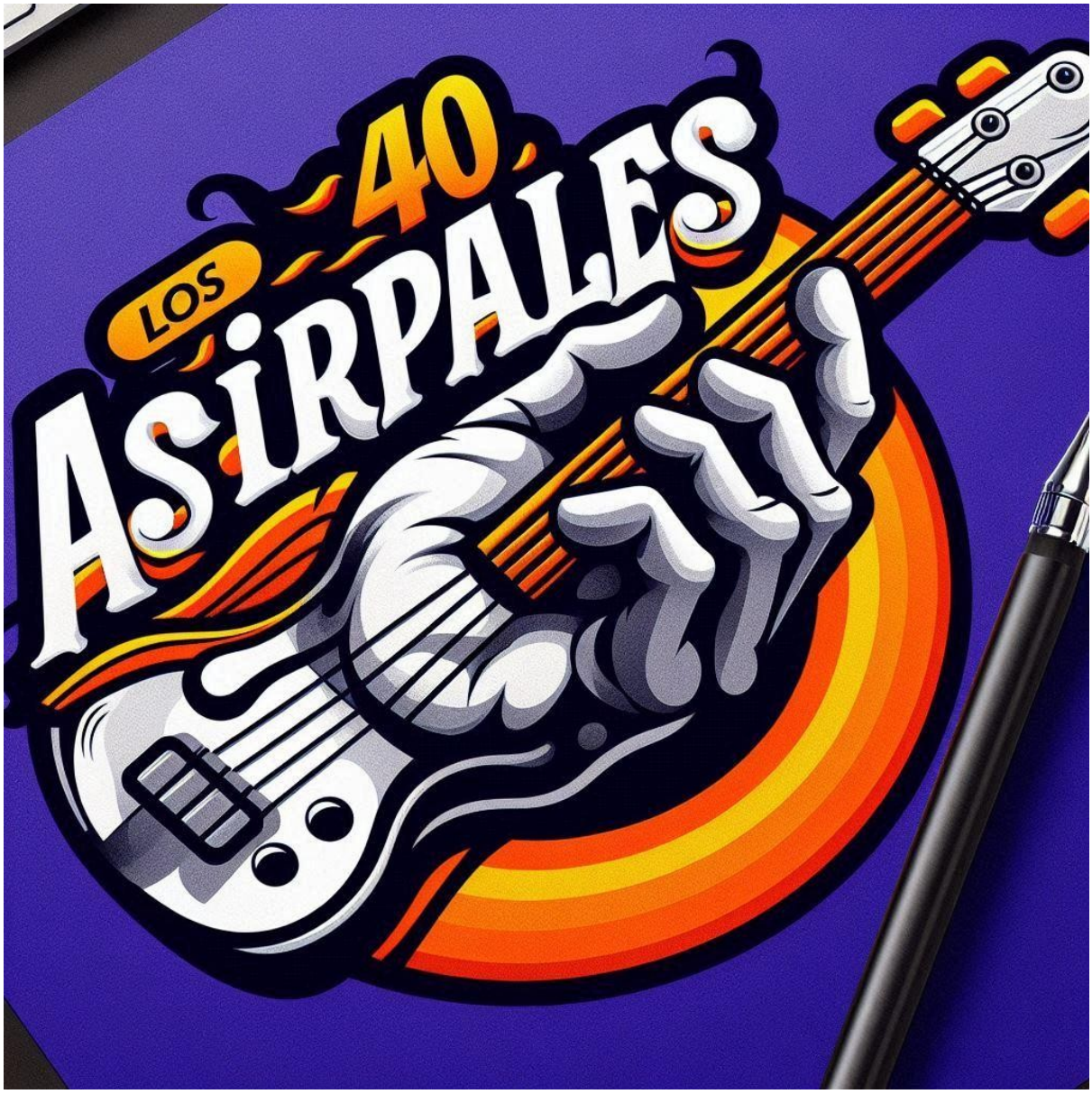
Los 40 Asirpales Plan de Seguridad



1. Identificación de Activos Críticos

Activos Digitales:

1. **Sitio Web en WordPress**
    - Base de datos (contenido, usuarios, configuraciones)
    - Temas y plugins instalados
    - Archivos del núcleo de WordPress
2. **Servidor de Hosting**
    - Sistema operativo y software del servidor
    - Configuración del servidor
    - Acceso SSH/FTP
3. **Datos de Usuarios**
    - Información de clientes y usuarios registrados
    - Datos personales y de contacto
4. **Contenido Multimedia**
    - Archivos de audio (programas, podcasts)
    - Imágenes y vídeos
5. **Correo Electrónico**
    - Cuentas de correo de la empresa
    - Comunicaciones internas y externas

Activos Físicos:

1. **Equipos de Transmisión**
    - Consolas de mezcla
    - Equipos de transmisión de radio
    - Antenas y equipos de broadcast
2. **Computadoras y Dispositivos**
    - Computadoras de trabajo
    - Dispositivos móviles

Activos Humanos:

1. **Personal**
    - Administradores de la página web
    - Técnicos de transmisión
    - Personal de soporte y atención al cliente

2. Evaluación de Riesgos

Riesgos para Activos Digitales:

1. **Ciberataques** (malware, ransomware, DDoS)

2. **Vulnerabilidades del Software** (plugins desactualizados, temas no seguros)
3. **Pérdida de Datos** (errores humanos, fallos en el servidor)

Riesgos para Activos Físicos:

1. **Robo de Equipos**
2. **Desastres Naturales** (incendios, inundaciones)
3. **Fallos de Hardware**

Riesgos para Activos Humanos:

1. **Errores Humanos** (configuraciones incorrectas, manejo inapropiado de datos)
2. **Amenazas Internas** (personal descontento, espionaje industrial)

3. Estrategias de Mitigación

Para Activos Digitales:

1. **Seguridad del Sitio Web:**
    - **Actualización Regular** de WordPress, temas y plugins.
    - **Uso de Plugins de Seguridad** (Wordfence, Sucuri).
    - **Copias de Seguridad** diarias de la base de datos y archivos.

