Threat and Vulnerability Identification Template

Use this template to identify key assets, associated threats, potential vulnerabilities, and initial ideas for mitigation. This exercise helps build foundational skills in cybersecurity risk assessment.

Asset Name	Asset Description	Associated Threats	Potential Vulnerabilities	Mitigation Notes
Dispositivos de empleados (BYOD)	Acceso a dispositivos propios para su uso en sistemas corporativos y datos críticos de clientes.	Malware (acceso no autorizado al dispositivo del empleado)	La política BYOD es débil ya que no está fuertemente gestionada ni tampoco dispone de segregación de datos.	Exigir antivirus actualizado, además de implementar MDM (mobile management)
Credenciales de empleados a través de un control por roles (RBAC)	Acceso a sistemas internos como AWS, SAP, Salesforce mediante (RBAC)	Ingeniería social/phishing (correo, suplantación de identidad)	Existe evidencia de un ataque de phishing del año 2023 que fue dirigido a representantes de servicio al cliente	Implementación de MFA (autenticación en dos factores para todos los dispositivos) y realizar simulaciones de phishing
Datos de Clientes (CRM/Marketing)	Bases de datos PII con nombres, correos electrónicos, teléfonos, historial de compras provenientes del Salesforce y proveedores externos	Ataque a la cadena de suministro a través del proveedor externo	Existe evidencia de una filtración por un proveedor externo que condujo la filtración de datos de correo electrónico de 5000 clientes el año 2025 (hay poca protección a los datos)	Realizar evaluaciones de riesgos a proveedores previamente, y cifrar datos de clientes en caso de filtraciones

Risk Criteria

The below explains what each item in the Risk Assessment means.

Criteria	Description
Risk Description	Detailed explanation of the scenario, what could go wrong, and why it matters.
Assets at Risk	The information, system, or service impacted (e.g. customer data, VDI environment).

Criteria	Description
Threat	Who or what could cause the risk (e.g., insider, cybercriminal, accident, malware). The action or event (e.g., data exfiltration, privilege misuse, physical theft).
Vulnerability	Weakness – the gap or condition that enables the threat (e.g., extended idle session, clipboard sharing).
Existing Controls	Current safeguards in place (e.g., MFA, logging, endpoint DLP).
Inherent Risk Rating	Risk level before any mitigations are applied.
Residual Risk Rating	Risk level after current controls are considered.
Likelihood	The probability of occurrence (e.g., Rare, Possible, Likely).
Consequence	Severity – level of damage if realised (e.g., Minor, Moderate, Major, Extreme).
Rating	The outcome of the risk likelihood and consequence evaluation.
Mitigations	Treatment Plan – actions to reduce, transfer, avoid, or accept the risk.
Risk Owner	Person or role accountable for managing the risk (e.g., the person who uses the software)

Risk Assessment

Complete this assessment for at least 3 risks.

Risk Details			
Risk ID	R-001	**Date Identified**	12/11/2025
Risk Title	Dispositivos de empleados (BYOD)	**Review Date**	
Risk Identification			
Risk Description	Un empleado descarga malware en su dispositivo, lo que puede conducir a acceso no autorizado del dispositivo. El atacante puede tener acceso a las redes internas a través de VPN		
Assets at Risk	Datos de clientes, inventario (SAP), Salesforce		

Threat	Malware/Cybercriminal	
Vulnerability	Falta de controles de seguridad/Autenticación dos factores	
Existing Controls	Politica de uso aceptable, VPN para red interna	
Inherent Risk Analysis		
Likelihood	**Consequence**	**Inherent Risk Rating**
Probable	HIGH	Ya que si acceden por VPN, pueden acceder a credenciales del sistema y comprometer el sistema con ransomware
Residual Risk Analysis		
Likelihood	**Consequence**	**Residual Risk Rating**
Improbable	LOW	Ya que si se implementa autenticación en dos factores, se reduce considerablemente el acceso no autorizado a la red interna
Risk Treatment		
Mitigations	Implementar autenticación MFA para todo dispositivo	
Risk Monitoring and Review		
Risk Owner	**Chief Information Officer (CIO) o IT Manager**	

To	CISO (Chief Information Security Officer), IT Manager
Cc	Analista de seguridad
Bcc	Analista de seguridad
Subject	**Subject:** Informe de Evaluación de Riesgos y Mitigación - Política BYOD

Estimados,

Adjunto encontrarán la evaluación de riesgos detallada para el entorno de Retail Nova.

