

Proyecto Integrador

Integrantes:

Adrián Viscaino

Bryam Barrera

Pedro Illaisaca

Estándares y Legislación para la protección de datos e información

Esta práctica presenta el desarrollo de administración de riesgos, y esta dividida en las siguientes secciones:

- **Resumen Ejecutivo**
- **Identificación de activos**
- **Priorización de activos por orden de importancia**
- **Evaluación de vulnerabilidades**
- **Evaluación del riesgo**
- **Identificación de posibles controles.**

Resumen Ejecutivo

En el siguiente reporte se presentan los siguientes hallazgos los cuales son el resultado del proceso de administración del riesgo realizado dentro de CopBank y revelan su situación actual. En esta etapa se realizaron las siguientes subsecciones:

1. **Identificación de los activos dentro de la organización:** En esta sección podemos determinar los activos que existen dentro de CopBank
2. **Riesgo asociado a los activos:** Se identificaron activos que presentan un alto riesgo, estos activos además son fundamentales para la correcta operación de la organización.
3. **Mitigar el riesgo:** Se establecen controles los cuales son implementados para mitigar cualquier tipo de riesgo dentro de la institución.
4. **Evaluación:** Dentro de la evaluación de riesgos, se toma en cuenta las posibles causas de los riesgos y los posibles eventos que significan un riesgo para los activos. Se determinan 3 categorías de riesgos: Humanos, Equipos, Software. Dentro de cada categoría se identificaron distintas causas para establecer los valores de porcentajes que nos ayudaron con los cálculos. Con esto se puede observar que existen activos con un riesgo alto que deberían ser tratados con distintos controles para reducir este riesgo.
5. **Establecer posibles controles a las vulnerabilidades:** Dentro de esta tarea se procede a brindar posibles soluciones a algunas vulnerabilidades de ciertos activos. Las propuestas planteadas en esta sección se consideran unos supuestos, debido a que implementarlas provocarían grandes costos a la empresa tanto económicamente como en el uso de recursos humanos y de equipos.

Identificación de activos

Nombre del sistema: CopBank

Fecha de evaluación: 05/12/2021

Evaluated por: Bryam Barrera

Activos de información	Clasificación de datos	Impacto a la rentabilidad
Información transmitida:		
Solicitud del cliente, transacciones (SSL)	Confidencial	Crítico
Personal:		
Gerente general	Privado	Crítico
Jefe de tecnologías de información.	Confidencial	Alto

Identificación de activos

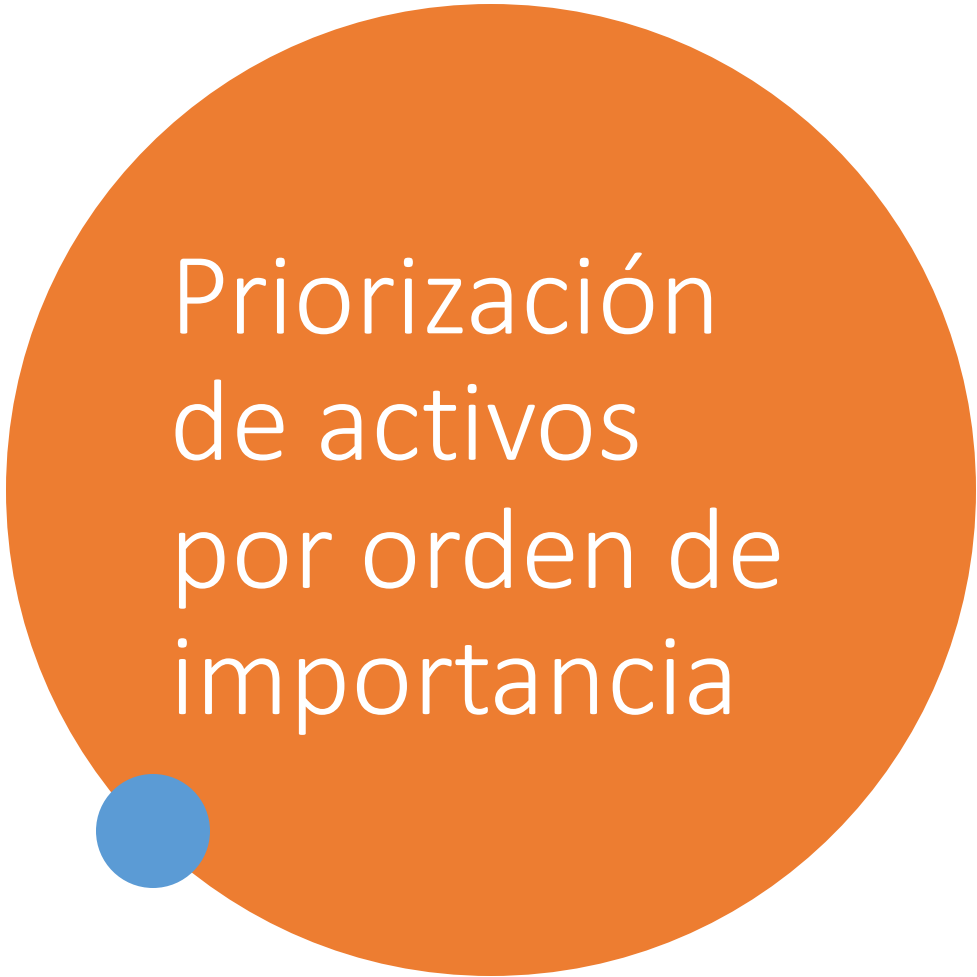
	Clasificación de datos	Impacto a la rentabilidad
Oficina central		
Jefes departamentales (2)	Confidencial	Alto
Departamento A:		
Empleados (2)	Confidencial	Medio
Departamento B:		
Empleados (2)	Confidencial	Medio
Cajeros (5)	Público	Crítico
Sucursal		
Gerente	Privado	Crítico
Cajeros (5)	Público	Crítico
Oficina general		
Empleados (3)	Confidencial	Medio
Oficina de seguridad		
Empleados (2)	Privado	Medio

