1.1. Manual de Actividades

Responsable: Joseph Anthony Meneses Salguero

Actividades:

1. Auditoría de Seguridad
2. Formación en Ciberseguridad
3. Gestión de Incidentes de Seguridad
4. Desarrollo y Mantenimiento de Infraestructuras de Seguridad
5. Cumplimiento Normativo en Ciberseguridad

1.1.1. Especificación: actividad 1

1.1.1.1. **Definición:** Evaluación sistemática de los sistemas de información y redes de Little Paw para identificar vulnerabilidades y riesgos de seguridad. Incluye la revisión de controles, políticas y procedimientos de seguridad.

1.1.1.2. **Objetivo:** Garantizar la robustez de las medidas de seguridad y la resiliencia frente a amenazas cibernéticas, manteniendo la protección de datos y la continuidad operativa de Little Paw.

1.1.1.3. Análisis SMART del Objetivo:

1.1.1.3.1. **Específico:** Identificar y mitigar vulnerabilidades en la infraestructura de TI.

1.1.1.3.2. **Medible:** Reducir en un 20% las incidencias de seguridad informática en el próximo año.

1.1.1.3.3. **Alcanzable:** Implementar herramientas avanzadas de detección y análisis de vulnerabilidades.

1.1.1.3.4. **Relevante:** Esencial para la seguridad de datos y la confianza de los usuarios en Little Paw.

1.1.1.3.5. **Temporalmente definido:** Realizar auditorías trimestrales y ajustar las estrategias de seguridad en consecuencia.

1.1.1.4. Análisis PART de la actividad:

1.1.1.4.1. **Procesos:** Evaluación de riesgos, pruebas de penetración, revisión de políticas de seguridad.

1.1.1.4.2. **Actores:** Equipo de ciberseguridad, personal de TI.

1.1.1.4.3. **Recursos:** Herramientas de análisis de seguridad, informes de auditorías anteriores.

1.1.1.4.4. **Tecnología:** Software de gestión de vulnerabilidades, sistemas de detección de intrusiones.

1.1.2. Formación en Ciberseguridad

1.1.2.1. **Definición:** Programa de capacitación y concienciación para empleados sobre prácticas seguras de TI, prevención de ataques de phishing, uso seguro de redes y gestión de contraseñas.

1.1.2.2. **Objetivo:** Incrementar la conciencia sobre ciberseguridad entre los empleados, reduciendo significativamente el riesgo de incidentes de seguridad internos.

1.1.2.3. Análisis SMART del Objetivo:

1.1.2.3.1. **Específico:** Realizar sesiones de formación trimestrales para todo el personal.

1.1.2.3.2. **Medible:** Disminuir en un 30% los incidentes de seguridad originados por errores humanos.

1.1.2.3.3. **Alcanzable:** Desarrollo de materiales de formación atractivos y prácticos.

1.1.2.3.4. **Relevante:** Fundamental para crear una cultura de seguridad y proteger los recursos de la empresa.

1.1.2.3.5. **Temporalmente definido:** Alcanzar una reducción significativa de incidentes en 12 meses.

1.1.2.4. Análisis PART de la actividad:

1.1.2.4.1. **Procesos:** Desarrollo de programas de capacitación, realización de simulacros de phishing.

1.1.2.4.2. **Actores:** Equipo de ciberseguridad, todos los empleados de la empresa.

1.1.2.4.3. **Recursos:** Materiales de capacitación, herramientas de simulación de phishing.

1.1.2.4.4. **Tecnología:** Plataformas de e-learning, herramientas de evaluación de seguridad.

1.1.3. Gestión de Incidentes de Seguridad

1.1.3.1. **Definición:** Proceso de identificación, análisis y respuesta a incidentes de ciberseguridad que puedan afectar a la empresa o comprometer datos.

1.1.3.2. **Objetivo:** Responder de manera rápida y efectiva a incidentes de seguridad, minimizando el impacto en las operaciones de la empresa y la pérdida de datos.

