6.5. Manual de Actividades

6.5.1. Responsable: Dylan Chambi

6.5.2. Actividades:

1. Desarrollo de políticas de gestión de tecnología.
2. Construcción de un manual de buenas prácticas de seguridad informática adaptado a las necesidades de la empresa.
3. Programación de presupuestos para proyectos y mejoras tecnológicas.
4. Coordinación de ejercicios de respuesta a incidentes de indisponibilidad o poca tolerancia a fallos.
5. Evaluación y selección de herramientas y tecnologías de seguridad para fortalecer la infraestructura tecnológica.
6. Mantenimiento y actualización de políticas de acceso y autorización a sistemas y datos sensibles.

6.5.3. Especificación: Actividad 1

6.5.3.1. Definición

La actividad de "Desarrollo de políticas de gestión de tecnología" se refiere al proceso de crear un conjunto estructurado de directrices, principios y normativas que rigen el uso, implementación y mantenimiento de tecnologías de la información en una organización. Estas políticas están diseñadas para establecer un marco claro y coherente que guíe las decisiones y acciones relacionadas con la gestión de la tecnología dentro de la empresa.

6.5.3.2. Objetivo

Definir e implementar las políticas de para la gestión informática que dan las pautas y rigen para la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general, sobre el ambiente tecnológico de la empresa “TIGO”, para su interiorización, aplicación y verificación permanente.

6.5.3.3. Análisis SMART

- **Específico:** Las políticas deben abordar áreas específicas, como el uso de recursos, seguridad de la información y cumplimiento normativo.
- **Medible:** Se establecerán indicadores para evaluar la conformidad, la eficiencia en el uso de recursos y la mejora continua de los procesos.
- **Alcanzable:** Se considerarán los recursos disponibles y se establecerá un cronograma realista para el desarrollo e implementación de las políticas.
- **Real:** Se evaluará la conexión entre las políticas y la estrategia general de la empresa, asegurando que aborden las necesidades y desafíos específicos.
- **Tiempo:** Se definirán fechas límite para la redacción, revisión y aprobación de las políticas, así como para la implementación de medidas concretas.

6.5.3.4. Definición PART

Procesos:

- Análisis de riesgos tecnológicos
- Desarrollo de roles y responsabilidades
- Creación de manuales de gestión informática
- Asignación de privilegios de acceso
- Revisión de flujos de información

Actores:

- Director Ejecutivo
- CIO
- Director de IT
- Jefe de Ingenieros de Redes
- Jefe de Administradores de Sistemas

Recursos:

- Equipos Informáticos

- Equipos Teleinformáticos
- Documentación Legal
- Servicios de Gestión de Servicios
- Sistemas de Seguridad Física

Tecnológica:

- Seguridad basada en el software
- Firewalls
- Seguridad en Internet de las cosas (IoT)
- Análisis del comportamiento del usuario y de las Entidades (UEBA)
- Microsegmentación y flujo de visibilidad
- Navegador remoto seguro

6.5.4. Especificación: Actividad 2

6.5.4.1. Definición

La actividad de "Construcción de un manual de buenas prácticas de seguridad informática adaptado a las necesidades de la empresa" es el proceso de desarrollar un documento detallado que establece las normas, directrices y procedimientos específicos para garantizar la seguridad de la información y los sistemas tecnológicos dentro de una organización.

6.5.4.2. Objetivo

El objetivo principal de la construcción de este manual es proporcionar a los usuarios internos una guía clara y práctica que les permita adoptar y mantener prácticas seguras en el uso de la tecnología y la gestión de la información.

6.5.4.3. Análisis SMART

- **Específico**: Las políticas deben abordar áreas específicas, como el uso de recursos, seguridad de la información y cumplimiento normativo.

- **Medible**: Se establecerán indicadores para evaluar la conformidad, la eficiencia en el uso de recursos y la mejora continua de los procesos.
- **Alcanzable**: Se considerarán los recursos disponibles y se establecerá un cronograma realista para el desarrollo e implementación de las políticas.
- **Real**: Se evaluará la conexión entre las políticas y la estrategia general de la empresa, asegurando que aborden las necesidades y desafíos específicos.
- **Tiempo**: Se definirán fechas límite para la redacción, revisión y aprobación de las políticas, así como para la implementación de medidas concretas.