2. **Protección del Servidor:**
    - **Firewalls** y sistemas de detección de intrusos (IDS).
    - **Acceso Restringido** (uso de claves SSH, autenticación de dos factores).
3. **Gestión de Datos de Usuarios:**
    - **Encriptación de Datos** sensibles.
    - **Política de Privacidad** clara y transparente.

Para Activos Físicos:

1. **Seguridad Física:**
    - **Cámaras de Vigilancia** y sistemas de alarma.
    - **Control de Acceso** a las áreas críticas.
2. **Plan de Continuidad del Negocio:**
    - **Equipos de Respaldo** para transmisión.
    - **Procedimientos de Recuperación** ante desastres.

Para Activos Humanos:

1. **Capacitación:**
    - **Formación Continua** en buenas prácticas de seguridad.
    - **Simulacros** y **Talleres** sobre ciberseguridad.
2. **Políticas de Seguridad:**
    - **Reglamentos Internos** claros sobre el manejo de información y equipos.
    - **Monitoreo y Auditorías** periódicas.

4. Implementación y Monitoreo

Implementación:

1. **Asignación de Responsabilidades:** Definir roles y responsabilidades específicas para cada área.
2. **Desarrollo de Procedimientos:** Documentar todos los procedimientos de seguridad.

Monitoreo:

1. **Sistemas de Monitoreo:** Implementar herramientas para monitorear en tiempo real la seguridad del sitio web y los sistemas.

2. **Revisiones y Auditorías:** Realizar auditorías periódicas para identificar y corregir vulnerabilidades.

5. Respuesta a Incidentes

1. **Plan de Respuesta:** Desarrollar un plan detallado de respuesta a incidentes.
2. **Equipo de Respuesta:** Establecer un equipo especializado para gestionar incidentes de seguridad.
3. **Comunicación:** Establecer protocolos claros de comunicación interna y externa en caso de un incidente.

6. Evaluación y Mejora Continua

1. **Revisiones Periódicas:** Evaluar regularmente la efectividad del plan de seguridad y realizar ajustes necesarios.
2. **Actualización de Políticas:** Mantener las políticas y procedimientos actualizados conforme a las nuevas amenazas y tecnologías.

Amenazas Relevantes y Potenciales

1. Amenazas Digitales

1. **Ciberataques:**
    - **Malware y Ransomware:** Programas maliciosos que pueden cifrar datos y exigir un rescate.
    - **Phishing:** Intentos de engañar a los usuarios para que revelen información sensible.
    - **DDoS (Denegación de Servicio Distribuido):** Ataques que buscan saturar el servidor para dejar el sitio web fuera de línea.
    - **SQL Injection:** Inyección de código malicioso en formularios web para acceder a la base de datos.
2. **Vulnerabilidades del Software:**
    - **Plugins y Temas Desactualizados:** Pueden tener vulnerabilidades que los atacantes pueden explotar.

    - **Errores en el Código:** Bugs y errores en el núcleo de WordPress o en personalizaciones.
3. **Acceso No Autorizado:**
    - **Fuerza Bruta:** Intentos de adivinar contraseñas mediante prueba y error.
    - **Explotación de Credenciales Robadas:** Uso de credenciales obtenidas de filtraciones en otros sitios.
4. **Pérdida de Datos:**
    - **Errores Humanos:** Borrado accidental o modificación incorrecta de datos.
    - **Fallos en el Servidor:** Problemas de hardware o software que resulten en pérdida de datos.
5. **Intercepción de Comunicaciones:**
    - **Ataques Man-in-the-Middle (MitM):** Interceptación de datos durante la transmisión entre usuarios y el servidor.
    - **Fugas de Información:** A través de conexiones no seguras o dispositivos comprometidos.

2. Amenazas Físicas

1. **Desastres Naturales:**
    - **Incendios:** Daños a equipos y datos.
    - **Inundaciones:** Afectación de equipos y pérdida de datos.
    - **Terremotos:** Daños estructurales y pérdida de equipos.
2. **Robo y Vandalismo:**
    - **Robo de Equipos:** Sustitución de equipos esenciales para la transmisión y operaciones.
    - **Sabotaje:** Daño intencionado a equipos o infraestructura.
3. **Fallos de Hardware:**
    - **Desgaste y Averías:** Fallos en discos duros, fuentes de alimentación, etc.
    - **Cortes de Energía:** Pérdida de datos y daño a equipos por interrupciones eléctricas.

3. Amenazas Humanas

1. **Errores Humanos:**
    - **Configuraciones Incorrectas:** Mala configuración de sistemas y redes.
    - **Manejo Inapropiado de Datos:** Exposición accidental de información sensible.
2. **Amenazas Internas:**
    - **Personal Descontento:** Empleados que pueden sabotear o filtrar información.
    - **Espionaje Industrial:** Competencia que infiltra a empleados para obtener información confidencial.
3. **Ingeniería Social:**
    - **Suplantación de Identidad:** Personas que se hacen pasar por empleados o socios para obtener acceso a información.
    - **Manipulación Psicológica:** Técnicas para engañar a los empleados y que revelen información sensible.

4. Amenazas a la Continuidad del Negocio

1. **Interrupciones en el Servicio:**
    - **Fallas en el Proveedor de Servicios de Internet (ISP):** Pérdida de conectividad.
    - **Problemas con el Proveedor de Hosting:** Caídas del servidor o problemas de rendimiento.

2. **Legislación y Cumplimiento:**
    - **Cambios Regulatorios:** Nuevas leyes o regulaciones que requieren cambios en las operaciones.
    - **Multas y Sanciones:** Por incumplimiento de normativas de protección de datos y privacidad.