1.1.3.3. Análisis SMART del Objetivo:

1.1.3.3.1. **Específico:** Establecer un equipo de respuesta ante incidentes.

1.1.3.3.2. **Medible:** Reducir el tiempo de respuesta a incidentes en un 50%.

1.1.3.3.3. **Alcanzable:** Capacitación y equipamiento adecuado del equipo de respuesta.

1.1.3.3.4. **Relevante:** Clave para la resiliencia y continuidad del negocio.

1.1.3.3.5. Temporalmente definido: Implementar el equipo de respuesta en 6 meses.

1.1.3.4. Análisis PART de la actividad:

1.1.3.4.1. **Procesos:** Monitoreo de sistemas, análisis de incidentes, respuesta y recuperación.
1.1.3.4.2. **Actores:** Equipo de respuesta a incidentes, personal de TI.
1.1.3.4.3. **Recursos:** Herramientas de monitoreo y análisis, protocolos de respuesta.
1.1.3.4.4. **Tecnología:** Sistemas de gestión de incidentes, software de recuperación de datos.

1.1.4. Desarrollo y Mantenimiento de Infraestructuras de Seguridad

1.1.4.1. **Definición:** Diseño, implementación y mantenimiento de soluciones de seguridad como firewalls, antivirus, y sistemas de detección de intrusiones.

1.1.4.2. **Objetivo:** Mantener una infraestructura de seguridad robusta y actualizada para proteger contra amenazas cibernéticas externas e internas.

1.1.4.3. Análisis SMART del Objetivo:

1.1.4.3.1. **Específico:** Implementar tecnologías de seguridad avanzadas en todos los sistemas críticos.
1.1.4.3.2. **Medible:** Alcanzar cero brechas de seguridad a través de estas tecnologías en un año.
1.1.4.3.3. **Alcanzable:** Actualización periódica y pruebas de las soluciones de seguridad.
1.1.4.3.4. **Relevante:** Fundamental para la protección de datos y sistemas de la empresa.
1.1.4.3.5. **Temporalmente definido:** Realizar actualizaciones de seguridad trimestrales.

1.1.4.4. Análisis PART de la actividad:

1.1.4.4.1. **Procesos:** Evaluación de tecnologías, instalación y configuración de herramientas, mantenimiento continuo.
1.1.4.4.2. **Actores:** Ingenieros de seguridad, administradores de sistemas.
1.1.4.4.3. Recursos: Soluciones de seguridad, presupuesto para tecnología.
1.1.4.4.4. **Tecnología:** Software y hardware de seguridad, sistemas de monitoreo.

1.1.5. Cumplimiento Normativo en Ciberseguridad

1.1.5.1. **Definición:** Asegurar que todas las operaciones de TI y manejo de datos cumplan con las leyes y regulaciones pertinentes en materia de ciberseguridad y privacidad de datos.

1.1.5.2. **Objetivo:** Garantizar el cumplimiento total con las normativas para evitar sanciones legales y mantener la reputación de la empresa.

1.1.5.3. Análisis SMART del Objetivo:

1.1.5.3.1. **Específico:** Implementar políticas de cumplimiento en toda la empresa.

1.1.5.3.2. **Medible:** Lograr cero infracciones en auditorías de cumplimiento.

1.1.5.3.3. **Alcanzable:** Capacitación regular sobre normativas y leyes.

1.1.5.3.4. **Relevante:** Crucial para la operación legal y ética de la empresa.

1.1.5.3.5. Temporalmente definido: Establecer programas de cumplimiento en 9 meses.

1.1.5.4. Análisis PART de la actividad:

1.1.5.4.1. **Procesos:** Revisión de políticas, auditorías internas, actualización de procedimientos.

1.1.5.4.2. **Actores:** Equipo legal, equipo de ciberseguridad.

1.1.5.4.3. **Recursos:** Documentación legal, herramientas de auditoría.

1.1.5.4.4. **Tecnología:** Plataformas de gestión de cumplimiento, bases de datos de regulaciones.