ÍNDICE

I. OBJETIVO

Establecer la normatividad de aplicación general en el uso correcto de los recursos, bienes y servicios informáticos y de tecnologías de la información y las responsabilidades que debe de seguir los usuarios de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Yucatán.

II. ALCANCE

Aplica al personal de base, confianza, prestadores de servicios profesionales, servicio social y a todo el personal que haga uso de recursos, bienes o servicios informáticos y de tecnologías de la información de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Yucatán.

III. FUNDAMENTO LEGAL

Ámbito Federal

Artículo 113, Constitución Política de los Estados Unidos Mexicanos

Artículos 1, y 3, fracciones VIII y XIII de la Ley General del Sistema Nacional Anticorrupción.

Ámbito Estatal

Artículo 101 Bis de la Constitución Política del Estado de Yucatán.

Artículos 1, 30, 32, fracción III y 36 de la Ley del Sistema Estatal Anticorrupción de Yucatán.

Artículo 7 de la Ley de Responsabilidades Administrativas del Estado de Yucatán.

Artículos 4, fracción II, 26, 27 fracciones I, III, IV y VII, 32 fracciones II, XIV, XV y XVI del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

Artículos 8, primer párrafo y 51 primer y cuarto párrafo del Código de la Administración Pública de Yucatán.

Artículos 5, 22, fracción III y 26, fracción VI, incisos a, e y f de los Lineamientos para la implementación del Sistema de Control Interno Institucional en las dependencias y entidades de la Administración Pública Estatal.

IV. DEFINICIONES

Carpetas Compartidas: Espacio de almacenamiento de archivos de trabajo centralizado que pueden ser accedidos por múltiples usuarios de forma segura.

DTI: Departamento de Tecnologías de la Información.

RVDV: Red de Voz, Datos y Video.

EDR: Equipos de red como: firewall, switches, Access Points.

CCTV: Sistema de Vigilancia.

Site: Cuarto de telecomunicaciones y equipos de computo.

PR: Plan de Respaldo.

PR: Plan de Recuperación.

PE: Plan de Emergencia.

Contingencia: Interrupción no planificada de la disponibilidad de los recursos informáticos.

Servidor de Archivos: Es un tipo de servidor que almacena y distribuye diferentes tipos de archivos informáticos entre los clientes de una red de computadoras. Su función es permitir el acceso remoto de otros modos a los archivos que almacena o sobre los que tiene acceso.

Servidor de Usuarios: Este servidor es propio de la Secretaría Ejecutiva y esta destinado para el trabajo del personal adscrito.

Direcciones: Direccion de Administración y Finanzas, Dirección Jurídica, Dirección de Analisis y Póliticas Públicas, Dirección de Vinculación Interinstitucional.

Secretario Técnico: Secretario Técnico de la Secretaria Ejecutiva del Sistema Estatal Anticorrupción.

SESEAY: Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Yucatán

V. POLÍTICAS

Políticas Generales:

1. El presentes Plan de Contingencia es aprobado por el Titular de la SESEAY en cumplimiento al Código de la Administración Pública de Yucatán.
2. Las situaciones no previstas dentro de las presentes políticas serán resueltas por el Director de Administración y Finanzas.

3. Cualquier modificación a las presentes políticas, deberá ser aprobada por el Director de Administración y Finanzas.
4. Las presentes políticas entran en vigor al día siguiente de su aprobación y publicación.
5. El responsable de dirigir el desarrollo integral del proyecto así como de verificar el cumplimiento de las actividades encargadas a cada uno de los lideres será el Jefe del Departamento de Tecnologías de la Información.

VI. DESCRIPCIÓN DEL PROCEDIMIENTO

Políticas Específicas:

1. Análisis y Valoración de Riesgos.

1.1. Identificar las preocupaciones y prioridades de que deberá asumir la SESEAY en el caso que exista una indisponibilidad en los sistemas informáticos producida por una contingencia.

1.2. Identificar el tiempo máximo en el que un proceso critico de la SESEAY deberá ser restaurado para su normal y eficiente continuidad.

1.3. Identificar el impacto en las aplicaciones que soportan los procesos críticos de la SESEAY.

1.4. Proporcionar las bases de una estrategia para la contingencia operativa en caso de un desastre.

1.5. Fallas probables que causen interrupción en la operación.

Corte en la comunicación Cliente/Servidor: Fallas en el medio físico del Cable UTP y Fibra Óptica, Fallas en las Tarjetas de Red, Fallas de alimentación y comunicación con switches, Fallas de alimentacioón y comunicación con Firewalls, Fallas de alimentación y comunicación con ONTS, Fallas en nodos de red, Fallas en nodos de Patch Panel, Rompimiento de la Fibra Óptica del ISP.

Problemas de Comunicación con los Servidores: Fallas en las tarjetas de Ethernet, Fallas con las fuentes de alimentación, Fallas con memorias RAM, Fallas con Tarjeta Madre, Fallas con los CPUS, Fallas en discos duros, Amenazas cibernéticas.
Problemas de energía: Fallas con transformadores, Fallas en tableros eléctricos, Problemas con supresor de tierra física, Problemas Eléctricos en subestaciones, Cortes eléctricos por desastres naturales.

Humanas: Ausencia de algún miembro del "DTI", por accidentes, enfermedades, vacaciones, renuncia imprevista o despido.

