
***Empresa : Berkshire
Emingway
Responsable de Seguridad: Daniel Stix***

Descripción de la Organización:

Berkshire Emingway es una compañía orientada al desarrollo, despliegue y administración de entornos web para terceros. Su operativa se basa en la utilización de servicios de hosting de terceros, los cuales son contratados a nombre del cliente final, garantizando así la titularidad directa al servicio.

Dentro de estos entornos, la empresa realiza la implementación de plataformas CMS, así como la instalación y configuración de temas y lleva a cabo procesos de customización funcional y estética conforme a los requerimientos del cliente.

Adicionalmente, Berkshire Emingway proporciona servicios de gestión de contenido y mantenimiento operacional, los cuales están regulados mediante SLA's

Identificación de Activos

Nº	Activo	Descripción
A1	Servidores Web en hosting	Servidores externos donde se aloja el contenido de clientes.
A2	Equipos de diseño	Ordenadores del personal encargado de diseño y actualización.
A3	Conexión a Internet FTTH	Línea de datos que conecta la oficina con el exterior.
A4	Firewall	Dispositivo de seguridad que protege la red interna.
A5	Router del operador	Dispositivo del proveedor de telecomunicaciones.
A6	Servicio de correo en cloud	Medio principal para recepción de contenidos de clientes. (Office 365)
A7	Aplicación de gestión	Portal web usado internamente para gestionar tareas.

Diagrama de Relaciones

El Router del operador (A5) conecta la línea FTTH (A3) con el Firewall (A4), que a su vez protege la LAN. En la LAN están los equipos de diseño (A2) que acceden a la aplicación de gestión (A7). El correo (A6) se accede mediante navegador desde los equipos (A2). El contenido se publica en los servidores web en hosting (A1), actualizados desde los equipos (A2). Todo el sistema depende del suministro eléctrico (A8).

Valoración cualitativa de Disponibilidad

Activo	Valor de Disponibilidad	Justificación
A1	Alto	Si los servidores están inactivos, las webs de clientes no están disponibles.
A2	Alto	Son los que ejecutan el trabajo crítico de actualización.
A3	Alto	Sin conexión a Internet no se pueden hacer actualizaciones.
A4	Medio	Su fallo puede bloquear la red, pero es sustituible.
A5	Medio	Similar al A4, aunque está fuera de control directo.
A6	Bajo	No entra en análisis (por estar garantizado con 99%).
A7	Medio	Es una herramienta de soporte.
A8	Alto	Sin energía nada funciona.

Caracterización de Amenazas

Nº	Amenaza	Descripción	Probabilidad
T1	Corte de suministro eléctrico	Fallo total de energía en la oficina.	Media
T2	Virus en la red	Infección que inhabilita los equipos o bloquea comunicaciones.	Alta
T3	Avería de hardware	Fallos físicos en equipos clave como ordenadores o router.	Media

Cálculo de Riesgo (Cualitativo)

Fórmula usada: Riesgo = Probabilidad × Impacto (Valor de disponibilidad)

Activo	Amenaza	Probabilidad	Impacto	Riesgo
A2	T2	Alta	Alto	Alto
A8	T1	Media	Alto	Alto
A2	T3	Media	Alto	Medio
A1	T2	Alta	Alto	Alto
A1	T3	Media	Alto	Medio
A3	T3	Media	Alto	Medio

Riesgos mayores a mitigar:

- Virus en la red afectando a A2 y A1
- Corte de suministro eléctrico afectando a A8

Propuesta de Salvaguardas

Riesgo	Salvaguarda Propuesta
Virus (T2) en Equipos (A2) y Servidores (A1)	<ul style="list-style-type: none">- Uso de antivirus actualizados- Segmentación de red- Formación al personal sobre ciberseguridad

Corte eléctrico (T1) en Suministro (A8)

- Instalación de SAI (Sistemas de Alimentación Ininterrumpida)
- Contrato con proveedor eléctrico alternativo

Avería hardware (T3) en Equipos (A2)

- Mantenimiento preventivo
- Equipos de backup y pólizas de soporte técnico urgente