Estrategias de Mitigación para las Amenazas Identificadas

1. Mitigación de Ciberataques

- **Implementar Firewalls y Sistemas de Detección de Intrusos (IDS):** Para prevenir y detectar intentos de ataque.
- **Actualización Regular de Software:** Mantener WordPress, plugins y temas actualizados.
- **Copias de Seguridad Frecuentes:** Realizar copias de seguridad automáticas y periódicas.

2. Mitigación de Amenazas Físicas

- **Medidas de Seguridad Física:** Implementar controles de acceso, cámaras de vigilancia y sistemas de alarma.
- **Planes de Recuperación ante Desastres:** Desarrollar y probar regularmente planes de continuidad del negocio.

3. Mitigación de Amenazas Humanas

- **Capacitación y Concienciación:** Entrenar al personal en buenas prácticas de seguridad y en el reconocimiento de amenazas.
- **Políticas de Seguridad:** Implementar y hacer cumplir políticas claras sobre el manejo de datos y acceso a sistemas.

4. Mitigación de Amenazas a la Continuidad del Negocio

- **Redundancia y Failover:** Implementar soluciones de redundancia para sistemas críticos y planes de failover.
- **Monitoreo y Auditorías:** Monitorear continuamente los sistemas y realizar auditorías de seguridad.

1. Vulnerabilidades en Activos Digitales

Sitio Web en WordPress

1. **Núcleo de WordPress:**
    - **Versiones Desactualizadas:** Utilizar una versión antigua del núcleo de WordPress que contiene vulnerabilidades conocidas.
    - **Configuraciones Inseguras:** Configuraciones predeterminadas o incorrectas que pueden ser explotadas.
2. **Temas y Plugins:**
    - **Plugins y Temas Desactualizados:** Uso de plugins y temas sin actualizaciones que contienen fallos de seguridad.
    - **Plugins y Temas No Confiables:** Instalación de plugins o temas de fuentes no verificadas que pueden incluir código malicioso.
    - **Falta de Validación de Datos:** Plugins que no validan adecuadamente la entrada de datos, susceptibles a ataques de inyección.
3. **Base de Datos:**
    - **Inyección SQL (SQLi):** Falta de sanitización de las entradas del usuario, permitiendo la ejecución de comandos SQL maliciosos.
    - **Acceso No Protegido:** Bases de datos accesibles sin restricciones adecuadas de acceso.
4. **Autenticación y Autorización:**
    - **Contraseñas débiles:** Uso de contraseñas fáciles de adivinar o predecibles.
    - **Autenticación de Dos Factores (2FA) Ausente:** No implementar 2FA para usuarios administrativos.
    - **Sesiones Inseguras:** Sesiones sin protección adecuada, susceptibles a secuestro de sesión.

Servidor de Hosting

1. **Configuraciones del Servidor:**
    - **Software desactualizado:** Uso de versiones obsoletas de software del servidor (Apache, Nginx, PHP, etc.).
    - **Permisos Inapropiados:** Configuración incorrecta de permisos de archivos y directorios.

2. **Seguridad de la Red:**
    - **Puertos Abiertos Innecesarios:** Exposición de servicios no necesarios a Internet.
    - **Falta de Firewalls:** Ausencia de firewalls que protegen el servidor contra ataques externos.

Datos de Usuarios

1. **Protección de Datos:**
    - **Datos No Encriptados:** Transmisión o almacenamiento de datos sensibles sin cifrado.
    - **Fugas de Información:** Exposición accidental o intencional de datos personales.

Contenido Multimedia

1. **Archivos de Medios:**
    - **Archivos No Verificados:** Subida de archivos sin escaneo de seguridad, permitiendo la carga de contenido malicioso.
    - **Acceso Público No Controlado:** Archivos accesibles públicamente sin restricciones necesarias.

Correo Electrónico

1. **Cuentas de Correo:**
    - **Phishing:** Vulnerabilidad a ataques de phishing debido a falta de concienciación y medidas de protección.
    - **Falta de Cifrado:** Correos electrónicos enviados sin cifrado, susceptibles a intercepción.

2. Vulnerabilidades en Activos Físicos

Equipos de Transmisión y Dispositivos

1. **Seguridad Física:**
    - **Acceso Físico No Restringido:** Falta de control sobre el acceso a equipos críticos.
    - **Equipos Sin Protección:** Equipos no asegurados físicamente contra robos o vandalismo.
2. **Fallos de Hardware:**
    - **Mantenimiento Insuficiente:** Falta de mantenimiento regular de equipos críticos.
    - **Dependencia de Hardware Único:** Sin planes de redundancia para equipos esenciales.

3. Vulnerabilidades en Activos Humanos

Personal

1. **Capacitación Insuficiente:**
    - **Desconocimiento de Buenas Prácticas:** Personal no capacitado en seguridad informática y procedimientos adecuados.
    - **Falta de Protocolos de Seguridad:** Ausencia de protocolos claros y aplicados de manejo de información y equipos.
2. **Amenazas Internas:**

- **Acceso No Restringido:** Acceso no controlado o inadecuadamente restringido a información y sistemas críticos.
- **Ausencia de Políticas de Auditoría:** Falta de monitoreo y auditoría de actividades del personal.

4. Vulnerabilidades a la Continuidad del Negocio

Infraestructura y Planificación

1. **Planes de Recuperación Inadecuados:**
   - **Falta de Planes de Respaldo:** Ausencia de planes de recuperación ante desastres o fallos.
   - **Pruebas de Recuperación Insuficientes:** Falta de pruebas regulares de los planes de recuperación y respaldo.
2. **Dependencia de Proveedores Externos:**
   - **Riesgos del Proveedor de Hosting:** Dependencia excesiva de un solo proveedor sin planes de contingencia.