Activos de la DMZ


Activos DMZ:		Clasificación de datos	Impacto a la rentabilidad
Servidor Web	Público		Crítico
Servidor DNS	Público		Crítico
Servidor FTP	Privado		Medio
Servidor E-mail	Público		Crítico

Identificación de activos

Activos Control de Acceso:	Clasificación de datos	Impacto a la rentabilidad
Firewall	Confidencial	Crítico
Activos oficina de seguridad:		
Servidor de base de datos de respaldo	Privado	Crítico
PC de escritorio	Privado	Medio
Laptop	Privado	Bajo
Switch	Confidencial	Alto
Activos oficina general:		
PC de escritorio (3)	Privado	Medio
Fotocopiadora	Público	Bajo
Impresora	Confidencial	Bajo
Teléfono	Confidencial	Bajo
Activos centro de datos:		
Servidor de aplicaciones	Privado	Crítico
Servidor de base de datos	Privado	Crítico
Activos Departamento A y B:		
PC de escritorio (2)	Privado	Medio
Laptop (2)	Privado	Medio
Impresora (2)	Confidencial	Bajo
Fotocopiadora (2)	Público	Bajo



Priorización de activos por orden de importancia



En este punto, continuamos calificando los activos de acuerdo con los estándares de revisión en el aula. Según el tipo de organización analizada, determinamos el rango de valor de 0.1-1, y el puntaje ponderado superará el 100. En cuanto al criterio de impacto de ingresos y rentabilidad se establece como los más importantes ya que van acorde con la línea de negocio.

Evaluación de vulnerabilidades

- Para la evaluación de vulnerabilidades se procedió a agrupar algunos activos como por ejemplo las fotocopadoras e impresoras, ordenadores de escritorio y portátiles para de este modo generalizar las amenazas.



Evaluacion de Riesgo

Valores utilizados

1. Tabla de porcentajes la estimación del riesgo

Valor del porcentaje	Descripción
1% - 25%	La empresa no tiene controles programados
25% - 50%	La empresa tiene planes de contingencia, pero no son correctos
50% 75%	La empresa tiene planes básicos que funcionan correctamente
75% - 100%	La empresa tiene controles detallados y estructurados.

2. Tabla de porcentajes para la incertidumbre

Valor del porcentaje	Descripción
1% - 25%	Para la empresa no es muy común que se den estos eventos
25% - 50%	Existen pocos eventos que podrían afectar un control de la empresa
50% 75%	La empresa no puede controlar los eventos y por ello los eventos tienen una alta posibilidad de ocurrir
75% - 100%	La empresa no conoce los procedimientos de los eventos y no puede controlar su ocurrencia

Controles existentes

Recursos Humanos

- Errores humanos
 - Confirmación de transacciones, Efectuar transacciones en un horario específico, Uso de log para control de eventos.
- Organización
 - Control de las tareas de cada departamento.
- Filtración de datos
 - Contratos de confidencialidad.
- Robos
 - Control del acceso a la información.
- Ausencias
 - Alternativas al trabajo presencial.

• Controles en los equipos técnicos

- a) Equipos obsoletos
 - Revisión anual de los equipos para una actualización.
- b) Fallos técnicos
 - Ausencia de departamento encargado.
- c) Acceso físico
 - Uso de elementos de autenticación.
- d) Condición climática
 - Estructuras acondicionadas.

