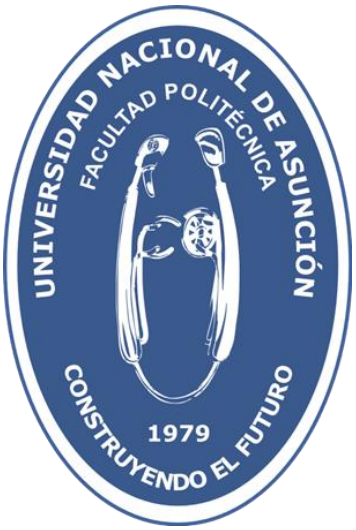
Universidad Nacional de Asunción

Facultad Politécnica



Laboratorio - Análisis de Riesgo

Integrantes:

- Marcos Raúl Flores Duarte
- Kevin Mathias Galeano Saldívar
- Jazmín Lucero Ruiz Díaz Villagra

Carrera: Ingeniería en Informática

Asignatura: Ciberseguridad

Profesor: Nicolás Pereyra

San Lorenzo – 2025

Fase 1. Definir el alcance

El primer paso a la hora de llevar a cabo el análisis de riesgo es establecer el alcance del estudio.

Proceso	Relación con el cliente
Procedimiento	Venta
Objetivo	Gestionar el cobro y despacho del cliente
Alcance	Desde la presentación de producto seleccionado por el cliente en la caja Hasta el despacho del cliente en la caja
Secuencia	Gestión de cobro y despacho del cliente
Definiciones	Cliente: Persona registrada en el sistema de cobro Producto: producto disponible en las instalaciones al alcance del cliente Medio de Pago: sistema de pago disponibilizado al cliente para la venta de productos y con los cuales la empresa tiene acuerdos vigentes. Cajero: Personal de la empresa encargado de verificar el producto vendido y registrar el proceso de venta. Empaquetador: Personal de la empresa encargado de acomodar los productos habilitados para ser retirados por el cliente. COBRA: Sistema de gestión de ventas de la empresa Código QR: Etiquetas con representación gráfica de información de productos disponibles para la venta Supervisor: Personal encargado de autorizar pasos identificados y no identificados dentro de este procedimiento
Cambios en la versión	Versión inicial
Fecha de vigencia	1/2/2022

Nro	Actividades	Descripción de la actividad	Registro generado	Responsable
1	Presentar producto en la caja	En la caja habilitada el Cliente presenta los productos que va a adquirir.	RUC o CI en COBRA	Cajero Supervisor
		El cajero solicita que el cliente ingrese su RUC o CI. Si no posee, se registra en COBRA como cliente 99.		
2	Preparar venta	El cajero solicita se indique uno de los medios de pago disponibles. En caso de falla de un medio de pago se solicita optar por otro. La última opción es el efectivo. Si ninguna de las opciones disponibles no es aceptado por el Cliente se cancela la venta y se registra el motivo en COBRA.	Factura	Cajero Supervisor
		A través del lector QR se registraen COBRA cada producto presentado por el cliente. En caso de falla del lector, se registra manualmente el número de identificación del producto ubicado al lado del código QR. En caso de falla para usar COBRA se utiliza el talonario de factura manual de venta y se utiliza la calculadora manual de respaldo ubicado en la caja para realizar las sumas. El precio de los productos se obtiene del listado impreso generado a la mañana.		

		Se confirma con el cliente si está dispuesto a proceder al pago. Si hay cambios, se debe generar una operación inversa del item que será cambiado. Se debe tener autorización del supervisor y registrar el motivo en COBRA. En caso de pago mediante factura manual se genera un item con el mismo valor, pero negativo. Finalmente se genera el pago. En caso de falla del medio de pago, se opta por otro medio hasta la opción de pago en efectivo. Si el cliente no acepta, se genera en COBRA la reversión. En caso de factura manual, se anula la factura. Ambos casos con autorización del supervisor y se registra.		
3	Despachar productos	Cuando el pago es aceptado, el Empaquetador prepara los productos para ser retirados por el cliente. El empaquetador verifica que el producto esté en buenas condiciones. En caso de identificar problemas, se genera una nota interna de cambio con el Depósito y se informa al cliente. En caso de no disponibilidad se informa al cliente de la situación. El supervisor genera una nota de crédito por el producto con problemas. Los productos se entregan con la conformidad del cliente y se sella la factura.	Factura Nota interna de Cambio Nota de Crédito	Empaquetador Supervisor

Consideraciones Generales

El supervisor debe registrar las situaciones identificadas y no identificadas en El libro de situaciones
El cajero debe cerrar la caja en caso que no se encuentre el supervisor

Fase 2. Identificar los activos

Una vez definido el alcance, se identifican los activos más importantes que guardan relación con el proceso de estudio.