6.5.4.4. Definición PART

Procesos:

- Investigación de Mejores Prácticas
- Desarrollo de Contenidos
- Revisión y Aprobación
- Implementación y Comunicación
- Capacitación y Concientización

Actores:

- Director Ejecutivo
- CIO
- Director de IT
- Jefe de Ingenieros de Redes
- Jefe de Administradores de Sistemas

Recursos:

- Equipos Informáticos
- Equipos Teleinformáticos
- Documentación Legal
- Servicios de Gestión de Servicios

- Sistemas de Seguridad Física

Tecnológica:

- Sistemas de Gestión de Contenidos (CMS)
- Herramientas de Seguimiento y Auditoría
- Plataformas de Encuestas y Retroalimentación
- Plataformas de Capacitación en Línea

6.5.5. Especificación: Actividad 3

6.5.5.1. Definición

La actividad de "Programación de presupuestos para proyectos y mejoras tecnológicas" se refiere al proceso de planificación y asignación de recursos financieros necesarios para la ejecución de proyectos y la implementación de mejoras tecnológicas dentro de una organización. Esta actividad implica la estimación y asignación de fondos de manera estratégica, considerando los costos asociados con la adquisición de tecnología, desarrollo de proyectos y cualquier otra iniciativa destinada a mejorar la infraestructura tecnológica de la empresa.

6.5.5.2. Objetivo

La programación de presupuestos para proyectos y mejoras tecnológicas es garantizar una asignación eficiente y efectiva de recursos financieros que respalden el desarrollo, implementación y mantenimiento de proyectos tecnológicos.

6.5.5.3. Análisis SMART

- **Específico**: Desarrollar un proceso detallado para la planificación y asignación de recursos financieros destinados a proyectos y mejoras tecnológicas dentro de la empresa.
- **Medible**: Establecer métricas y criterios cuantificables para evaluar la eficacia y la eficiencia en la asignación de recursos financieros.

- **Alcanzable**: Cumplir con los presupuestos establecidos y lograr los objetivos tecnológicos sin comprometer la estabilidad financiera.
- **Real**: Alinear la programación de presupuestos con los objetivos estratégicos de la empresa y las necesidades críticas de la infraestructura tecnológica.
- **Tiempo**: Cumplir con los plazos establecidos para cada fase del proceso de programación de presupuestos.

6.5.5.4. Definición PART

Procesos:

- Análisis de Costos y Estimaciones
- Priorización de Proyectos
- Desarrollo de Presupuestos
- Revisión y Aprobación
- Monitoreo y Control
- Reporte de Rendimiento

Actores:

- Director Ejecutivo
- CIO
- Director de IT
- Jefe de Ingenieros de Redes
- Jefe de Administradores de Sistemas

Recursos:

- Software de Contabilidad y Presupuesto
- Historial de Gastos
- Equipos Informáticos
- Documentación Legal

Tecnológica:

- Software de Gestión de Proyectos

- Herramientas de Análisis Financiero
- Sistemas de Monitoreo Financiero
- Sistemas de Informes Empresariales

6.5.6. Especificación: Actividad 4

6.5.6.1. Definición

La actividad de "Coordinación de ejercicios de respuesta a incidentes de indisponibilidad o poca tolerancia a fallos" se refiere al proceso planificado y controlado de organizar y llevar a cabo simulacros o ejercicios prácticos diseñados para evaluar y mejorar la capacidad de una organización para responder de manera efectiva a incidentes que afectan la disponibilidad o la tolerancia a fallos de sus sistemas o servicios. Estos ejercicios simulan situaciones de crisis con el propósito de fortalecer la preparación, identificar áreas de mejora y garantizar una respuesta rápida y eficiente en situaciones reales.

6.5.6.2. Objetivo

El objetivo de la coordinación de ejercicios de respuesta a incidentes de indisponibilidad o poca tolerancia a fallos es mejorar la resiliencia y capacidad de recuperación de una organización frente a eventos que puedan afectar la disponibilidad de sus sistemas críticos.

6.5.6.3. Análisis SMART

- **Específico**: Diseñar y ejecutar simulacros realistas que imitan situaciones de indisponibilidad o poca tolerancia a fallos en los sistemas críticos de la organización.
- **Medible**: Establecer métricas cuantificables para evaluar la eficacia de la respuesta a incidentes, el tiempo de recuperación y la capacidad de los equipos para seguir los procedimientos establecidos.

- **Alcanzable**: Garantizar que los ejercicios sean realistas y realizables, considerando los recursos disponibles y la complejidad de los sistemas involucrados.
- **Real**: Asegurar que los ejercicios estén alineados con los riesgos específicos de indisponibilidad y poca tolerancia a fallos enfrentados por la organización.
- **Tiempo**: Establecer un cronograma claro para la planificación, ejecución y evaluación de los ejercicios de respuesta a incidentes.

6.5.6.4. Definición PART

Procesos:

- Planificación de Pruebas no Funcionales
- Simulación de Escenarios
- Comunicación y Notificación
- Monitoreo y Evaluación en Tiempo Real
- Recopilación de Datos y Retroalimentación
- Actualización de Procedimientos

Actores:

- Director Ejecutivo
- CIO
- Director de IT
- Jefe de Ingenieros de Redes
- Jefe de Administradores de Sistemas

Recursos:

- Personal Encargado de Pruebas como Cliente
- Equipos Informáticos
- Equipos Teleinformáticos
- Datos de Casos Máximos para cada Sistema

Tecnológica:

- Herramientas de Monitoreo y Registro
- Software de Logs de Sistemas
- Software de Pruebas de Sistemas Informáticos
- Software de Simulación de Datos y Escenarios

6.5.7. Especificación: Actividad 5

6.5.7.1. Definición

La actividad de "Evaluación y selección de herramientas y tecnologías de seguridad para fortalecer la infraestructura tecnológica" se refiere al proceso sistemático y cuidadoso de analizar, comparar y elegir las soluciones tecnológicas más adecuadas para mejorar la seguridad de la infraestructura tecnológica de una organización.

