Carrera de Computación

Título:

Estándares y Legislación para la protección de datos e información

Asignatura:

Seguridad de la información

Estudiantes:

Adrián Viscaino

Bryam Barrera

Pedro Illaisaca

Docente:

Ing. Jennifer Yepez

Cuenca, 07de diciembre de 2021

Informe de la administración del riesgo

1. 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 la situación actual de la organización al 5 de diciembre de 2021.

1.1 Identificación de los activos dentro de la organización

En esta sección podemos determinar que dentro de CopBank se han encontrado alrededor de 21 activos los cuales están repartidos entre activos de información transmitida, personal, activos de la zona desmilitarizada (DMZ), del control de acceso, la oficina de seguridad y oficina general, activos del centro de datos de los departamentos A y B y los activos de red. Por cada uno de estos se determinó un impacto a la rentabilidad de la organización y una clasificación de los datos.

1.2 Riesgo asociado a los activos

De los activos identificados existen 5 activos que presentan un alto riesgo, estos activos además son fundamentales para la correcta operación de la organización. Estos activos son:

1. Servidor Web.
2. Servidor de Base de Datos.
3. Servidor de Aplicaciones.
4. Servidor DNS.
5. Routers, Firewall y Switch.

Estos activos tienen un riesgo asociado representado por un valor dado por la probabilidad de ocurrencia de esa vulnerabilidad, el porcentaje del riesgo, el cual ha sido moderado y el porcentaje de inseguridad de esa vulnerabilidad es decir que a pesar de los controles aplicados no se sabe con certeza que vulnerabilidad pueda ocurrir.

Entre los riesgos asociados a estos activos se encuentran: desastres naturales, errores humanos, robo de los equipos, ataques de software, fallos o errores tanto de software y hardware, sabotaje o vandalismo, exposición de los datos, entre otros detallados más adelante en este reporte.

1.3 Mitigar el riesgo

En esta sección los controles desarrollados e implementados para mitigar los riesgos consisten en la ubicación de los equipos en locaciones dentro de las instalaciones de manera que no se vean afectados ante daños en las instalaciones o posibles desastres naturales.

Dentro de la organización la información se encuentra clasificada, pertenece a un departamento y tiene un responsable a cargo, de manera que cualquier actividad que involucre el acceso a información de carácter confidencial de la organización quedará

registrada en el sistema con la fecha y la persona que tuvo acceso a la información.

Los fallos o errores humanos son una de las vulnerabilidades con más alta probabilidad de ocurrencia, en dónde plan contemplado para mitigar este riesgo consiste en realizar procesos con diferentes fases, para completar con un proceso estas deben ser probadas y debidamente verificadas.

Para la moderación de los riesgos relacionados a los fallos o errores de software, el equipo del departamento de sistemas deberá encargarse de dar una pronta solución a los problemas que ocurriesen y de la misma manera el departamento de mantenimiento se ocupará de los problemas de hardware.

Existen diferentes controles que deberían ser implementados relacionados a los activos de la DMZ y la oficina de seguridad, estos posibles controles se encuentran detallados en el reporte, más específicamente en el punto 6 (Identificación de posibles controles).

1.5 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. Entre los activos más riesgosos están: el gerente, jefes de departamento y empleados. Lo que nos deja concluir que esto se debe a la condición humana que puede provocar fallos y como no se puede conocer las intenciones de una persona esto nos deja vulnerables a sus acciones.

1.6 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. Sin embargo, la implementación de estos ayudaría a reducir los riesgos de los activos.

2. Identificación de activos

Nombre del sistema: CopBank **Fecha de evaluación:** 05/12/2021 **Evaluado 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
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 DMZ:		
Servidor Web	Público	Crítico

Servidor DNS	Público	Crítico
Servidor FTP	Privado	Medio
Servidor E-mail	Público	Crítico
Activos Control de Acceso:		
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
Activos de red:		
Router (9)	Confidencial	Crítico

Justificación

Información transmitida

Las transacciones financieras las cuales realiza el usuario se realizan a través de la aplicación web mediante la solicitud del cliente, estas se manejan bajo protocolos que deban garantizar la confidencialidad de la información del usuario. Las solicitudes de los clientes tienen un impacto crítico en la rentabilidad, donde si la información es incorrecta el funcionamiento de la aplicación web seria errónea.

