LA(S) SALIDA(S)	MEDIO DE ENVÍO	PERIODICIDAD DE ENTREGA
				<Correo electrónico, físico directo, mensajería, usb, cd,etc.>	

Tabla 13: Process outputs

Outputs					
Interna / Externa	**Unidad de negocio / Entidad**	**Ente regulatorio**	**Descripción de la(s) salida(s)**	**Medio de envío**	**Periodicidad de entrega**
Externa	Consultor	S	Sprints y avances del producto.	Físico	Cada 2 semanas
Externa	Cliente	S	Producto terminado	Digital	Al finalizar el desarrollo
Interna	Gerente de proyecto	S	Diseño de plan de trabajo	Físico,Digital	En el inicio del proyecto
Externa	Cliente	S	Prerrequisitos del proyecto	Físico, Digital	En el inicio del proyecto
Interna	Gestión de proyecto	N	Repositorio y tableros con los avances de los Sprints	Digital	Cada semana

Tabla 14: Process outputs

- 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.

PROCESO CRÍTICO	PERÓIODOS DE MAYOR CRITICIDAD EN EL AÑO	HORARIOS DE MAYOR CRITICIDAD EN EL DÍA
<Digite el proceso crítico del negocio>	<Digite los períodos más críticos durante el año>	<Digite el horario más crítico durante el día>

Tabla 15: Critical operation periods and schedules

Proceso Critico	Periodos de mayor criticidad en el año	Horarios de mayor criticidad en el día
Gestión de desarrollo de producto	Entre Abril y Junio ya que los clientes desean innovar, remplazar y actualizar sus herramientas de trabajo.	Diurno, para no intervenir con las fechas de entrega y por el horario de los empleados.

Tabla 16: Critical operation periods and schedules

- 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:

PROCESO CRÍTICO	RTO	JUSTIFICACIÓN RTO	RPO	JUSTIFICACIÓN RPO
<Digite el proceso crítico dentro de la organización>	<Digite el tiempo objetivo de recuperación que se cree conveniente>	<Realice una pequeña justificación del RTO, antes escrito>	<Digite el punto objetivo de recuperación que se cree conveniente>	<Realice una pequeña justificación del RPO, antes escrito>

Tabla 17: Critical process RTO and RPO

Proceso crítico	Rto	Justificación Rto	Rpo	Justificación Rpo
Gestión de desarrollo de producto	1 dia	El tiempo objetivo de recuperación para el proceso de gestión de desarrollo de producto es de 1 día debido a que la empresa no puede seguir con las funcionalidades normales y cumplir con las fechas de entrega estipuladas en el programa de desarrollo de los productos de software	Los datos en las últimas 2 Sprints y su respectivo código	En este proceso de gestión de desarrollo de producto la cantidad de datos que se están dispuestos a perder son los equivalentes a 2 Sprints, donde cada Sprint tiene información fundamental para el proceso de desarrollo, y el backup se realiza cada tres días.

Tabla 18: Critical process RTO and RPO

Recovery strategies

- 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:

NOMBRE DEL EQUIPO FUNCIONAL:			PROCESO CRITICO:			
COMPOSICIÓN INICIAL DEL EQUIPO FUNCIONAL						
ROL DENTRO DEL EQUIPO FUNCIONAL	CARGO	NOMBRE	UBICACIÓN OFICINA	TELÉFONO OFICINA	TELÉFONO CELULAR	TELÉFONO CASA
Líder del equipo						
Miembro del equipo						
Miembro del equipo						
Miembro del equipo						
Miembro del equipo						
Miembro del equipo						