6.5.7.2. Objetivo

El objetivo principal de la evaluación y selección de herramientas y tecnologías de seguridad es fortalecer la postura de seguridad de la infraestructura tecnológica de la organización.

6.5.7.3. Análisis SMART

- **Específico**: Evaluar y seleccionar herramientas y tecnologías de seguridad específicas que aborden las vulnerabilidades y riesgos identificados en la infraestructura tecnológica de la organización.
- **Medible**: Establecer criterios de evaluación cuantificables para comparar y medir el rendimiento, la eficacia y la adecuación de las herramientas y tecnologías de seguridad.
- **Alcanzable**: Garantizar que la evaluación y selección se realicen de manera realista, considerando los recursos disponibles y la viabilidad de implementar las soluciones seleccionadas.

- **Real**: Asegurar que la evaluación y selección estén alineadas con las metas y objetivos de seguridad de la organización, abordando las amenazas y riesgos más pertinentes.
- **Tiempo**: Establecer un cronograma claro y realista para llevar a cabo la evaluación, toma de decisiones y la implementación de las nuevas herramientas y tecnologías de seguridad.

6.5.7.4. Definición PART

Procesos:

- Investigación de Soluciones en el Mercado
- Definición de Criterios de Evaluación
- Evaluación de Cumplimiento Normativo
- Selección y Toma de Decisiones
- Planificación de Implementación

Actores:

- Director Ejecutivo
- CIO
- Director de IT
- Jefe de Ingenieros de Redes
- Jefe de Administradores de Sistemas

Recursos:

- Herramientas de Evaluación
- Ambiente de Pruebas
- Marco Normativo y Requisitos de Cumplimiento

Tecnológica:

- Sistemas de Gestión de Identidad (IDM)
- Soluciones de Seguridad en la Nube
- Sistemas de Prevención de Pérdida de Datos (DLP)
- Sistemas de Registro y Auditoría

6.5.8. Especificación: Actividad 6

6.5.8.1. Definición

La actividad de "Mantenimiento y actualización de políticas de acceso y autorización a sistemas y datos sensibles" se refiere al proceso continuo de revisar, ajustar y mejorar las políticas y procedimientos que rigen el acceso y la autorización a sistemas informáticos y a datos confidenciales o sensibles dentro de una organización. Esta actividad implica la gestión proactiva de las políticas para garantizar que reflejen de manera precisa y efectiva las necesidades cambiantes del negocio, los requisitos de seguridad y las amenazas emergentes.

6.5.8.2. Objetivo

El objetivo principal de esta actividad es asegurar que la infraestructura tecnológica y los datos sensibles de la organización estén protegidos de manera eficiente y en línea con las mejores prácticas de seguridad.

6.5.8.3. Análisis SMART

- **Específico**: Revisar y actualizar de manera regular las políticas de acceso y autorización para reflejar cambios organizativos, tecnológicos y normativos, asegurando que estén alineadas con las necesidades actuales de seguridad.
- **Medible**: Establecer métricas para evaluar la eficacia y la actualización de las políticas, incluyendo la reducción de incidentes de seguridad relacionados con el acceso no autorizado y la adaptación a nuevos requisitos normativos.
- **Alcanzable**: Asegurar que la actividad sea realizada de manera realista y factible, considerando la disponibilidad de recursos y la capacidad de implementar los cambios necesarios en tiempo y forma.
- **Real**: Evaluación de la relevancia de las actualizaciones en relación con los cambios identificados.

- **Tiempo**: Establecer plazos y frecuencias definidas para la revisión y actualización de políticas, garantizando que la actividad sea oportuna y se lleve a cabo regularmente.

6.5.8.4. Definición PART

Procesos:

- Monitoreo Continuo de Cambios
- Evaluación de Riesgos y Amenazas
- Actualización de Controles de Acceso
- Auditoría de Acceso
- Gestión de Incidentes

Actores:

- Director Ejecutivo
- CIO
- Director de IT
- Jefe de Ingenieros de Redes
- Jefe de Administradores de Sistemas

Recursos:

- Herramientas de Gestión de Políticas
- Sistema de Auditoría y Monitoreo
- Documentación de Políticas
- Sistema de Comunicación Interna

Tecnológica:

- Sistemas de Gestión de Identidad y Acceso (IAM)
- Sistemas de Detección de Intrusiones (IDS)
- Sistemas de Gestión de Eventos e Información de Seguridad
- Sistemas de Gestión de Políticas de Seguridad