Personal

Los **gerentes** que manejan la información privada de la empresa y el impacto hacia la rentabilidad son críticos serian una parte vital para la operación de la organización.

Los **jefes departamentales** que manejen información confidencial en su departamento y el impacto a la rentabilidad se alto, estos manejarían todo un departamento el cual debe que estar correctamente gestionado para un correcto funcionamiento en conjunto de esta organización.

Los **empleados** que se encuentran dentro de departamentos u oficinas controlan información confidencial sobre las operaciones de su departamento y su alto impacto hacia la rentabilidad es un nivel inferior referente a los jefes departamentales. Si bien sabemos que es el jefe quien controla el departamento son los empleados los cuales realizan correctamente las tareas que les son asignadas.

Los **cajeros,** estos manejan información pública y su impacto llega a ser crítico pues realizan las transacciones financieras importantes, además de manejar su propia información financiera de su caja.

Activos Control de Acceso:

1. **Firewall:** este nos permitirá tener un mejor control de acceso a los puertos de los servicios que puedan estar expuestos dentro de la DMZ de manera que el impacto para la rentabilidad sea **crítico** ya que si no está debidamente configurado llegaría a estar en riesgo a ataques aprovechando esta vulnerabilidad.

Activos DMZ:

2. **Servidor Web:** Este al ser un servicio de ventas online, el cual debe estar activo las 24 horas recibiendo solicitudes. El impacto del activo es **crítico** pues al existir una inactividad de este servicio los clientes no podrían acceder al catálogo de productos de la empresa. En el peor de los casos debemos procurar que no cuente con más de 15 minutos de inactividad.
3. **Servidor DNS:** Los clientes por lo general cuando ingresan el nombre de la tienda en internet y acceden al primer enlace que se presente, en este caso el impacto es **crítico** pues si el servidor se encuentra inactivo o presenta problemas, los clientes no encontrarán nuestra página web, llegando así a perder clientes.
4. **Servidor email:** Con los correos que existen para el personal y también para facturación electrónica debido a esto es que el impacto es **crítico** ya que al existir algún inconveniente en este servicio muchos clientes sufrieran demoras o en el peor de los casos no llegasen a recibir alguna facturación o tramite, llegando así a causar malestar en los clientes.

5. **Servidor FTP:** Este servicio exclusivo para personal de la empresa, en el que se manejan diferentes tipos de archivos. El impacto es **medio** pues este servicio contará con guías de operación para los empleados los cuales puedan acceder en cualquier horario que se les permita.

Activos Oficina Seguridad:

6. **Servidor BD respaldo:** Realizando una copia de todos los datos del servidor BD principal debido a esto el impacto a la rentabilidad seria **crítico** ya que si el servidor llegase a estar inactivo y que a su vez también ocurran fallas o incluso no realice una copia recurrente de los datos, puede hacer que datos de suma importancia puedan perderse o filtrase de manera negativa.
7. **PC Escritorio**: Este permite conectarse directamente a los recursos de la empresa y trabajar en ellos, donde el impacto de rentabilidad seria **alto** pues al no contar con uno de estos equipos llegaría a darse algún problema en las mejoras del sistema o partes del sistema.
8. **Laptop:** Los empleados al tener un computador personal para realizar multitareas, guardar información personal, etc. Por lo que el impacto es **bajo** ya que no afectaría directamente como un riesgo para la empresa ya que estos dispositivos no cuentan con acceso a los recursos de la empresa.
9. **Switch:** Su nivel de impacto a la rentabilidad es **alto** pues si existiesen fallas en sus protocolos de comunicación no podríamos conectarnos entre los diferentes equipos dentro de esta área.