	Identificador	Activo	Aplicación
Web	A1	Router	SI
	A2	Switch	SI
Cobros	B1	Cobra (Servidor)	SI
	B2	Supervisor (PC)	SI
	B3	Caja 1 (PC)	SI
	B4	Caja 2 (PC)	SI
	B5	Caja 3 (PC)	SI
Clientes	C1	WiFi	SI
	C2	Smarphone Cliente	SI

Fase 3. Identificar / seleccionar las amenazas

Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos.

En el caso de este proceso, se identificaron las siguientes amenazas:

- Fuego
- Daños por agua
- Fuga de información
- Corte del suministro eléctrico
- Acceso no autorizado
- Errores de los usuarios

Fase 4. Identificar vulnerabilidades y salvaguardas

La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades.

Amenaza/Activo	A1	A2	B1	B2	B3	B4	B5	C1	C2
Fuego	SI	SI	SI	SI	SI	SI	SI	SI	NO
Daños por agua	SI	SI	SI	SI	SI	SI	SI	SI	NO
Desastres naturales	NO	NO	NO	NO	NO	NO	NO	NO	NO
Fuga de información	SI	SI	SI	SI	SI	SI	SI	SI	NO
Introducción de falsa información	NO	NO	NO	NO	NO	NO	NO	NO	NO
Alteración de la información	NO	NO	NO	NO	NO	NO	NO	NO	NO
Corrupción de la información	NO	NO	SI	NO	NO	NO	NO	NO	NO
Destrucción de información	NO	NO	NO	NO	NO	NO	NO	NO	NO
Interceptación de información (escucha)	NO	NO	NO	NO	NO	NO	NO	NO	NO
Corte del suministro eléctrico	SI	SI	SI	SI	SI	SI	SI	SI	NO
Condiciones inadecuadas de temperatura o humedad	NO	NO	NO	NO	NO	NO	NO	NO	NO
Fallo de servicios de comunicaciones	NO	NO	NO	NO	NO	NO	NO	NO	NO
Interrupción de otros servicios y suministros esenciales	NO	NO	NO	NO	NO	NO	NO	NO	NO
Desastres industriales	NO	NO	NO	NO	NO	NO	NO	NO	NO
Degradación de los soportes de almacenamiento de la información	NO	NO	NO	NO	NO	NO	NO	NO	NO
Difusión de software dañino	NO	NO	NO	NO	NO	NO	NO	NO	NO
Errores de mantenimiento / actualización de programas (software)	NO	NO	NO	NO	NO	NO	NO	NO	NO
Errores de mantenimiento / actualización de equipos (hardware)	NO	NO	NO	NO	NO	NO	NO	NO	NO
Caída del sistema por sobrecarga	NO	NO	NO	NO	NO	NO	NO	NO	NO
Pérdida de equipos	NO	NO	NO	NO	NO	NO	NO	NO	NO
Indisponibilidad del personal	NO	NO	NO	NO	NO	NO	NO	NO	NO
Abuso de privilegios de acceso	NO	NO	NO	NO	NO	NO	NO	NO	NO
Acceso no autorizado	SI	SI	NO	NO	NO	NO	NO	NO	NO
Errores de los usuarios	NO	NO	SI	NO	NO	NO	NO	SI	NO
Errores del administrador	NO	NO	NO	NO	NO	NO	NO	NO	NO
Errores de configuración	NO	NO	NO	NO	NO	NO	NO	NO	NO
Denegación de servicio	NO	NO	NO	NO	NO	NO	NO	NO	NO
Robo	NO	NO	NO	NO	NO	NO	NO	NO	NO
Indisponibilidad del personal	NO	NO	NO	NO	NO	NO	NO	NO	NO
Extorsión	NO	NO	NO	NO	NO	NO	NO	NO	NO
Ingeniería social	NO	NO	NO	NO	NO	NO	NO	NO	NO

Fase 5. Evaluar el riesgo

Para cada par activo-amenaza, se estima la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría.