Estrategias de Mitigación para las Vulnerabilidades Identificadas

1. **Para el Sitio Web en WordPress:**
    - **Mantener Todo Actualizado:** Actualizar regularmente WordPress, temas y plugins.
    - **Realizar Auditorías de Seguridad:** Auditorías periódicas para identificar y corregir vulnerabilidades.
    - **Implementar 2FA:** Utilizar autenticación de dos factores para accesos administrativos.
2. **Para el Servidor de Hosting:**
    - **Configurar Firewalls:** Implementar firewalls y revisar configuraciones de puertos abiertos.
    - **Permisos Seguros:** Asegurar la correcta configuración de permisos en archivos y directorios.
3. **Para la Protección de Datos de Usuarios:**
    - **Encriptar Datos Sensibles:** Implementar cifrado para la transmisión y almacenamiento de datos.
    - **Controlar Acceso a Datos:** Restringir y monitorear el acceso a datos personales y sensibles.
4. **Para el Correo Electrónico:**
    - **Usar Cifrado de Correos:** Implementar cifrado para correos electrónicos sensibles.
    - **Concienciación sobre Phishing:** Capacitar al personal para reconocer y evitar ataques de phishing.
5. **Para Equipos Físicos:**
    - **Seguridad Física:** Implementar controles de acceso y medidas de seguridad física para equipos críticos.
    - **Planes de Redundancia:** Establecer planes de redundancia y mantenimiento regular para equipos esenciales.
6. **Para el Personal:**
    - **Capacitación Continua:** Proveer capacitación regular en buenas prácticas de seguridad.
    - **Monitoreo y Auditoría:** Implementar políticas de monitoreo y auditoría de actividades del personal.
7. **Para la Continuidad del Negocio:**
    - **Desarrollar Planes de Recuperación:** Crear y probar regularmente planes de recuperación ante desastres.
    - **Evaluar Proveedores:** Realizar evaluaciones periódicas de los proveedores y establecer planes de contingencia.

Matriz de Análisis de Riesgos

1. Riesgos Digitales

1. **Ciberataques:**
    - **Malware y Ransomware:**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** Puede causar cifrado de datos críticos, interrumpiendo las operaciones y potencialmente causando pérdida de datos sensibles.
    - **Phishing:**
        - **Probabilidad:** Alta
        - **Impacto:** Medio
        - **Descripción:** Puede conducir a la divulgación de credenciales y otros datos sensibles, facilitando otros ataques.
    - **DDoS (Denegación de Servicio Distribuido):**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** Puede hacer que el sitio web esté inaccesible, afectando la disponibilidad del servicio.
    - **SQL Injection:**
        - **Probabilidad:** Baja
        - **Impacto:** Alto
        - **Descripción:** Puede permitir a los atacantes acceder y manipular la base de datos, causando pérdida o corrupción de datos.
2. **Vulnerabilidades del Software:**
    - **Plugins y Temas Desactualizados:**
        - **Probabilidad:** Alta
        - **Impacto:** Alto
        - **Descripción:** Las versiones desactualizadas son un objetivo común para los atacantes, y pueden permitir la ejecución de código malicioso.
    - **Errores en el Código:**
        - **Probabilidad:** Media
        - **Impacto:** Medio
        - **Descripción:** Bugs y errores pueden ser explotados para comprometer la seguridad del sitio web.
3. **Acceso No Autorizado:**
    - **Fuerza Bruta:**
        - **Probabilidad:** Alta
        - **Impacto:** Medio
        - **Descripción:** Los intentos de adivinación de contraseñas pueden llevar a la toma de control de cuentas administrativas.
    - **Explotación de Credenciales Robadas:**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** El uso de credenciales obtenidas de filtraciones puede permitir acceso no autorizado a sistemas críticos.
4. **Pérdida de Datos:**
    - **Errores Humanos:**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** Borrado accidental o modificación incorrecta de datos puede resultar en pérdida de información valiosa.
    - **Fallos en el Servidor:**
        - **Probabilidad:** Baja

        - **Impacto:** Alto
        - **Descripción:** Problemas de hardware o software pueden causar pérdida de datos y tiempo de inactividad.
5. **Intercepción de Comunicaciones:**
    - **Ataques Man-in-the-Middle (MitM):**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** La interceptación de datos puede llevar a la exposición de información sensible.
    - **Fugas de Información:**
        - **Probabilidad:** Media
        - **Impacto:** Medio
        - **Descripción:** A través de conexiones no seguras o dispositivos comprometidos, los datos pueden ser expuestos.

2. Riesgos Físicos

1. **Desastres Naturales:**
    - **Incendios:**
        - **Probabilidad:** Baja
        - **Impacto:** Alto
        - **Descripción:** Daños a equipos y datos pueden ser catastróficos para las operaciones.
    - **Inundaciones:**
        - **Probabilidad:** Baja
        - **Impacto:** Alto
        - **Descripción:** Puede afectar equipos y causar pérdida de datos.
2. **Robo y Vandalismo:**
    - **Robo de Equipos:**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** La pérdida de equipos puede interrumpir las operaciones y requerir reemplazo costoso.
    - **Sabotaje:**
        - **Probabilidad:** Baja
        - **Impacto:** Alto
        - **Descripción:** Daño intencionado a equipos o infraestructura puede tener consecuencias graves.
3. **Fallos de Hardware:**
    - **Desgaste y Averías:**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** Fallos en discos duros y otros componentes críticos pueden causar interrupciones y pérdida de datos.
    - **Cortes de Energía:**
        - **Probabilidad:** Media
        - **Impacto:** Medio
        - **Descripción:** Pérdida de datos y daño a equipos debido a interrupciones eléctricas.