Tabla 19: Functional team of the process

Nombre del equipo funcional: Desarrollo de producto			**Proceso crítico: Gestión de desarrollo de producto**			
Composición inicial del equipo funcional						
Rol dentro del equipo	**Cargo**	**Nombre**	**Ubicación oficina**	**Teléfono oficina**	**Teléfono celular**	**Teléfono casa**
Lider de desarrollo Front	Líder de área	Konrrad Alvarado	Zona T	3577666	311836666	6682233
Lider de desarrollo Back	Líder de área	Álvaro Rojas	Zona T	3577666	311836666	6682233
Gerente de proyecto	Líder de proyecto	carlitos Quiroz	Zona T	3577666	311836666	6682233
Desarrollador full stack	Desarrollador	Juan Torres	Zona T	3577666	311836666	6682233
Desarrollador full stack	Desarrollador	Mateo Hoyos	Zona T	3577666	311836666	6682233
Diseñador UI	Diseñador	Daniel Pinto	Zona T	3577666	311836666	6682233
Desarrollador full stack	Desarrollador	Carlos Ramirez	Zona T	3577666	311836666	6682233

Tabla 20: Functional team of the process

COMPOSICIÓN ALTERNA 1 DEL EQUIPO FUNCIONAL						
ROL DENTRO DEL EQUIPO FUNCIONAL	CARGO	NOMBRE	UBICACIÓN OFICINA	TELÉFONO OFICINA	TELÉFONO CELULAR	TELÉFONO CASA
Líder alterno 1						
Alterno 1 Miembro del equipo						

Tabla 21: Backup of functional team

Composición alterna 1 del equipo funcional						
Rol dentro del equipo funcional	**Cargo**	**Nombre**	**Ubicación oficina**	**Teléfono oficina**	**Teléfono celular**	**Teléfono casa**
Gerente de proyecto	Líder de proyecto	carlitos Quiroz	Zona T	3577666	311836666	6682233
Lider de desarrollo Back	Líder de área	Álvaro Rojas	Zona T	3577666	311836666	6682233

Tabla 22: Backup of functional team

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

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)
<Digite el número de funcionales que soporta el proceso actualmente>	<Digite el número de funcionales mínimos requeridos para soportar el proceso>	<Digite el hardware necesario para operar en el Centro alterno de operación>	<Digite el software necesario para operar en el Centro alterno de operación>	<Digite cuáles son las conexiones especiales para operar en contingencia en el centro alterno de operación>	<Digite cuáles son los útiles de escritorio necesarios para operar en el Centro alterno de operación>

Tabla 23: 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)**
Aproximadamente 10 personas, expertos en FrontEnd y en Backend para desarrollar como también el gerente de proyecto	4 Desarrolladores y el entre los cuales se pueden dividir 2 entre labores de FrontEnd BackEnd y el tercer desarrollador puede enfatizar en el diseño del producto. Por último, se encuentra el gerente del proyecto	10 computador: para el desarrollo del producto y tablero el levantamiento de requerimientos	- Sistema operativo: Requerimiento básico para el funcionamiento del computado. - IDE: para que se pueda llevar ordenadame el proceso de desarrollo de software.	Ninguna	Ninguna

Tabla 24: Minimum resources

Registros Vitales (archivos locales)						
Registros Vitales	**Frecuencia del respaldo**	**Ubicación del respaldo**	**Medio**	**Criticidad (Muy crítico Medianamente critico)**	**Requerimiento Regulatorio. S/N**	**Descripción**
<Digite cuáles son los registros vitales (archivos locales) para operar en el Centro alterno de operación>	<Digite la frecuencia de respaldo que se realiza a la información>	<Digite la ubicación de respaldo de la información>	<Digite el medio de respaldo de la información(disco duro, cd, usb>	<Digite que tan crítica es la información que se maneja (muy crítica, crítica, medianamente crítica, menos crítica>	<Digite si existen o no requerimientos regulatorios a los registros>	<Digite una breve descripción de los registros vitales que se utilizan frecuentemente>

Tabla 25: Vital registers

Registros vitales (archivos locales)						
Registros vitales	**Frecuencia del respaldo**	**Ubicación del respaldo**	**Medio**	**Criticidad (Muy crítico medianamente critica)**	**Requerimiento Regulatorio. S/N**	**Descripción**
Los modelos de las bases de datos y Mockups de las aplicaciones.	Semanal mente	Cloud data, oficina y correo electrónico	Físico y digital	Muy critico	N	Los modelos y el diseño del producto es lo más importante para saber a lo que se debe llegar.