Equipos y dispositivos

Los computadores que pertenecen a una empresa contienen y manejan información privada sobre trabajos de la empresa, su impacto es **medio** ya que ante un posible problema que esté presente debe ser llevado a mantenimiento, donde se pueda recuperar la información o en el peor de los casos la información llega a perderse.

Las impresoras y teléfonos se clasifican dentro de confidencial debido a que la información es transmitida a través de estos es relativa a la empresa y sus operaciones. Y su impacto es **bajo** ya que si se sucediera algún problema este no compromete a la continuidad de las operaciones de la empresa.

Las fotocopiadoras se encuentran clasificadas como públicas, pues dentro de una cooperativa son utilizadas por todos los empleados y en ciertos casos por los mismos usuarios. Su impacto es **bajo** ya que no representan un problema de consideración.

Activos Centro de Datos

Los activos dentro de esta área tienen una alta importancia ya que para el desarrollo de las actividades diarias de la empresa como el servidor de aplicaciones maneja el sistema financiero como también el sistema propio de la empresa. Juntamente con la base de datos los cuales son necesarios para su desarrollo eficiente, es por eso por lo que el impacto en la rentabilidad es **crítico** pues afectaría potencialmente tanto a los ingresos de la empresa como a las actividades que existan dentro de ellas.

3. Priorización de activos por orden de importancia

En el presente punto se procede a poner una calificación a los activos según los criterios revisados en clase, en función a el tipo de organización analizada establecemos el rango de valores serán de 0.1 - 1 y los puntajes ponderados sobre 100, En cuanto a los criterios el referente a el impacto de los ingresos

y el criterio a impacto en la rentabilidad son los que tiene más importancia ya que está más apegados al giro del negocio.

Activos de información	**Criterio 1:** **Impacto en los ingresos 40**	**Criterio 2:** **Impacto en la rentabilidad 40**	**Criterio 3:** **Impacto en la imagen pública 20**	**Puntuación ponderada** **100**
Información transmitida:				
Solicitud del cliente, transacciones (SSL)	1	1	1	**100**
Personal:				
Gerente general	1	1	1	100
Jefe de tecnologías de información.	1	1	0,4	80
Oficina central				
Jefes departamentales	1	1	0,4	80
Departamento A:				
Empleados (2)	0,4	0,8	1	73
Departamento B:				
Empleados (2)	0,4	0,8	1	73
Cajeros (5)	0,7	0,9	1	87
Sucursal				
Gerente	1	1	1	100
Cajeros (5)	0,7	0,9	1	87
Oficina general				
Empleados (3)	0,4	0,8	1	73
Oficina de seguridad				
Empleados (2)	0,4	0,8	1	73
Activos Oficina General:				
PC de escritorio (3)	0,4	1	0,6	67
Fotocopiadora	0,1	0,4	0,5	33
Impresora	0,1	0,4	0,5	33
Teléfono	0,2	0,5	0,4	37
Activos DMZ:				
Servidor Web	1	1	1	100
Servidor DNS	0,9	1	1	97
Servidor FTP	0,6	0,4	0,4	47
Servidor e-mail	0,6	0,5	0,7	60
Activos Control Acceso:				

Firewall	0,4	0,6	0,8	60
Activos Oficina Seguridad:				
Servidor BD respaldo	0,8	0,7	0,8	77
PC escritorio	0,4	1	0,6	67
Laptop	0,4	1	0,6	67
Switch	0,5	0,7	0,3	50
Activos Centro de Datos:				
Servidor Aplicaciones	1	1	1	100
Servidor Base de Datos	1	1	1	100
Activos Departamento A y B:				
PC de escritorio	0,4	1	0,6	67
Laptop	0,4	1	0,6	67
Impresora	0,1	0,4	0,5	33
Fotocopiadora	0,1	0,4	0,5	33
Activos de red:				
Router	0,5	1	0,3	60

4. Evaluación de vulnerabilidades

En esta sección presentamos las vulnerabilidades con un numero de 4 vulnerabilidades por activo

Posibles vulnerabilidades de Solicitud del usuario, transacciones (SSL)

