PLAN DE CAPACITACIÓN PARA EL MANEJO DEL PLAN DE CONTINGENCIA

ANAS WAYUU
EMPRESA PROMOTORA DE SALUD INDÍGENA
E.P.S.I.
Juntos Gestionamos Salud.

Maicao, La Guajira

CONTENIDO

1. INTRODUCCIÓN

La continuidad operativa es esencial para garantizar la prestación de servicios de calidad en cualquier organización, especialmente en el ámbito de la salud. Ante la diversidad de riesgos que pueden afectar nuestros sistemas de información, es imperativo contar con un Plan de Contingencia sólido y, sobre todo, con un equipo capacitado para implementarlo eficazmente.

En la EPSI Anas Wayuu, reconocemos la vital importancia de prepararnos para afrontar y superar posibles interrupciones en nuestras operaciones. La continuidad de nuestros servicios es vital, especialmente en el contexto de la gestión del riesgo de salud.

A lo largo de este plan de capacitación, abordaremos estrategias específicas diseñadas para afrontar los riesgos identificados en nuestro entorno operativo. Desde la concientización inicial sobre la importancia del Plan de Contingencia hasta la capacitación detallada en acciones concretas ante escenarios críticos, donde cada etapa de este programa busca fortalecer nuestras capacidades individuales y colectivas.
Esta capacitación no solo se enfoca en la teoría, sino que se nutre de ejercicios prácticos, simulacros y la revisión constante de nuestros procedimientos. Además, se plantea como un proceso de mejora continuo, para fortalecer nuestra preparación y capacidad de respuesta.

En EPSI Anas Wayuu, nos comprometemos a estar a la vanguardia en la gestión de riesgos y la protección de nuestros sistemas de información. Este plan de capacitación es un paso clave en nuestra misión de asegurar la continuidad de nuestras operaciones, proteger la información sensible y garantizar la atención ininterrumpida a nuestros afiliados y beneficiarios.

2. OBJETIVO DE LA CAPACITACIÓN

Capacitar al personal de EPSI Anas Wayuu en el reconocimiento, evaluación y manejo efectivo de riesgos que puedan afectar los sistemas de información de la organización, dotándolos de las habilidades y conocimientos esenciales para enfrentar y gestionar contingencias de manera eficaz.

3. OBJETIVOS ESPECÍFICOS

- Capacitar al personal en la identificación proactiva de posibles riesgos para los sistemas de información, mediante la comprensión y análisis de vulnerabilidades potenciales en la red y las plataformas tecnológicas de EPSI Anas Wayuu.

- Dotar al equipo con las herramientas y metodologías necesarias para evaluar la magnitud y el impacto de los riesgos identificados, permitiendo priorizar y categorizar las amenazas potenciales en los sistemas de información de la organización.

- Capacitar al personal en la elaboración y ejecución de planes de contingencia efectivos, proporcionando pautas y procedimientos claros para responder de manera ágil y eficiente ante posibles incidentes o vulnerabilidades que puedan afectar los sistemas de información de EPSI Anas Wayuu.

4. PÚBLICO OBJETIVO

Este plan de capacitación está específicamente diseñado para los empleados del área de Tecnología y Comunicaciones (TYC) de la EPSI ANAS WAYUU, quienes están directamente involucrados en el manejo, procesamiento o acceso a datos personales en el curso de sus funciones.

5. DURACIÓN Y FORMATO

La capacitación se llevará a cabo una vez al año a lo largo de un periodo de dos semanas. Estas sesiones se realizarán de manera presencial en las instalaciones de la empresa para facilitar la participación de los empleados del área de Tecnología y Comunicaciones (TYC) de la EPSI Anas Wayuu. Los métodos de entrega pueden incluir sesiones presenciales, seminarios web y material impreso. La duración total de la capacitación se organizará en sesiones gestionables.

6. CONTENIDO DE LA CAPACITACIÓN

6.1 INTRODUCCIÓN A LA GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

- Definición de riesgos operativos en sistemas de información.

- Importancia del Plan de Contingencia en la continuidad del negocio.
- Identificación y comprensión de los riesgos previamente identificados en el plan de contingencia.

6.2 ESTRATEGIAS DE CONTINUIDAD ANTE RIESGOS DE INFRAESTRUCTURA TECNOLÓGICA

- Acciones preventivas y de respuesta frente a daños en la infraestructura tecnológica.
- Alternativas operativas para garantizar la continuidad en caso de no disponibilidad de la infraestructura física.

6.3 RESPALDO Y PROTECCIÓN DE INFORMACIÓN CRÍTICA

- Prácticas de seguridad informática para evitar la pérdida de información por ciberataques, virus informáticos y otros riesgos identificados.
- Uso de herramientas y servicios de respaldo de información en la nube.

6.4 GESTIÓN DE FALLOS DEL SISTEMA DE INFORMACIÓN Y CONECTIVIDAD

- Identificación de medidas para enfrentar fallas en el sistema principal y falta de conectividad a internet.
- Estrategias para mantener la continuidad de operaciones ante estas eventualidades.

6.5 PLANIFICACIÓN DE RECURSOS HUMANOS PARA CONTINUIDAD OPERATIVA

- Acciones específicas para abordar la falta de disponibilidad de recursos humanos en situaciones críticas.
- Documentación y entrenamiento para asegurar la ejecución de procesos incluso ante ausencias imprevistas.

6.6 IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA Y EVALUACIÓN FINAL

- Ejercicio práctico: simulación de un escenario crítico para aplicar lo aprendido.
- Revisión y evaluación del aprendizaje, identificación de áreas de mejora y próximos pasos.

7. SEGUIMIENTO Y ACTUALIZACIÓN

Se establecerán mecanismos de seguimiento para evaluar la efectividad de la capacitación y se programarán actualizaciones periódicas para mantener a los empleados informados sobre cambios en las políticas o regulaciones.

8. CONTROL DE CAMBIOS

VERSIÓN	PAGINAS	FECHA INICIAL	FECHA DE ACTUALIZACIÓN	DESCRIPCIÓN DE CAMBIOS
1.0	Seis (6)	14/05/2023	No Aplica	Creación