Tabla 26: Vital registers

3. SECTION THREE- RECOVERY STRATEGY

- 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:

Riesgo	**Amenaza**	**Controles**	**Calificación del control**	**Riesgo residual**			**Recomendaciones sobre los controles**	**Recomendaciones generales**
				Probabilidad	**Consecuencia**	**Valoración del riesgo**		
Fallo del uso de servidores, instalaciones y servicios Cloud.	Incendio	Sistema de control temprano de incendios	3	Posible	Moderado	M	Contratar servicio de vigilancia, crear puntos de control, salidas de emergencia y simulacros	Se podría contar con la posibilidad de comprar otra sede. o tener una segunda sede lista para funcionamiento.
	Sismos	Cuarto de computación con protección especial ante terremotos	4				ninguno	Tener especial cuidado de la zona en la que se ubicara el cuarto y su distrucion de equipos.
	Fallo en creden	Backups	4				ninguno	Guardar estas credencia

	ciales de acceso							les en un lugar seguro.
	Borrado de información en la base de datos y fallos en servidores Cloud	Backups y controles de archivo	3				Manejar controles de archivo y servidores de archivos internos	No siempre se contara con las backups disponibles, evitar eliminar archivos sin tener conocimientos sobre el.
Perdida de data y procesos de desarrollo durante la creación de un producto	Ciberataque	Firewalls, herramientas y personal de control en ciberseguridad y Backups	4	Probable	Mayor	H	Ninguno	Manejar auditorias externas a la empresa
	Error personal	Backups, herramientas de versionamientos.	3				Verificar los avances de cada empleaado durante el dearrollo	No siempre se cometen errores pero se debe estar preparados
	Acceso administradora personal no	Auditoria de cuentas y permisos de usuario	3				Expropiar el correo institucional a los ex empleados y permisos.	Ninguno

	necesario							
	Filtrado de archivos privados	Servidor de archivos privados	4				Verificar perdida de información y su origen	Mantener en constante monitoreo el gestor de archivos
Falta del personal critico	Calamidad domestica	Se tienen reemplazos	4	Probable	Insignificante	M	Ninguno	Se podría re distribuir el trabajo por los días de calamidad.
	Pandemia	Se tienen reemplazos	4				Ninguno	Se podría contratar empleados Freelancer por si ocurre alguna calamidad
Falta de disponibilidad de servicios	Fallas en el servicio	Backups	4	Posible	Menor	M	Contactar con empresa prestadora de servicio	ninguna
	Perdida de acceso	Soporte técnico	3				Contactar con empresa prestadora de servicio	Estar en constante comunicación con las empresas prestadoras del servicio

CONCLUSIONS

In this laboratory we learned to identify, analyze and evaluate the risks of interruption that can compromise the provision of critical services in an organization, we also review the risks and classify them from a scale where we will see or not affect our assets and we will observe through from these scales the impact it can have on our company and how we can avoid the interruption of the service as well as we also carry out a mitigation plan for this interruption.

REFERENCES

- Trendmicro, cybercriminals, https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals
- Samsungmobile, securityupdate https://security.samsungmobile.com/securityUpdate.smsb
- First, cvss, https://www.first.org/cvss/v3.0/specification-document
- Android, security bulletin, https://source.android.com/security/bulletin/2021-01-01
- Ncsc, cyberaware, https://www.ncsc.gov.uk/cyberaware/home
- BBC, technology, https://www.bbc.com/news/technology
- OWASP, OWASP Risk Rating Methodology, https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology