65tg

|  |  |  |
| --- | --- | --- |
| **Nombre / Número del Proyecto:** | **Preparado por:** | **Fecha:** |
| **Digitalización de Tienda** | **Harold Castillo** | **28/3/2023** |
| **Líder de Proyecto (LP):** | | **Patrocinador del Proyecto:** |
| Francela Ortiz | | **Sergio Gamboa** |

Identificación de posibles debilidades y amenazas que pueden afectar el éxito del proyecto, en conjunto con las contramedidas a tomar en el caso de que existieran, con el fin de reducir el nivel de riesgo hasta un nivel aceptable. Buscando un balance eficiente en costos, entre las medidas a tomar durante el desarrollo del proyecto y el impacto que podrían ocasionar las amenazas.

Para la asignación y peso de los riesgos se deberá de tomar en cuenta la siguiente escala de clasificación:

- Se utilizará para calificar el impacto y la vulnerabilidad como 1 la escala más Baja y 3 la escala más Alta; a donde sí:

Campo Total es Menor o Igual que 2 el riesgo es BAJO

Campo Total es Mayor que 2 pero Menor o Igual que 4 el riesgo es MEDIO

Campo Total es Mayor que 4 pero Menor o Igual que 6 el riesgo es ALTO

| **Tipo** | **Nombre del Riesgo** | **Impacto** | **Vulnerabilidad** | **Total** | **Descripción de la Mitigación** |
| --- | --- | --- | --- | --- | --- |
| 1 | Caída de los enlaces de comunicación | Alto | Física | 6 | Tener enlaces redundantes con diferentes proveedores y asegurar que este distribuidos en diferentes rutas |
| 2 | Falta de disponibilidad del servidor | Alto | Lógica | 5 | Realizar copias de seguridad periódicas de los datos del servidor |
| 3 | Riesgo de Calidad de software,  El software no puede producir resultados que no cumplan con los estándares de calidad esperados. | Medio | Lógica | 4 | Definir los requisitos de calidad del software desde el principio del proyecto y asegurarse de que todos los miembros del equipo estén alineados. |
| 4 | Fallas en la parte física (Hardware) de servidores, data-center o servicio de hosting | Alto | Física |  | incluir la transferencia de servicios a otro servidor teniendo en cuenta una alta disponibilidad como plan de contingencia y de paso contar con copias de seguridad para pronta reacción |
| 5 | Riesgo de Seguridad (USB habilitado) | Medio | lógica | 3 | Inhabilitar la lectura y escritura de las unidades de almacenamiento externas |
| 6 | Filtraciones y violaciones de datos | Alto | Lógica | 6 | Cifrar los datos sensibles, utilizar controles de acceso estrictos, mantener copias de seguridad periódicas y realizar auditorías de seguridad frecuentes para identificar vulnerabilidades. |
| 7 | Phishing y ataques de ingeniería social | Alto | Lógica | 6 | Formar a los empleados para que reconozcan las tácticas de phishing e ingeniería social, implantar soluciones de seguridad para el correo electrónico y utilizar la autenticación multifactorial para proteger las cuentas sensibles. |
| 8 | Ataques DDoS (denegación de servicio distribuido) | Alto | Lógica | 6 | Despliegue una solución de protección DDoS robusta, supervise el tráfico de la red en busca de anomalías y cree un plan de respuesta a incidentes para minimizar el tiempo de inactividad en caso de ataque. |
| 9 | Errores humanos | Medio | Física | 4 | Proporcione formación y apoyo continuos al personal, aplique estrictos controles de acceso y políticas de manejo de datos, y utilice herramientas automatizadas para reducir el riesgo de errores humanos. |
| 10 | Amenazas internas | Medio | Física / lógica | 4 | Establezca estrictos controles de acceso de los usuarios, supervise sus actividades e imparta formación periódica sobre seguridad a los empleados. |

Campo Total = Impacto + Vulnerabilidad.

**De manera periódica estos datos deben ser analizados y actualizados.**