3. Riesgos Humanos

1. **Errores Humanos:**
    - **Configuraciones Incorrectas:**
        - **Probabilidad:** Alta

        - **Impacto:** Medio
        - **Descripción:** Mala configuración de sistemas y redes puede abrir puertas a ataques y fallos.
    - **Manejo Inapropiado de Datos:**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** Exposición accidental de información sensible puede tener consecuencias legales y de reputación.
2. **Amenazas Internas:**
    - **Personal Descontento:**
        - **Probabilidad:** Baja
        - **Impacto:** Alto
        - **Descripción:** Empleados descontentos pueden sabotear o filtrar información crítica.
    - **Espionaje Industrial:**
        - **Probabilidad:** Baja
        - **Impacto:** Alto
        - **Descripción:** Competencia infiltrando empleados para obtener información confidencial.
3. **Ingeniería Social:**
    - **Suplantación de Identidad:**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** Personas haciéndose pasar por empleados pueden obtener acceso a información y sistemas sensibles.
    - **Manipulación Psicológica:**
        - **Probabilidad:** Media
        - **Impacto:** Medio
        - **Descripción:** Técnicas para engañar a los empleados y que revelen información sensible.

4. Riesgos a la Continuidad del Negocio

1. **Interrupciones en el Servicio:**
    - **Fallas en el Proveedor de Servicios de Internet (ISP):**
        - **Probabilidad:** Media
        - **Impacto:** Medio
        - **Descripción:** Pérdida de conectividad puede interrumpir operaciones en línea.
    - **Problemas con el Proveedor de Hosting:**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** Caídas del servidor o problemas de rendimiento pueden afectar la disponibilidad del sitio web.
2. **Legislación y Cumplimiento:**
    - **Cambios Regulatorios:**
        - **Probabilidad:** Baja
        - **Impacto:** Medio
        - **Descripción:** Nuevas leyes o regulaciones pueden requerir cambios en las operaciones y políticas.
    - **Multas y Sanciones:**
        - **Probabilidad:** Media
        - **Impacto:** Alto
        - **Descripción:** Incumplimiento de normativas de protección de datos y privacidad puede resultar en sanciones financieras y de reputación.

Matriz de riesgos

Riesgo	Probabilidad	Impacto	Nivel de Riesgo
Malware y Ransomware	Media	Alto	Alto
Phishing	Alta	Medio	Alto
DDoS	Media	Alto	Alto
SQL Injection	Baja	Alto	Medio
Plugins y Temas Desactualizados	Alta	Alto	Alto
Errores en el Código	Media	Medio	Medio
Fuerza Bruta	Alta	Medio	Alto
Explotación de Credenciales Robadas	Media	Alto	Alto
Errores Humanos (Pérdida de Datos)	Media	Alto	Alto
Fallos en el Servidor	Baja	Alto	Medio
Ataques Man-in-the-Middle (MitM)	Media	Alto	Alto
Fugas de Información	Media	Medio	Medio
Incendios	Baja	Alto	Medio
Inundaciones	Baja	Alto	Medio
Robo de Equipos	Media	Alto	Alto
Sabotaje	Baja	Alto	Medio
Desgaste y Averías	Media	Alto	Alto
Cortes de Energía	Media	Medio	Medio
Configuraciones Incorrectas	Alta	Medio	Alto

Estrategias de Mitigación de Riesgos

1. Para Ciberataques:
    - Implementar Firewalls y Sistemas de Detección de Intrusos (IDS).
    - Mantener software y plugins actualizados.
    - Realizar copias de seguridad regulares y usar cifrado de datos.
    - Implementar autenticación de dos factores (2FA).
2. Para Vulnerabilidades del Software:
    - Auditorías de seguridad regulares.
    - Escaneo y análisis de código para detectar y corregir errores.
3. Para Acceso No Autorizado:
    - Políticas de contraseñas seguras y 2FA.
    - Monitoreo continuo de accesos y actividades sospechosas.
4. Para Pérdida de Datos:
    - Capacitación del personal en manejo de datos.
    - Sistemas de respaldo y recuperación robustos.
5. Para Intercepción de Comunicaciones:
    - Implementar HTTPS y cifrado de datos en tránsito.
    - Monitorear y proteger conexiones de red.
6. Para Desastres Naturales y Robo:
    - Controles de acceso físico y medidas de seguridad en instalaciones.
    - Planes de recuperación ante desastres.
7. Para Fallos de Hardware:
    - Mantenimiento regular y uso de sistemas redundantes.
    - Implementación de soluciones de energía ininterrumpida (UPS).
8. Para Errores Humanos y Amenazas Internas:
    - Capacitación continua en seguridad y manejo de información.
    - Políticas de monitoreo y auditoría.
9. Para Continuidad del Negocio:
    - Planes de contingencia y recuperación probados regularmente.
    - Evaluaciones periódicas de proveedores y soluciones de respaldo.

1. Introducción

1.1 Objetivo del Plan

El objetivo de este plan es proporcionar un conjunto de procedimientos y directrices para responder eficazmente a los incidentes de seguridad que puedan afectar a los activos críticos de la empresa, asegurando la mínima interrupción de las operaciones y protegiendo la información sensible.

1.2 Alcance

Este plan se aplica a todos los empleados, contratistas y terceros que tienen acceso a los sistemas y datos de la empresa. Cubre incidentes de seguridad cibernética, física y de continuidad del negocio.

2. Estructura del Equipo de Respuesta a Incidentes (ERI)

2.1 Composición del ERI

- **Líder del ERI:** Responsable de la coordinación general del plan de respuesta.
- **Especialista en Seguridad Informática:** Encargado de la identificación y mitigación de amenazas digitales.

- **Administrador de Sistemas:** Responsable de la recuperación y restauración de sistemas afectados.
- **Representante Legal:** Asegura el cumplimiento con las regulaciones y maneja las implicaciones legales.
- **Especialista en Comunicación:** Maneja la comunicación interna y externa durante el incidente.

2.2 Responsabilidades del ERI

- **Detección y Análisis:** Identificar y evaluar la naturaleza del incidente.
- **Contención:** Limitar el alcance y el impacto del incidente.
- **Erradicación:** Eliminar la causa raíz del incidente.
- **Recuperación:** Restaurar los sistemas y datos a su estado normal.
- **Análisis Posterior al Incidente:** Evaluar la respuesta y mejorar las estrategias.

