Logotipo

Descripción generada automáticamente

COMPAÑÍA DE SISTEMAS DEL BATALLÓN DE TIC’S

NO. WGCR-01-02-23

EJÉRCITO DE GUATEMALA

REPÚBLICA DE GUATEMALA

PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO NO. CIASISOP-002-CIT-WGCR-2022-A

EJÉRCITO DE GUATEMALA

**PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO NO. CIASISOP-002-CIT-WGCR-2022-A**

1. **INTRODUCCIÓN:**

El Comando de Informática y Tecnología debe estar organizado y preparado para prevenir, proteger y reaccionar ante un incidente en los servicios críticos los cuales se encuentra ubicados en el Centro de Datos de la zona 10, en el interior del Ministerio de la Defensa Nacional. Con este Plan se describirán las fases para establecer un periodo de recuperación mínimo, considerando no comprometer la disponibilidad de los servicios para todas las dependencias del Ministerio de la Defensa Nacional. El tiempo para resolver una caída de los servicios críticos es de mucha importancia, debido a que muchas operaciones y órdenes a nivel Ejército, dependen de ellos.

1. **FASES DEL PLAN:**
2. **FASE 0. DETERMINACIÓN DEL ALCANCE:**
3. **ENFOQUE POR ACTIVO:**

Mantener en estado operativo el Data Center, para que, al momento de ser interrumpidos los servicios, puedan ser recuperados en el término no mayor a tres horas. Que exista una comunicación de datos e internet por medio de los enlaces estratégicos del MDN.

1. **ENFOQUE POR PROCESO:**

Que los servicios de base de datos, correo militar, correo institucional, AUTOCOM, Active Directory y enlaces de datos e internet se encuentren funcionando normalmente.

1. **FASE 1. ANÁLISIS DE LA ORGANIZACIÓN:**
2. **MANTENER REUNIONES:**

El Comando de Informática y Tecnología, organizará reuniones semestrales (enero y julio) con el personal de la Compañía de Sistemas y con los administradores del Correo militar de cada dependencia militar, a efecto se den a conocer las fases del plan de contingencia. Así mismo se tendrán reuniones con el proveedor del servicio de datos e internet, a efecto se establezcan las medidas a tomar y tiempo de respuesta en caso el servicio sea inestable o nulo.

1. **ANALISIS DE IMPACTO SOBRE EL NEGOCIO:**
2. **RTO (Tiempo de Recuperación):**

El tiempo máximo que se tendrá para restaurar el servicio de correo militar en el Data Center es de **tres (03) horas**.

El tiempo máximo que se tendrá para restaurar el servicio de correo institucional en el Data Center es de **cinco (05) horas**.

El tiempo máximo que se tendrá para restaurar los enlaces de datos e internet en el Data Center es de **tres (03) horas**.

El tiempo máximo que se tendrá para restaurar el servicio de AUTOCOM en el Data Center es de **tres (03) horas**.

El tiempo máximo que se tendrá para restaurar el servicio de Base de Datos en el Data Center es de **una (01) hora**.

**Recursos Humanos y Tecnológicos empleados en el proceso:**

Es necesario una persona con conocimientos de sistemas operativos, una persona con conocimientos de las configuraciones de la red e internet, una persona con conocimientos de soporte técnico en software, hardware y redes; como recurso tecnológico es necesario: Servidores de respaldo que posea las mismas configuraciones e información de los servidores principales que presenten problemas (un espejo), una redundancia de internet y redundancia de energía eléctrica. El personal determinado como **crítico** sin reemplazo es el Encargado de sistemas operativos, el administrador de la base de datos y el encargado de redes.

1. **MTD (Tiempo máximo tolerable de caída):**

El servicio de correo militar puede permanecer caído **1 día.**

El servicio de correo institucional puede permanecer caído **5 días**

El servicio de enlaces de datos e internet puede permanecer caído **1 día.**

El servicio de AUTOCOM puede permanecer caído **3 días.**

El servicio de Base de Datos puede permanecer caído **1 días.**

 Posterior a este tiempo se crearía un caos en la comunicación de información.

1. **ROL (Niveles mínimos de recuperación de servicio):**

Tres (03) horas es el tiempo mínimo de recuperación del servicio en caso de cualquier desastre en el Centro de Datos, pudiendo ser un **75% funcional.**

**Dependencias de otros procesos internos o proveedores externos:**

Se coordinará con la empresa proveedora de internet un plan de recuperación ante desastres de la inmediata restauración del servicio que provee; con la finalidad de no heredar una contingencia al Comando de Informática y Tecnología.