Amenaza	Posibles Vulnerabilidades
Falsificación de la solicitud	Intercepción y modificación de la solicitud. No validación de los parámetros de la solicitud.
Heartbleed	Permite acceder a información personal incluido claves de cuentas personales
Poodle	Vulnerabilidad presente en una versiones específicas de certificado, y en certificados obsoletos
Freak	Es un tipo de vulnerabilidad donde se pueden ejecutar ataque de hombre en el medio que permite ver cómo está transitando la comunicación

Posibles vulnerabilidades de Gerentes

Amenaza	Posibles Vulnerabilidades
Errores humanos	Uso incorrecto del software y hardware. Ausencia de procesos de capacitación.
Filtración de datos confidenciales.	Formación insuficiente en ciberseguridad.
Nula organización.	Ineficientes procesos de contratación. Muy condescendiente con algunos miembros del grupo. En términos de seguridad de la red.
Hurto	No supervisar a empleados

Posibles vulnerabilidades de jefes

Amenaza	Posibles Vulnerabilidades
Errores humanos	Uso incorrecto del software y hardware. Ausencia de procesos de capacitación.
Filtración de datos confidenciales.	Formación insuficiente en ciberseguridad.
Nula organización.	Ineficientes procesos de contratación. Muy condescendiente con algunos miembros del grupo. En términos de seguridad de la red.
Falta de comunicación	No existe una correcta comunicación con el personal que se encuentra a cargo

Posibles vulnerabilidades Empleados

Amenaza	Posibles Vulnerabilidades
Errores humanos	Uso incorrecto del software y hardware. Ausencia de procesos de capacitación.
Información dudosa	Proviene de fuentes no confiables.
Acciones no autorizadas	Corrupción de los datos. Procesamiento ilegal de los datos. Uso no concedido de los equipos.
Compromiso funcional	Violación de la disponibilidad de los empleados.

Hurto	No supervisar a empleados

Posibles vulnerabilidades Cajeros

Amenaza	Posibles Vulnerabilidades
Fallas de Físicas	Todo suceso relacionado con averías que presentan los cajeros
Robo	Estructura que dispone el cajero no presenta las seguridades insuficientes para evitar robos, ubicación del cajero con poco resguardo policial
Medio para Secuestro de datos	Todo proceso relacionado con clonaciones de tarjetas y acceso a contraseñas
Errores de Software	Uso de herramientas que carecen de alta disponibilidad

Posibles vulnerabilidades de PC de escritorio y laptop

Amenaza	Posibles Vulnerabilidades
Daños y fallas	Funcionamiento incorrecto de software o hardware. Falta de mantenimiento de equipos.
Obsolescencia Tecnológica	Equipos con ciertos años de antigüedad
Catástrofes climáticas	Todos los activos de información dentro de la organización se encuentran vulnerables ante la fuerza de la naturaleza.
ciberataques	Ausencia de instalación y no actualizar antivirus, acceso a páginas inseguras

Posibles vulnerabilidades de impresoras y fotocopiadoras

Amenaza	Posibles Vulnerabilidades
Daños y fallas	Funcionamiento incorrecto de software o hardware. Falta de mantenimiento de equipos.
Obsolescencia Tecnológica	Equipos con ciertos años de antigüedad
Catástrofes climáticas	Todos los activos de información dentro de la organización se encuentran vulnerables ante la fuerza de la naturaleza.

ciberataques	Ausencia de instalación y no actualizar antivirus, acceso a páginas inseguras

Posibles vulnerabilidades de Teléfonos

Amenaza	Posibles Vulnerabilidades
Daños y fallos	Incorrecta manipulación reparaciones en centros no autorizados,
Ataques	Intercepción de comunicación
Escuchas ilegales o interceptación	Uso con redes de otra compañía y desbloqueo de funciones propietario de empresa
Hurto	No supervisar a empleados

Posibles Vulnerabilidades Router, Firewall y Switch

Amenaza	Posibles Vulnerabilidades
Fallos físicos	Incorrecta manipulación de los equipos. Ausencia de protección en la red eléctrica
Catástrofes	Los activos que se encuentran dentro de esta zona se encuentran vulnerables ante cualquier desastre natural.
Errores Humanos	La mala administración o configuración de los protocolos de comunicación.
Sabotaje	Atacantes con objetivo de causar daños
Obsolescencia	Límite de garantía expedido.