3. Procedimientos de Respuesta a Incidentes

3.1 Detección y Análisis

1. **Monitoreo Continuo:**
    - Implementar herramientas de monitoreo para detectar actividades inusuales o sospechosas.
    - Revisar alertas y logs regularmente para identificar posibles incidentes.
2. **Evaluación Inicial:**
    - Determinar el tipo de incidente (ciberataque, falla de hardware, desastre natural, etc.).
    - Evaluar la magnitud y el impacto potencial del incidente.
    - Notificar al Líder del ERI y activar el equipo de respuesta.
3. **Documentación:**
    - Registrar toda la información relevante sobre el incidente (tiempo, naturaleza, sistemas afectados, etc.).
    - Mantener un registro detallado de todas las acciones tomadas durante la respuesta.

3.2 Contención

1. **Contención a Corto Plazo:**
    - Aislar los sistemas afectados para evitar la propagación del incidente.
    - Implementar soluciones temporales para limitar el impacto.
2. **Contención a Largo Plazo:**
    - Desarrollar e implementar medidas más sostenibles para contener el incidente.
    - Continuar monitoreando los sistemas para detectar cualquier actividad residual.

3.3 Erradicación

1. **Identificación de la Causa Raíz:**
    - Realizar un análisis exhaustivo para identificar la causa raíz del incidente.
    - Evaluar si el incidente es el resultado de una vulnerabilidad específica o una amenaza persistente.
2. **Eliminación de la Amenaza:**
    - Aplicar parches y actualizaciones necesarios para eliminar vulnerabilidades.
    - Remover cualquier malware, archivos dañinos o accesos no autorizados.

3.4 Recuperación

1. **Restauración de Sistemas:**
    - Restaurar los sistemas y servicios afectados a partir de las copias de seguridad.
    - Verificar la integridad y funcionalidad de los sistemas restaurados.
2. **Revisión de Seguridad:**
    - Implementar medidas de seguridad adicionales para evitar recurrencias.
    - Realizar una revisión completa de los sistemas para asegurar que estén completamente libres de amenazas.

3.5 Análisis Posterior al Incidente

1. **Revisión del Incidente:**
    - Reunir al equipo de respuesta para discutir el incidente y la respuesta.
    - Evaluar la eficacia de las estrategias de mitigación y respuesta.
2. **Lecciones Aprendidas:**
    - Identificar áreas de mejora en las políticas y procedimientos de seguridad.
    - Actualizar el plan de respuesta a incidentes con base en las lecciones aprendidas.
3. **Informe del Incidente:**
    - Elaborar un informe detallado del incidente que incluya:
        - Descripción del incidente.
        - Cronología de los eventos.
        - Acciones tomadas.
        - Impacto en el negocio.
        - Recomendaciones para el futuro.

4. Comunicación

4.1 Comunicación Interna

- **Notificación Temprana:** Informar a los empleados relevantes sobre el incidente y las medidas a tomar.
- **Actualizaciones Regulares:** Proveer actualizaciones regulares sobre el progreso de la respuesta al incidente.
- **Política de Transparencia:** Mantener una política de transparencia y comunicación clara con todos los miembros de la organización.

4.2 Comunicación Externa

- **Notificación a Clientes:** Informar a los clientes afectados sobre el incidente y las medidas de mitigación implementadas.
- **Relaciones Públicas:** Coordinar con el especialista en comunicación para manejar la comunicación con los medios y el público.
- **Reportes Regulatorios:** Cumplir con los requisitos de notificación a las autoridades regulatorias y organismos pertinentes.

5. Recursos y Herramientas

5.1 Herramientas de Seguridad

- **Sistemas de Detección de Intrusos (IDS):** Para detectar accesos no autorizados.
- **Antivirus y Antimalware:** Para proteger contra software malicioso.
- **Firewalls:** Para controlar el tráfico de red y bloquear accesos no autorizados.

5.2 Herramientas de Monitoreo

- **Sistemas de Monitoreo de Red:** Para supervisar el tráfico y detectar anomalías.
- **Sistemas de Gestión de Eventos e Información de Seguridad:** Para recopilar y analizar datos de seguridad.

5.3 Recursos Humanos

- **Equipo de Seguridad Informática:** Personal especializado en ciberseguridad.
- **Equipo de TI:** Administradores de sistemas y redes.
- **Asesoría Legal:** Abogados especializados en derecho tecnológico y cumplimiento normativo.

6. Entrenamiento y Pruebas

6.1 Entrenamiento Regular

- **Capacitación del Personal:** Entrenar a todos los empleados en la identificación y respuesta a incidentes de seguridad.
- **Simulacros de Incidentes:** Realizar simulacros regulares para probar la eficacia del plan de respuesta.

6.2 Revisión y Actualización

- **Revisión Anual:** Revisar y actualizar el plan de respuesta a incidentes al menos una vez al año.
- **Actualización Post-Incidente:** Actualizar el plan basado en las lecciones aprendidas de incidentes pasados.

1. Establecimiento del Equipo de Implementación

1.1 Asignación de Responsabilidades

- **Líder del Proyecto (Responsable: Director de TI)**
  - Coordinar todas las actividades de implementación.
  - Asegurar la disponibilidad de recursos necesarios.
  - Informar al equipo ejecutivo sobre el progreso y cualquier problema.
- **Especialista en Seguridad Informática (Responsable: Jefe de Seguridad)**
  - Implementar medidas de seguridad cibernética.
  - Configurar herramientas de detección y respuesta a incidentes.
  - Capacitar al personal en buenas prácticas de seguridad.
- **Administrador de Sistemas (Responsable: Jefe de Operaciones de TI)**
  - Configurar y mantener los sistemas de respaldo y recuperación.
  - Implementar actualizaciones de software y parches de seguridad.
  - Monitorear el rendimiento y la integridad de los sistemas.
- **Representante Legal (Responsable: Asesor Legal)**
  - Asegurar el cumplimiento con las leyes y regulaciones relevantes.
  - Manejar cualquier implicación legal derivada de incidentes de seguridad.
- **Especialista en Comunicación (Responsable: Director de Comunicaciones)**
  - Manejar la comunicación interna y externa durante incidentes.
  - Mantener a los clientes informados sobre medidas de seguridad y actualizaciones.