1. **RPO (Grado de dependencia de la actualidad de los datos):**

El servicio de datos e internet tiene un impacto enorme para los comandos y dependencias militares, ya que sin este servicio no podrían recibir ningún correo militar o tener acceso al AUTOCOM, sin embargo, en el Data Center no daría problema, ya que en el servidor de correo se alojan todos los correos enviados y recibidos de todas las dependencias del Ejército de Guatemala. Este grado de dependencia es alto para los Comandos y bajo para el Comando de Informática y Tecnología.

1. **ANÁLISIS DE RIESGO:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **ACTIVO** | **AMENAZA** | **DESCRIPCIÓN** | **SALVAGUARDA** |
| 1 | Data Center zona 10 | Desastres Naturales y antropogénicos. | Rayos, tormenta eléctrica, ciclones, inundaciones, terremoto, fuego, etc. | Data center redundante, extintores tipo A, B y C, DRP. |
|  |  | Industriales | Sobrecarga eléctrica, fluctuaciones eléctricas | Reguladores, UPS, generador de energía alterno. |
|  |  | Contaminación mecánica (accidental o deliberado) | Vibraciones, polvo y suciedad | Mantenimiento preventivo, piso sustentado, control biométrico de ingreso. |
|  |  | Avería de origen físico o lógico | Fallos en los equipos, fallos en los programas, piratería. | Mantenimiento preventivo, actualizaciones de software constante, hardware actualizado, licenciamiento a toda herramienta lógica. |
|  |  | Condiciones inadecuadas de temperatura o humedad | Exceso de calor, frío o humedad. | Mantenimiento preventivo, equipo de medición de temperatura, equipos alternos de temperatura. |
|  |  | Fallo de servicios de comunicaciones | Destrucción física o lógica de cualquiera de los componentes del sistema de transmisión de datos | Enlace redundante, servidores espejos, control biométrico de acceso. |
| 2 | Correo Militar | Errores de uso | Equivocación de los usuarios y del administrador | Capacitaciones constantes para usuarios y administradores, directiva de correo militar, manuales actualizados |
|  |  | Difusión de software dañino | Virus, espías, gusanos, troyanos, malware. | Uso de antivirus, firewall, políticas de acceso a la red, equipo de correo alterno. |
|  |  | Error de secuencia | Alteración de los mensajes transmitidos | Servidor de encriptamiento y licencias de cifrado. |
|  |  | Reencaminamiento de mensajes | Envío de mensajes a un destino incorrecto | Capacitación y programación. |
|  |  | Interceptación de la información | Acceso a la información por personas no autorizadas | Cifrado de la información, VPN, doble factor de autenticación. |
|  |  | Avería de origen físico o lógico | Fallos en los equipos, fallos en los programas, piratería. | Mantenimiento preventivo, actualizaciones de software constante, hardware actualizado, licenciamiento a toda herramienta lógica. |
|  |  | Industriales | Sobrecarga eléctrica, fluctuaciones eléctricas | Reguladores, UPS, generador de energía alterno, DRP. |
| 3 | Correo Institucional | Errores de uso | Equivocación de los usuarios y del administrador | Capacitaciones constantes para usuarios y administradores, directiva de correo militar, manuales actualizados |
|  |  | Difusión de software dañino | Virus, espías, gusanos, troyanos, | Uso de antivirus, firewall, políticas de acceso a la red, equipo de correo alterno. |
|  |  | Error de secuencia | Alteración de los mensajes transmitidos | Servidor de encriptamiento y licencias de cifrado. |
|  |  | Reencaminamiento de mensajes | Envío de mensajes a un destino incorrecto | Capacitación y programación. |
|  |  | Interceptación de la información | Acceso a la información por personas no autorizadas | Cifrado de la información, doble factor de autenticación. |
|  |  | Avería de origen físico o lógico | Fallos en los equipos, fallos en los programas, piratería. | Mantenimiento preventivo, actualizaciones de software constante, hardware actualizado, licenciamiento a toda herramienta lógica. |
|  |  | Industriales | Sobrecarga eléctrica, fluctuaciones eléctricas | Reguladores, UPS, generador de energía alterno, DRP. |
| 4 | Enlaces de Datos e Internet | Avería de origen físico o lógico | Fallos en los equipos físicos, interrupción en la fibra óptica, malas configuraciones | Mantenimiento preventivo, actualizaciones de software constante, hardware actualizado, licenciamiento a toda herramienta lógica. |
|  |  | Difusión de software dañino | Virus, espías, gusanos, troyanos, malware. | Uso de antivirus, firewall, políticas de acceso a la red, equipo de correo alterno. |
|  |  | Interceptación de la información | Acceso a la información por personas no autorizadas | Cifrado de la información, VPN, doble factor de autenticación. |
|  |  | Industriales | Sobrecarga eléctrica, fluctuaciones eléctricas | Reguladores, UPS, generador de energía alterno, DRP. |
|  |  | Error de secuencia | Alteración de los mensajes transmitidos | Servidor de encriptamiento y licencias de cifrado. |
|  |  | Errores de uso | Equivocación de los usuarios y del administrador | Capacitaciones constantes para usuarios y administradores, manuales actualizados |
| 5 | Servidor de Base de Datos | Avería de origen físico o lógico | Fallos en los equipos físicos, corrupción de la base de datos | Mantenimiento preventivo, actualizaciones de software constante, hardware actualizado, licenciamiento a toda herramienta lógica.  Servidor de Respaldo |
|  |  | Industriales | Sobrecarga eléctrica, fluctuaciones eléctricas | Reguladores, UPS, generador de energía alterno, DRP. |
|  |  | Difusión de software dañino | Virus, espías, gusanos, troyanos, | Uso de antivirus, firewall, políticas de acceso a la red, equipo de correo alterno. |
|  |  | Errores de uso | Equivocación de los usuarios y del administrador, privilegios excesivos , exposición de los datos de back-up | Capacitaciones constantes para usuarios y administradores, manuales actualizados |
| 6 | AUTOCOM | Avería de origen físico o lógico | Fallos en los equipos físicos, corrupción de la base de datos | Mantenimiento preventivo, actualizaciones de software constante, hardware actualizado, licenciamiento a toda herramienta lógica.  Servidor de Respaldo |
|  |  | Industriales | Sobrecarga eléctrica, fluctuaciones eléctricas | Reguladores, UPS, generador de energía alterno, DRP. |
|  |  | Errores de uso | Equivocación del administrador, mal uso del usuario | Capacitaciones constantes para usuarios y administradores, manuales actualizados |
|  |  | Difusión de software dañino | Virus, espías, gusanos, troyanos, | Uso de antivirus, firewall, políticas de acceso a la red, equipo de correo alterno. |