Posibles Vulnerabilidades Servidor Web

Amenaza	Posibles Vulnerabilidades
Calidad de servicio	Servicio de proveedores de internet tiene constantes caídas y servicios intermitentes

Ataques De Software	Se basa en enviar al servidor una cantidad abrumadora de paquetes ping con la finalidad de sobrecargar el servidor y ocasionar una parada del servicio.
Denegación de Servicios	Ciberdelincuentes realizan ataques a determinadas entidades
Obsolescencia	Equipos con cierto tiempo de antigüedad

Posibles Vulnerabilidades Servidor Base Datos

Amenaza	**Posibles vulnerabilidades**
Ataques de software.	Ataques de denegación de servicio. SQL injection
Acceso a personal.	Ausencia de administración de usuarios y sus debidos permisos
Intrusión y exposición de los datos.	Bases de datos desactualizadas. Datos almacenados sin cifrar. Bases de datos con parámetros de configuración por defecto.
Error humano	Errores en la manipulación de la base de datos. Personal de soporte con poca experiencia.

Posibles Vulnerabilidades Servidor DNS

Amenaza	Posibles Vulnerabilidades
Caída de Servicio	Cualquier tipo de evento que ocasione que el servicio sea interrumpido falla eléctrica, error de certificado
Error Humano	Configuración deficiente o mala manipulación de las direcciones ip
Ataque	Un envenenamiento de cache DNS enviando direcciones IP que no existen a los usuarios, secuestro de direcciones

Deficiencia de mantenimiento	No chequear el funcionamiento y revisión de posibles fallas que se puedan presentar

Posibles Vulnerabilidades Servidor E-mail

Amenaza	Posibles Vulnerabilidades
Catástrofes	Ubicación Geográfica con mayores probabilidades de presentarse un desastre natural
Intercepción de Datos	Procesos que realiza el correo conlleva a que datos puedan ser interceptados poniendo en peligro la seguridad de la información
Spam	Una mala gestión de este tipo de correo puede ocasionar que ataques como phishing puedan ser ejecutados de una manera más fácil
Malware	En caso de presentarse servidores infectados con un virus que use correo como medio de propagación

Posibles Vulnerabilidades Servidor Aplicaciones

Amenaza	Posibles Vulnerabilidades
Ausencia de un servidor alterno	Al usar un solo servidor de aplicaciones se corre el riesgo de cuando ocurre un error con el servidor principal todo el sistema se paralice
Catástrofes	Ubicación Geográfica con mayores probabilidades de presentarse un desastre natural

Configuración Deficiente	La mala configuración o inclusive uso de configuración básica que no es capaz de evitar problemas.
Comunicaciones inseguras	Ausencia de uso de cifrado en contraseñas de acceso y no usar certificados de seguridad

Posibles Vulnerabilidades Servidor FTP

Amenaza	Posibles Vulnerabilidades
Catástrofes	Ubicación Geográfica con mayores probabilidades de presentarse un desastre natural
Configuración ineficiente	Configuración incorrecta del servidor o configuraciones básicas
Acceso a información confidencial	Las configuraciones no exigen el ingreso de contraseñas fuertes a los usuarios
Ataques	Ingreso de personal no autorizado al área de los servidores. Ausencia de dispositivos de vigilancia.

Posibles Vulnerabilidades de Servidor BD respaldo

Amenaza	Posibles Vulnerabilidades
Catástrofes	Ubicación Geográfica con mayores probabilidades de presentarse un desastre natural
Error Humano	Ineficiente configuración del servidor que alberga la base de datos
Acceso a datos	Ausencia en la configuración de roles de usuarios y niveles de permisos.
Acceso Físico	Ausencia de personal de vigilancia y dispositivos de video en el lugar donde se encuentran los servidores.