Resumen del hallazgo principal (Riesgo R-001): Hemos identificado un **riesgo alto** asociado al uso de dispositivos personales (BYOD) sin gestión centralizada. Actualmente, un dispositivo infectado podría acceder a la red interna vía VPN, comprometiendo datos en SAP y Salesforce.

Plan de Tratamiento: Proponemos implementar las siguientes mitigaciones inmediatas para reducir este riesgo a un nivel **Bajo/Medio**:

1. **MFA Obligatorio:** Implementar autenticación multifactor para todas las conexiones VPN.
2. **Solución MDM:** Desplegar software de gestión de dispositivos móviles para segregar datos corporativos.

Quedo a la espera de su aprobación para proceder con la hoja de ruta de implementación.

Atentamente, Alex Mellado Gamboa

Cybersecurity Risk Prioritisation Matrix

Understanding the Likelihood Rating

The table below provides the categories and ratings for likelihood:

Likelihood Ratings	Description	Criteria
Rare (1)	Exceptional circumstances only	May occur only in very unusual situations
Unlikely (2)	Possible, but not expected	Could happen but not typical; requires specific conditions (e.g. targeted phishing bypassing all filters).
Possible (3)	Might occur at some point	Has occurred in similar organisations; realistic but not frequent (e.g. ransomware attempt on enterprise endpoint).
Likely (4)	Will probably occur in most circumstances	Expected to happen periodically (e.g. phishing emails, credential stuffing attempts).
Almost Certain (5)	Expected to occur frequently	Has occurred multiple times, highly predictable (e.g. malware probes, daily scanning activity).

Understanding the Consequence Ratings Table

The table below provides the categories and ratings for impacts:

Consequence Rating	Description	Criteria
Insignificant (1)	Negligible impact	No compromise of sensitive data, no disruption, minimal financial or reputational impact.
Minor (2)	Small impact	Limited operational disruption; minimal data exposure (non-sensitive data); easily contained.
Moderate (3)	Noticeable impact	Partial service disruption; limited sensitive data exposure; moderate cost or compliance breach.

Major (4)	Severe impact	Significant outage of critical systems; large-scale sensitive data breach; regulatory non-compliance with penalties.
Extreme (5)	Catastrophic impact	Extended enterprise-wide outage; compromise of PROTECTED/SECRET data; severe financial/reputational damage; possible criminal or regulatory prosecution.

The 5x5 Risk Matrix

Use this 5x5 risk matrix to evaluate and prioritise cybersecurity risks. For each identified risk, assess its likelihood (1 = Rare, 5 = Almost Certain) and impact (1 = Insignificant, 5 = Critical). Plot the risk in the matrix and use the result to guide mitigation priorities.

Risk Levels

Likelihood ↓ Impact →	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
5 – Almost Certain	**MEDIUM**	**HIGH**	**HIGH**	**EXTREME**	**EXTREME**
4 – Likely	**MEDIUM**	**MEDIUM**	**HIGH**	**HIGH**	**EXTREME**
3 – Possible	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**	**HIGH**
2 – Unlikely	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**
1 – Rare	**LOW**	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**

- **Low** – Acceptable; manage by routine controls and monitoring.
- **Medium** – Requires management attention; additional controls may be needed.
- **High** – Significant; must be treated with priority, monitored closely, and escalated to senior management.
- **Extreme** – Unacceptable; immediate executive-level attention and remediation required.

Tips for Completing the Matrix

- Start by identifying the risk scenario (e.g., data breach, system outage).
- Assign a likelihood score based on how often this type of risk occurs.

- Assign an impact score based on potential damage to operations, reputation, or finances.
- Use the matrix to prioritise: risks in the top-right corner (high likelihood and impact) need urgent attention.