1. **FASE 2. DETERMINACIÓN DE LA ESTRATEGIA DE CONTINUIDAD:**

Los procesos críticos del Comando de Informática y Tecnología, sus tiempos de recuperación y sus requisitos de pérdidas de datos, serán de acuerdo a la razón del ser de dicho Comando, siendo los siguientes:

Caída de Data Center: es el proceso critico que presenta la transferencia de todos los datos y comunicación, además es la misma que permite a todas las aplicaciones funcionar, entre ellas, correo militar, acceso a la base de datos, generación de nóminas de pago entre otros, por lo que representa para el CIT el proceso más crítico que puede ocurrir que hará que su funcionamiento sea el óptimo o adecuado.

La caída de la energía eléctrica, que no permitirá que el Data Center funcione correctamente.

Que ocurra un incidente dentro de las instalaciones donde se encuentra ubicado el Data Center que obstaculice el funcionamiento de los servidores correctamente, entre estos tenemos (incendio, inundación, etc).

El MTD (tiempo máximo tolerable de caída) es de 24 horas, tiempo en el que el Data Center puede permanecer caído antes de que se produzcan consecuencias para el Ejército de Guatemala. Debemos tener en cuenta que esta valoración será en la mayoría de los casos subjetiva, ya que incluso si podemos medir cuantitativamente el impacto de una contingencia (los usuarios de las diferentes Brigadas y Dependencias no podrán interactuar justo a tiempo o de una forma ligera, oportuna y confiable con los niveles de mando del Ejército de Guatemala, etc.), determinar en qué momento dicho impacto pone en riesgo la continuidad de labor que realiza el CIT es una tarea muy compleja.

El MTD está relacionado con el CIT, mientras que el RTO será determinado, por lo general, por personal usuario del servicio.