ANÁLISIS DE RIESGOS				
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Router	Fuego	Medio (2)	Alto (3)	6
Router	Daños por agua	Medio (2)	Medio (2)	4
Router	Fuga de información	Bajo (1)	Alto (3)	3
Router	Corte del suministro eléctrico	Medio (2)	Medio (2)	4
Router	Acceso no autorizado	Bajo (1)	Alto (3)	3
Switch	Fuego	Medio (2)	Alto (3)	6
Switch	Daños por agua	Bajo (1)	Alto (3)	3
Switch	Fuga de información	Medio (2)	Medio (2)	4
Switch	Corte del suministro eléctrico	Medio (2)	Medio (2)	4
Switch	Acceso no autorizado	Medio (2)	Medio (2)	4
Cobra (Servidor)	Fuego	Medio (2)	Medio (2)	4
Cobra (Servidor)	Daños por agua	Medio (2)	Medio (2)	4
Cobra (Servidor)	Fuga de información	Medio (2)	Medio (2)	4
Cobra (Servidor)	Corrupción de la información	Medio (2)	Medio (2)	4
Cobra (Servidor)	Corte del suministro eléctrico	Medio (2)	Medio (2)	4
Cobra (Servidor)	Errores de los usuarios	Medio (2)	Medio (2)	4
Supervisor (PC)	Fuego	Bajo (1)	Bajo (1)	1
Supervisor (PC)	Daños por agua	Bajo (1)	Bajo (1)	1
Supervisor (PC)	Fuga de información	Bajo (1)	Alto (3)	3
Supervisor (PC)	Corte del suministro eléctrico	Medio (2)	Bajo (1)	2
Caja 1 (PC)	Fuego	Bajo (1)	Bajo (1)	1
Caja 1 (PC)	Daños por agua	Bajo (1)	Bajo (1)	1
Caja 1 (PC)	Fuga de información	Medio (2)	Medio (2)	4
Caja 1 (PC)	Corte del suministro eléctrico	Medio (2)	Bajo (1)	2
Caja 2 (PC)	Fuego	Bajo (1)	Bajo (1)	1
Caja 2 (PC)	Daños por agua	Bajo (1)	Bajo (1)	1
Caja 2 (PC)	Fuga de información	Medio (2)	Medio (2)	4
Caja 2 (PC)	Corte del suministro eléctrico	Medio (2)	Bajo (1)	2
Caja 3 (PC)	Fuego	Bajo (1)	Bajo (1)	1
Caja 3 (PC)	Daños por agua	Bajo (1)	Bajo (1)	1
Caja 3 (PC)	Fuga de información	Medio (2)	Medio (2)	4
Caja 3 (PC)	Corte del suministro eléctrico	Bajo (1)	Bajo (1)	1
WiFi	Fuego	Bajo (1)	Medio (2)	2
WiFi	Daños por agua	Bajo (1)	Medio (2)	2
WiFi	Fuga de información	Medio (2)	Medio (2)	4
WiFi	Corte del suministro eléctrico	Medio (2)	Medio (2)	4
WiFi	Errores de los usuarios	Bajo (1)	Medio (2)	2

Fase 6. Tratar el riesgo

Una vez calculado el riesgo, se deben tratar aquellos riesgos que superen el límite establecido:

- Riesgo ≤ 4: La organización considera el riesgo poco reseñable.
- Riesgo > 4: La organización considera el riesgo reseñable y debe proceder a su tratamiento.

Algunas estrategias que pueden ser aplicadas para el tratamiento de los riesgos reseñables que se han obtenido en la fase anterior son:

- Monitoreo constante: supervisar la infraestructura con herramientas de seguridad de forma constante para detectar anomalías en el router y switch. Implementar alertas en tiempo real para incendios y sobrecalentamiento.
- Capacitación: formar al personal en prevención y respuesta ante incidentes de seguridad y fallas en la red para garantizar la continuidad del sistema COBRA y el procesamiento manual de ventas sin afectar al cliente.
- Redundancia y respaldo: implementar conexiones de respaldo para garantizar la operatividad del sistema y la validación de pagos en caso de fallos en la red principal.
- Pruebas y simulacros: realizar simulaciones de fallos en la red para evaluar la efectividad de los planes de respuesta, asegurando que el personal esté preparado para actuar con rapidez y minimizar el impacto en las operaciones.