5. Evaluación de riesgo

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

Activo	Vulnerabilidad	Valor del activo	Probabilidad de ocurrencia (%)	Riesgo Mitigado (%)	Incertidumbre (%)	Riesgo
Gerente General	Errores humanos	100	30	50	10	***18***
	Filtración de datos confidenciales.		40	40	80	***56***
	Nula organización.		30	0	70	***51***
	Hurto		20	10	10	***20***
Jefes de área	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***
Empleados y cajeros	Errores humanos	87	60	30	10	***41.76***
	Información dudosa		25	80	5	***5.4375***
	Acciones no autorizadas		20	80	3	***4.002***
	Compromiso funcional		10	75	15	***3.48***
	Hurto		20	85	5	***3.48***
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***
Impresora y Fotocopiadora	Daños y fallas	33	40	20	5	***11.22***
	Obsolescencia Tecnológica		25	60	12	***4.29***
	Catástrofes climáticas		20	30	60	***8.58***
	ciberataques		5	75	20	***0.7425***
Teléfono	Daños y fallos	37	30	20	35	***12.765***
	Ataques		5	10	3	***1.7205***
	Escuchas ilegales o interceptación		25	20	75	***14.3375***
	Hurto		5	20	80	***2.96***
Router, Firewall y Switch	Fallos físicos	60	45	20	20	***27***
	Catástrofes		20	30	60	***15.6***
	Errores Humanos		15	45	15	***6.3***
	Sabotaje		70	25	20	***39.9***
	Obsolescencia		50	60	15	***16.5***
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***
Servidor DNS	Caída de Servicio	97	30	80	5	***2.775***
	Error Humano		10	70	20	***1.85***
	Ataque		25	85	20	***3.2375***
	Deficiencia de mantenimiento		30	90	10	***2.22***
Servidor E-mail	Catástrofes	60	20	30	60	***9.62***
	Intercepción de Datos		20	50	20	***5.18***
	Spam		60	80	35	***12.21***
	Malware		30	80	5	***2.775***
Servidor de aplicaciones	Ausencia de un servidor alterno	100	30	90	10	***2.22***
	Catástrofes		20	10	10	***7.4***
	Configuración Deficiente		30	30	70	***15.54***
	Comunicaciones inseguras		40	60	20	***8.88***
Servidor FTP	Catástrofes	47	20	30	60	***9.62***
	Configuración ineficiente		30	75	10	***3.885***
	Acceso a información confidencial		25	90	5	***1.3875***
	Ataques		10	80	15	***1.295***
Servidor BD Respaldo	Catástrofes	77	20	30	60	***9.62***
	Error Humano		40	50	50	***14.8***
	Acceso a datos		60	85	10	***5.55***
	Acceso Físico		60	80	20	***8.88***

Controles tomados en cuenta para la asignación de porcentajes

- **Controles en los factores humanos**

1) Errores humanos

Este tipo de vulnerabilidades tiene controles de distinto tipo para intentar mitigar su impacto, se tiene controles: de confirmación antes de realizar cualquier transacción en los sistemas, permite asegurar los datos ingresados; los procesos de transacciones de montos altos son procesados al final de la jornada diaria, dando tiempo a cualquier cancelación; manejo de log en el sistema, permitiendo verificar todo evento en el sistema.

2) Organización

Se mantienen reuniones semanales para verificar la organización y cumplimiento de tareas del personal de la empresa, verificando que cada departamento cumpla de manera eficaz y eficiente sus tareas.

3) Filtración de datos

Al inicio de un contrato los empleados deben firmar un acuerdo de confidencialidad, con esto se tiene un respaldo legal de protección de la información de la empresa.

4) Robos

Todos los procesos son debidamente asignados según el grado de criticidad de la información, con ello se puede tener un control de las personas que acceden a los datos.

5) Ausencias

La empresa cuenta con planes de contingencia para los distintos motivos de ausencia de los empleados, pudiendo ser: home office, remplazos por compañeros del departamento, buenos tiempos de manejo en los procesos para tener una ventaja de perder un día de trabajo, personal capacitado para evitar que un empleado sea indispensable.