Si el MTD de nuestro proceso de correo son 24 horas y su RTO 12 horas, entonces:

Tardaremos 12 horas, con los recursos actuales, en poner en marcha de nuevo el proceso.

Si no recuperamos el proceso en 24 horas, el proceso puede dañar de manera irreversible la comunicación en el MDN y el acceso a la información solicitada por todas las aplicaciones que se interrelacionan o accedan al DATA CENTER del CIT.

Los niveles mínimos de recuperación de servicio o ROL son de 24 horas, aunque no se cuente con la rapidez que debería tener, entenderemos que la redundancia de la comunicación con todas las unidades del ejército ya fue reestablecida.

Aunque no siempre será posible determinar este valor, si nuestro proceso se basa por ejemplo en mantener los canales de comunicación entre todas las unidades del Ejército, podemos establecer un ROL en el 70%, tras lo cual consideraremos que el proceso está recuperado (lo que no implica que dejemos de aplicar las medidas de recuperación hasta el 100% que se logre la comunicación con todas las unidades del Ejército).

Si dentro del proceso intervienen proveedores externos, en función de la criticidad de las actividades en las que el proveedor esté implicado, dicho proveedor deberá disponer de un Plan de Recuperación ante Desastres y qué intervalos temporales maneja. El propósito es verificar que una situación de desastre en un proveedor crítico no traslada dicha contingencia al CIT.

Grado de dependencia de la actualidad de los datos o RPO (Recovery Point Objective) debe ser mínimo en cuanto a la pérdida de datos. Este valor es crítico a la hora de determinar las políticas de copias de la organización, y no guarda relación con el RTO visto anteriormente, para lo cual se tendrá un servidor que almacene toda esta información en otra instalación, para que sea levantado el sistema en el menor tiempo posible.

Es importante que todas nuestras actividades de contingencia se encaminen a obtener los siguientes datos:

Lo primero que debemos de recuperar es el Data Center, el TIEMPO MAXIMO RECUPERABLE DE CAIDA (MTD) es de 24 horas.

Lo segundo en la escala de prioridades o importancia es el Correo Militar, para reestablecer nuevamente las comunicaciones y los enlaces dentro del Ministerio de la Defensa Nacional.

1. **FASE 3. RESPUESTA A LA CONTINGENCIA:**
2. **PLAN DE CRISIS (O DE INCIDENTES):**

El plan de crisis o de incidentes se deberá elaborar en cada una de las dependencias militares, con el objetivo de actuar correctamente en una situación de crisis, evitando que se tomen decisiones improvisadas o que puedan empeorar la crisis; debiendo considerar los elementos siguientes:

1. Condiciones de disparo, es decir qué situación límite debe darse para que declaremos una situación de crisis.
2. Flujo de toma de decisiones.
3. Medios para la declaración de la situación de crisis.
4. Personal responsable para activar el plan de crisis y gestionarla.
5. Tener actualizado los teléfonos y datos de contacto, del personal implicado en la gestión de crisis.
6. Niveles de priorización en la recuperación de la infraestructura de la organización.
7. Requisitos temporales de tiempo en marcha.
8. Planes operativos existentes y personal responsable de su recuperación.

1. **PLANES OPERATIVOS DE RECUPERACIÓN DE ENTORNOS:**

Una vez contenido el momento inicial de la crisis, debemos realizar una evaluación del alcance de la crisis y determinar qué planes operativos de recuperación se deben activar. Estos documentos pueden abarcar uno o más entornos independientes y contienen información específica sobre el entorno al cual se aplican, este puede ser el Correo Militar, la aplicación de nóminas, el Sistema AUTOCOM.

1. **PROCEDIMIENTOS TÉCNICOS DE TRABAJO (O DE INCIDENTES):**

En esta situación se establece el procedimiento que describa la gestión y recuperación de toda aplicación en su entorno de sistema, para la continuidad diaria del proceso. Mantener los documentos que contengan la información específica para el incidente y procedimiento a seguir.

1. **FASE 4. PRUEBA, MANTENIMIENTO Y REVISIÓN:**
2. **PRUEBA:**

El plan de continuidad TIC, tiene como objeto, gestionar de manera óptima en tiempo y forma una situación de crisis no prevista, reduciendo así los tiempos de recuperación y vuelta a la normalidad. Por tanto, es imperativo que lo mantengamos actualizado en todo momento, que su vigencia sea comprobada regularmente. Para esto es necesario realizar diferentes pruebas en el entorno definido en el alcance, con diferentes grados de complejidad y elaboración. Entre todas las pruebas, debemos realizar pruebas de todos los entornos al menos una vez al año para cubrir el conjunto de amenazas que hemos definido como potencialmente catastróficas.