2. Plan de Implementación Detallado

2.1 Evaluación Inicial y Priorización

- **Inventario de Activos (Responsable: Administrador de Sistemas)**
  - **Plazo: 1 semana**
  - Realizar un inventario detallado de todos los activos críticos.
  - Clasificar los activos según su importancia y vulnerabilidad.
- **Evaluación de Amenazas y Vulnerabilidades (Responsable: Especialista en Seguridad Informática)**
  - **Plazo: 2 semanas**
  - Identificar amenazas y vulnerabilidades relevantes.
  - Realizar un análisis de riesgos para priorizar acciones.

2.2 Implementación de Medidas de Seguridad

- **Ciberseguridad**
  - **Implementación de Firewalls y IDS (Responsable: Especialista en Seguridad Informática)**
    - **Plazo: 2 semanas**
    - Configurar y desplegar firewalls y sistemas de detección de intrusos.
  - **Actualización de Software y Plugins (Responsable: Administrador de Sistemas)**
    - **Plazo: 1 semana**
    - Asegurar que todos los sistemas, plugins y temas de WordPress estén actualizados.
  - **Autenticación de Dos Factores (2FA) (Responsable: Administrador de Sistemas)**
    - **Plazo: 1 semana**
    - Implementar 2FA para todos los accesos administrativos.
  - **Copias de Seguridad Automáticas (Responsable: Administrador de Sistemas)**
    - **Plazo: 1 semana**
    - Configurar sistemas automáticos de copias de seguridad.
- **Seguridad Física**
  - **Instalación de Sistemas de Seguridad Física (Responsable: Jefe de Seguridad Física)**
    - **Plazo: 2 semanas**
    - Implementar controles de acceso, cámaras de seguridad y sistemas de alarma.
  - **Planes de Recuperación ante Desastres (Responsable: Administrador de Sistemas)**
    - **Plazo: 2 semanas**
    - Desarrollar y probar planes de recuperación ante desastres naturales y fallas de hardware.
- **Capacitación y Concienciación**
  - **Capacitación en Seguridad (Responsable: Especialista en Seguridad Informática)**
    - **Plazo: 1 mes**
    - Desarrollar e implementar programas de capacitación en seguridad para todo el personal.
  - **Simulaciones de Incidentes (Responsable: Líder del Proyecto)**
    - **Plazo: 1 semana**
    - Realizar simulaciones periódicas de incidentes de seguridad.

2.3 Monitoreo y Mantenimiento Continuo

- **Monitoreo de Seguridad (Responsable: Especialista en Seguridad Informática)**
  - **Ongoing**
  - Implementar herramientas de monitoreo continuo para detectar actividades sospechosas.
- **Auditorías de Seguridad (Responsable: Auditor de Seguridad)**
  - **Plazo: Trimestral**
  - Realizar auditorías regulares para evaluar la eficacia de las medidas de seguridad implementadas.
- **Revisión y Actualización del Plan (Responsable: Líder del Proyecto)**
  - **Plazo: Anual o Post-Incidente**
  - Revisar y actualizar el plan de respuesta a incidentes y las políticas de seguridad según sea necesario.

3. Recursos Necesarios

3.1 Humanos

- **Equipo de TI y Seguridad Informática**
  - Especialistas en ciberseguridad y administradores de sistemas.
- **Consultores Externos**
  - Asesores en seguridad y cumplimiento regulatorio.
- **Personal de Apoyo**
  - Personal de comunicaciones y apoyo administrativo.

3.2 Tecnológicos

- **Hardware de Seguridad**
  - Firewalls, sistemas de detección de intrusos y dispositivos de copia de seguridad.
- **Software de Seguridad**
  - Antivirus, antimalware, sistemas de gestión de eventos e información de seguridad (SIEM).
- **Herramientas de Monitoreo**
  - Herramientas de monitoreo de red y sistemas.

3.3 Financieros

- **Presupuesto para Implementación**
  - Asignación de presupuesto para la compra de hardware, software y contratación de personal adicional.
- **Fondo de Contingencia**
  - Reserva financiera para incidentes imprevistos y recuperación ante desastres.

4. Cronograma de Implementación

Actividad	Responsable	Plazo
Inventario de Activos	Administrador de Sistemas	1 semana
Evaluación de Amenazas y Vulnerabilidades	Especialista en Seguridad	2 semanas
Implementación de Firewalls e IDS	Especialista en Seguridad	2 semanas
Actualización de Software y Plugins	Administrador de Sistemas	1 semana
Implementación de 2FA	Administrador de Sistemas	1 semana
Copias de Seguridad Automáticas	Administrador de Sistemas	1 semana
Instalación de Sistemas de Seguridad Física	Jefe de Seguridad Física	2 semanas
Planes de Recuperación ante Desastres	Administrador de Sistemas	2 semanas
Capacitación en Seguridad	Especialista en Seguridad	1 mes
Simulaciones de Incidentes	Líder del Proyecto	1 semana
Monitoreo de Seguridad Continuo	Especialista en Seguridad	Ongoing
Auditorías de Seguridad	Auditor de Seguridad	Trimestral
Revisión y Actualización del Plan	Líder del Proyecto	Anual/Post-Incidente

Monitoreo

1. Introducción

1.1 Objetivo del Proceso de Monitoreo y Revisión

El objetivo de este proceso es establecer un marco sistemático para la supervisión continua y la revisión periódica de las medidas de seguridad implementadas, garantizando que permanezcan efectivas y actualizadas frente a nuevas amenazas y vulnerabilidades.