- **Controles en los equipos técnicos**

a) Equipos obsoletos

La empresa tiene como política hacer una revisión anual de los equipos, para verificar nuevas opciones de renovación y el beneficio de esto.

b) Fallos técnicos

La empresa n o cuenta con un departamento de Tics o mantenimiento para una pronta respuesta a fallos por ello los porcentajes de mitigación son bajos

c) Acceso físico

Dentro de cada departamento existe un control de ingreso por tarjetas de identificación, con eso se mantiene un acceso restringido por personal.

d) Condición climática

La empresa esta adecuada a las catástrofes climáticas, teniendo características como: estructura antisísmica, piso falso para inundaciones, sistemas de apagado de incendios.

- **Controles en el software**

1) Controles de ataques al software

Mensualmente el departamento de seguridad de la información mantiene controles en los servidores para comprobar buenas prácticas de gestión en servidores, como puertos abiertos, servicios en ejecución, consumos excesivos de recursos, estado de los servicios y reportes de fallos.

2) Licenciamientos

Para asegurar que no exista código malicioso en los programas la empresa tiene políticas de no usar software con cracks o activadores, si no únicamente software con licencias.

3) Auditoria de configuraciones

Cada 6 meses la empresa mantiene controles de auditoría a todos los equipos y sus sistemas, para controlar una buena configuración de los mismos.

4) Manejo de reportes mensuales

Mensualmente se presentará un informe de los fallos del sistema y la solución para determinar si son casos especiales o programados en el funcionamiento del sistema.

5) Control de acceso por usuario y contraseña

Para evitar que empleados y usuarios accedan a información crítica se maneja un acceso por usuario y contraseña a los sistemas, de esa forma se controla y protege la información delicada.

Consideración para la asignación del valor de la incertidumbre

- **Controles en los factores humanos**

a) Errores humanos

Aunque se realicen planes para controlar los errores humanos se debe tener como principal idea que los usuarios siempre usaran el software de manera incorrecta.

b) Organización

Los valores asignados aquí son altos debido a que los empleados presentan mala relación con los jefes departamentales.

c) Filtración de datos

La información tecnológica se encuentra categorizada por acceso de usuario y contraseña, sin embargo, los empleados se encuentran dentro de un mismo espacio en las oficinas lo que puede provocar un acceso no autorizado.

d) Robos

Existen sitios donde las cámaras de seguridad no tienen acceso por ello no se puede controlar todas las áreas de la empresa.

e) Ausencias

La actual epidemia provoca retrasos o ausencias por parte de los empleados usando esto como excusa.

- **Controles en los equipos técnicos**

a) Equipos obsoletos

EL cambio de equipos se hará cuando el presupuesto lo permita, por ello existe cierta incertidumbre de si los equipos serán cambiados a tiempo.

b) Fallos técnicos

Las instalaciones no son hechas de manera correcta, por lo que puede provocar componentes electrónicos averiados.

c) Acceso físico

Las tarjetas y códigos de acceso pueden ser tomadas y descubiertos por el resto de los empleados.

d) Condición climática

Aunque las estructuras estén adecuadas al clima, este es muy impredecible y la estructura presentara fallos para soportar una catástrofe grave.

- **Controles en el software**

a) Controles de ataques al software

Al realizar controles de manera mensual puede existir un ataque que no será visto hasta la auditoria próxima.

b) Licenciamientos

Los usuarios de los terminales pueden hacer uso de programas pirateados poniendo en riesgo a los equipos.

c) Auditoria de configuraciones

Aunque existan manuales, estos pueden ser no entendidos por todos por lo que aún existe la probabilidad de un equipo mal configurado.

d) Manejo de reportes mensuales

Al ser una tarea tediosa puede ser pasada por alto por el departamento de seguridad.

e) Control de acceso por usuario y contraseña

Con ingeniería social los usuarios y contraseñas pueden ser fácilmente descubiertas.

6. Identificación de 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 critica 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.