• Controles en el software

- Ataques al software
 - Control de cada servicio de los servidores.
- Licenciamientos
 - Uso de programas oficiales.
- Auditoria de configuraciones
- Control de acceso por usuario y contraseña

Consideraciones para la incertidumbre.oles existentes

Recursos Humanos

- Errores humanos
 - Los usuarios siempre usan el software de manera incorrecta.
- Organización
 - Mala relación laboral.
- Filtración de datos
 - Los empleados pueden proveer información confidencial.
- Robos
 - Sistema de seguridad ineficiente
- Ausencias
 - Ausentismo por la situación actual.

• Controles en los equipos técnicos

- Equipos obsoletos
 - Impedimento por recursos.
- Fallos técnicos
 - Infraestructuras deficientes.
- Acceso físico
 - Robo y pérdida de tarjetas.
- Condición climática
 - Cambios climáticos agresivos.

• Controles en el software

- Controles de ataques al software
 - Periodos largos de control de ataques.
- Licenciamientos
 - Usos de programas sin licencia
- Auditoria de configuraciones
 - Mala redacción de manuales.
- Manejo de reportes mensuales
 - Control de acceso por usuario y contraseña
- Posibles robos de cuentas.

Activo	Vulnerabilidad	Valor del activo	Probabilidad de ocurrencia (%)	Riesgo Mitigado (%)	Incertidumbre (%)	Riesgo
Jefes de area	Errores humanos	80	30	60		9.6
	Filtración de datos confidenciales.		40	70	5	11.2
	Nula organización.		30	0	70	40.8
	Falta de comunicación		15	40	5	7.8
PC Escritorio y Laptop	Daños y fallas	67	50	20	35	38.525
	Obsolescencia Tecnológica		70	60	12	24.388
	Catástrofes climáticas		20	30	60	17.42
	Ciberataques		40	75	20	12.06
Servidor Web	Calidad de servicio	100	15	80	10	1.665
	Ataques De Software		60	80	15	7.77
	Denegación de Servicios		50	80	15	6.475
	Obsolescencia		40	60	10	7.4
Servidor Base de datos	Ataques de software.	100	40	85	10	3.7
	Acceso a personal.		15	85	5	1.11
	Intrusión y exposición de los datos.		25	5	10	9.7125
	Error humano		10	90	5	0.555

Posibles controles

Activo 1. Empleados y Cajeros

Vulnerabilidad	Solución
Información dudosa	Presentar de manera pública los datos de las transacciones hechas por los usuarios, como los números de cuenta, los montos de transacción y tipos de transacción.
Errores Humanos	Capacitación constante de las tecnologías utilizadas, supervisión de manera continua a los empleados y una auditoria de manera semestral.

Activo 2. Servidor Web

Vulnerabilidad	Solución
Calidad del servicio	Tener un proveedor de internet de respaldo, de manera que cuando un ISP no pueda proveer el servicio este sea remplazado por el otro.
Equipo Obsoleto	Realizar anualmente o según la necesidad un escalamiento del equipo de manera que mejore sus capacidades y rendimiento, para estar a la par de los equipos nuevos.

Activo 3. PC y Laptops

Vulnerabilidad	Solución
Catástrofes climáticas	Asegurar los equipos de manera que, si se llega a dar un accidente por una catástrofe climática, estos sean cubiertos por la aseguradora, reduciendo las pérdidas de la empresa
Daños y fallas	Trabajar toda la información no crítica de la empresa dentro de un servidor de la nube, de tal forma que si un equipo se llega a dañar la información no se pierde y se puede seguir trabajando desde otro terminal.

Activo 4. Servidor de aplicaciones

Vulnerabilidad	Solución
Ausencia de un servidor de respaldo	Para los usuarios los mismos trámites pueden ser hechos a través del sistema web o dentro de las oficinas, de esa manera cuando haya un fallo en el servidor, las tareas aún se podrían realizar en la oficina.
Configuraciones erróneas	El departamento de seguridad se encargará de desarrollar un manual de configuración del servidor de manera que los técnicos se apegaran a un procedimiento y se puede tener noción de donde se produjeron los fallos.

Activo 5. Servidor de respaldo BD	
Vulnerabilidad	Solución
Acceso a datos	De manera general este servidor solo funcionará como un clúster de datos y no de servicio de manera que no se podrá acceder por medio del motor de la base de datos. Los datos son protegidos por encriptación
Acceso físico	Aparte de la seguridad en la oficina donde se encuentra el servidor, este estará dentro de una estructura protegida a las catástrofes climáticas y con una seguridad extra como puertas de acceso por código.