1.2 Alcance

Este proceso se aplica a todos los sistemas, aplicaciones, y datos críticos de la empresa, así como a las prácticas y políticas de seguridad de la información.

2. Componentes del Proceso de Monitoreo y Revisión

2.1 Monitoreo Continuo

1. **Herramientas de Monitoreo**
    - **Sistemas de Gestión de Eventos e Información de Seguridad (SIEM):** Para recopilar, correlacionar y analizar datos de seguridad en tiempo real.
    - **Antivirus y Antimalware:** Para la detección y eliminación de software malicioso.
    - **Sistemas de Detección de Intrusos (IDS):** Para identificar accesos no autorizados.
    - **Monitoreo de Red:** Para supervisar el tráfico de red y detectar actividades sospechosas.
2. **Actividades de Monitoreo**
    - **Supervisión de Logs:** Revisión regular de logs de sistema y aplicaciones para detectar anomalías.
    - **Análisis de Tráfico de Red:** Monitoreo del tráfico de red para identificar patrones inusuales.
    - **Escaneos de Vulnerabilidades:** Realización periódica de escaneos de vulnerabilidades en todos los sistemas y aplicaciones.
3. **Alertas y Notificaciones**
    - **Configuración de Alertas:** Establecer alertas para eventos críticos (por ejemplo, intentos de acceso no autorizados, detección de malware).
    - **Notificaciones en Tiempo Real:** Asegurar que las notificaciones se envíen inmediatamente al equipo de seguridad cuando se detectan incidentes.

2.2 Revisión Periódica

1. **Frecuencia de Revisiones**
    - **Revisión Mensual:** Evaluación mensual de los logs de seguridad y los informes de monitoreo.
    - **Revisión Trimestral:** Auditoría trimestral de seguridad para revisar políticas, procedimientos y configuraciones de seguridad.
    - **Revisión Anual:** Revisión exhaustiva anual del plan de seguridad y respuesta a incidentes.
2. **Actividades de Revisión**

    - **Auditorías de Seguridad:** Realización de auditorías de seguridad internas y externas para evaluar la efectividad de las medidas de seguridad implementadas.
    - **Pruebas de penetración:** Contratación de expertos externos para realizar pruebas de penetración y detectar vulnerabilidades.
    - **Revisión de Políticas y Procedimientos:** Evaluación y actualización de políticas y procedimientos de seguridad para asegurar que sigan siendo efectivos y estén alineados con las mejores prácticas y regulaciones actuales.
3. **Informe de Revisión**
    - **Documentación de hallazgos:** Registrar todos los hallazgos de las revisiones y auditorías.
    - **Recomendaciones:** Proporcionar recomendaciones detalladas para abordar cualquier debilidad o área de mejora identificada.
    - **Plan de Acción:** Desarrollar y seguir un plan de acción para implementar las recomendaciones.

3. Asignación de Responsabilidades

3.1 Equipo de Monitoreo

- **Especialista en Seguridad Informática**
    - Monitorear sistemas y redes en tiempo real.
    - Configurar y gestionar herramientas de monitoreo y alertas.
- **Administrador de Sistemas**
    - Supervisar la integridad y disponibilidad de los sistemas.
    - Realizar escaneos de vulnerabilidades y mantener actualizados los sistemas y aplicaciones.

3.2 Equipo de Revisión

- **Auditor de Seguridad Interno**
    - Realizar auditorías internas y revisiones trimestrales.
    - Documentar hallazgos y recomendar mejoras.
- **Consultores Externos**
    - Realizar auditorías externas y pruebas de penetración anuales.
    - Proporcionar una perspectiva independiente sobre la seguridad de la empresa.

3.3 Responsabilidades de Reporte

- **Líder del Proyecto**
    - Coordinar las actividades de monitoreo y revisión.
    - Informar al equipo ejecutivo sobre el estado de la seguridad y cualquier problema identificado.
- **Especialista en Comunicación**
    - Manejar la comunicación interna sobre hallazgos y mejoras.
    - Informar a los clientes y stakeholders sobre las medidas de seguridad y actualizaciones relevantes.

4. Recursos Necesarios

4.1 Tecnológicos

- **Herramientas de Monitoreo y SIEM:** Soluciones como Centreon.
- **Software de Seguridad:** Antivirus, antimalware, y herramientas de escaneo de vulnerabilidades.
- **Infraestructura de Red:** Equipos de red y dispositivos de seguridad actualizados.

4.2 Humanos

- **Equipo de Seguridad Informática:** Especialistas en ciberseguridad y administradores de sistemas.
- **Auditores de Seguridad:** Personal interno y consultores externos especializados en auditorías y pruebas de penetración.

4.3 Financieros

- **Presupuesto para Herramientas de Seguridad:** Asignación de recursos para la adquisición y mantenimiento de herramientas de seguridad.
- **Fondo de Contingencia:** Reserva financiera para responder a incidentes de seguridad imprevistos.

5. Procedimientos de Mejora Continua

5.1 Capacitación y Concienciación

- **Programas de Capacitación Regulares:** Capacitar al personal en nuevas amenazas y mejores prácticas de seguridad.
- **Simulaciones de Incidentes:** Realizar simulaciones periódicas para probar y mejorar la capacidad de respuesta a incidentes.

5.2 Actualización de Políticas y Procedimientos

- **Revisión de Políticas:** Actualizar políticas de seguridad y procedimientos basados en los hallazgos de las auditorías y revisiones.
- **Implementación de Mejores Prácticas:** Adoptar mejores prácticas de la industria y lecciones aprendidas de incidentes previos.

5.3 Innovación Tecnológica

- **Evaluación de Nuevas Tecnologías:** Evaluar e implementar nuevas tecnologías y soluciones de seguridad que puedan mejorar la protección de los activos críticos.
- **Actualización Continua:** Mantener todas las herramientas y sistemas de seguridad actualizados con las últimas versiones y parches.