En la Ejecución de las pruebas, es necesario realizar a cabo una planificación previa que tenga en cuenta los diferentes aspectos:

1. Personal técnico
2. Usuario del aplicativo implicado en la prueba
3. Personal externo implicado en la prueba: Usuarios del correo y proveedores del servicio de internet.
4. Descripción de la prueba a realizar.
5. Descripción del resultado esperado tras las pruebas.
6. Hora y fecha de la realización; debemos tener en cuenta que siempre que la prueba pueda implicar una pérdida de servicio, sea ejecutada con éxito o no, debe planificarse este en un horario de mínimo impacto.
7. Tras la prueba deberá elaborarse un informe, que recoja los resultados y describa las posibles incidencias surgidas durante esta: Resultados no esperados, tiempo estimado superado, mala comunicación con el personal, indisponibilidad de proveedores, etc.

1. **PLAN DE MANTENIMIENTO:**

Tener actualizada la documentación de cada dependencia militar, siempre que exista una modificación en personal u otros. Se debe tener en cuenta que esta documentación debe mostrar la organización actual, de personal y de procesos críticos.

1. **PLAN DE PRUEBAS:**

Cualquier incidencia que se haya producido debe analizarse para la aplicación de las medidas correctivas que sean necesarias. Algunas posibles pruebas que pueden realizarse siempre teniendo en cuenta que estas dependen de la idiosincrasia de cada Comando o dependencia militar y que deben analizarse y planificarse cuidadosamente, siendo las siguientes:

1. Realizar la comprobación de que, ante la caída del suministro eléctrico, el sistema de alimentación ininterrumpida y el grupo electrógeno entra en funcionamiento.
2. Verificar los tiempos de recuperación de las posibles soluciones documentales de la organización en una máquina de pruebas. Los permisos de los usuarios deben ser los mismos que cada uno tenía antes de la recuperación.
3. Recuperación de las aplicaciones críticas del servicio (y los datos asociados) durante las pruebas.
4. Acceso remoto a la infraestructura desde una ubicación remota.
5. Si disponemos de entornos replicados debemos garantizar que ambos elementos pueden funcionar de manera independiente y que ante la caída de uno de ellos el otro dispositivo funciona correctamente.

1. **FASE 5. CONCIENCIACIÓN:**
2. **CONCIENCIACIÓN**:

El personal de la Compañía de Sistemas, será sometido a un proceso de concienciación en ciberseguridad que sirva para la formación, conocimiento, capacitación y buenas prácticas dentro del data center, por medio de un kit de concienciación, de la siguiente manera:

Diagrama

Descripción generada automáticamente

Se contará con un manual que contendrá información sobre los materiales y una programación para su distribución dentro de la Compañía de Sistemas.

1. **ATAQUES DIRIGIDOS:**

La conciencia iniciara con ejercicios para evaluar el nivel de concienciación en seguridad para despertar el interés del personal de oficiales y especialistas. Los ejercicios tomarán la forma de ataques sorpresa, a través de correos electrónicos, memorias USB.

1. **POSTERS:**

Se colocarán posters distribuidos en la Compañía de sistemas, con la finalidad de hacer conciencia sobre la seguridad para los oficiales y especialistas con los objetivos de transmitir aspectos importantes de seguridad relacionados al data center.

1. **PROCESO FORMATIVO:**

Se implementarán lecturas, conferencias, videos con la finalidad de dar a conocer conceptos, medidas y buenas prácticas necesarias para la ciberseguridad del Data Center.

1. **CONSEJOS DE SEGURIDAD MENSUALES:**

Tener visibles ficheros gráficos que contengan consejos temáticos para reforzar lo aprendido con las otras herramientas, pueden ser enviados también por correo electrónico, publicar en un blog interno o distribuirse en forma impresa.

Por último, se puede medir el aprendizaje a través de encuestas o lecciones aprendidas además de otro lanzamiento de un ataque como recordatorio.

Ciudad de Guatemala, 01 de Julio del 2022

Capitán Segundo de Infantería

Comandante de la compañía de sistemas del Btn. de TIC’S.

**WILDER GILBERTO CUM RAMÍREZ**