Perdida de Servicio de Internet: Fallas de comunicación con Switches, Fallas de comunicación por cortes en Fibra Óptica, Daños en la Infraestructura del ISP, Fallas con software de equipos de comunicación.

Indisponibilidad del Centro de Datos: Destrucción del Site por desastre naturales, Sabotaje, Cortos circuitos, Incendios, Secuestro de Servidores por malware.

2. MEDIDAS PREVENTIVAS Y EVALUACIÓN DE RIESGOS

2.1. Definir medidas efectivas para controlar los diferentes accesos a los activos computacionales, e identificar en caso de que existan.
   2.1.1. Acceso físico de personas no autorizadas
   2.1.2. Acceso a la red
   2.1.3. Acceso a servidores
   2.1.4. Acceso a "EDR"
   2.1.5. Acceso restringido a programas y datos
2.2. Medidas prventivas.
   2.2.1. Portar indentificación y llave para acceder al "SITE".

2.2.2. Generar contraseñas y usuarios para acceder a los "EDR"

2.2.3. Generar contraseñas y usuarios para acceder a Servidores

2.2.4. Sistema de "CCTV" para monitorear áreas restringidas y de acceso

2.2.5. Capacitación del "DTI" para mantener al día la seguridad del "SITE"

2.2.6. Realizar simulacros y Auditorias internas.

2.2.7. Realizar Respaldos de información por parte de usuarios y del personal de "DTI"

2.2.8. Respaldos independientes para información financiera y cualquier información que sea sensible e importante por parte del área de Administración

3. Procesos Indentificados.

3.1. De alto riesgo.

Equipo	Costo	Riesgo	Impacto
Servidor de Usuarios	Medio	Alto	Alto
Servidor de Aplicativos	Alto	Alto	Alto
Switch core	Medio	Alto	Alto
Firewall Core	Medio	Alto	Alto
UPS Core	Medio	Alto	Alto
www.seay.org.mx	Medio	Alto	Alto
L1 Total Play	Medio	Alto	Alto
L2 Total Play	Medio	Alto	Alto
Transformador principal	Alto	Alto	Alto
Servidor de archivos	Alto	Alto	Alto

3.2. De riesgo medio.

Equipo	Costo	Riesgo	Impacto

Terminales de usuarios	Medio	Medio	Medio
Equipos de directores	Medio	Medio	Medio
Equipo de telefonia	Medio	Medio	Medio

4. Previsión de desastres naturales.

    4.1. Monitorear sobre posibles desastres naturares que puedan afectar la continuidad de la operación, los desastres que puedan afectar son los siguientes:
    - Huracanes
    - Ciclones
    - Tormentas electricas
    - Inundaciones

    4.2. Acciones en caso de existir alguna amenaza natural:
    - Respaldo de información en discos externos
    - Respaldo de información en el servidor de archivos
    - Resguardo de terminales y equipos de usuarios
    - Verificar el estado de los UPS y su baterias
    - Reforzar entradas y accesos al "SITE"
    - Reforzar entradas y accesos al area del "DTI"
    - Realizar guardias para monitoreo del "SITE" y de la "RVDV" por parte del "DTI"

5. Previsión de riesgos tecnológicos.
    5.1. Riesgos de naturaleza tecnologica, que puedan afectar la continuidad de la operación, tales como:

    - Incendios eléctricos
    - Fallas de energía y accidentes de transmisión y transporte
    - Corto circuito en los "EDR"
    - Corto circuito en los "SERVIDORES"

5.2. Acciones en caso de existir algun riesgo tecnologíco:

- Extintores especiales para fuego de clase C y clase D
- Respaldos diarios para evitar la perdida de información
- Equipos de redundacia para garantizar la pronta recuperación
- Generador electrico de respaldo
- Pólizas de garantias vigentes

6. Previsión de riesgos sociales.

6.1. Riesgos de naturaleza social, que puedan afectar la continuidad de la operación, tales como:

- Sabotaje en el suministro electrico
- Sabotaje en la Red del ISP
- Violación en las zonas restringidas
- Robo de los "EDR"
- Actos terroristas y desordenes
- Amenazas ciberneticas
- Secuestro de informacion por ransomware
- Errores humanos que puedan generar la perdida de datos

6.2. Acciones en caso de existir algun riesgo social:

- Política de respaldo actualizada
- Política de ciberseguridad actualizada
- Controles de acceso en SITE y DTI
- Sistema de CCTV actualizado y funcionando
- Licenciamiento activo para Firewall
- Capacitación para los usuarios

VII. INDICADOR

Indicador	Fórmula	Unidad de medida	Periodicidad	Meta
N/A	N/A	N/A	N/A	N/A

VIII. ANEXOS

Código	Nombre del anexo	Ubicación	AT*	AC*	PTC*	Disposición final
N/A	N/A	N/A	N/A	N/A	N/A	N/A

*AT= Archivo de trámite; AC= Archivo de concentración; PTC= Plazo total de conservación.

IX. CONTROL DE CAMBIOS

Fecha	Número de revisión	Actividad
02/12/2021	00	Generación del Documento para el Plan de Contingencia Informático de la Secretaria Ejecutiva del Sistema Estatal Anticorrupción de Yucatán

X. FIRMA DE AUTORIZACIÓN DEL DOCUMENTO

Autorizó	**Vo Bo**
Lic. Edwin Manuel Rejón Pacheco **Secretario Técnico**	**C.P. Lauro Ismael Canché Cháves** **Director de Administración y Finanzas**