encuentro agesic 2018

CONTINUIDAD DE LA TRANSFORMACIÓN: aprendizaje permanente

Taller de Recuperación ante desastres

agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
República Oriental del Uruguay

Agenda

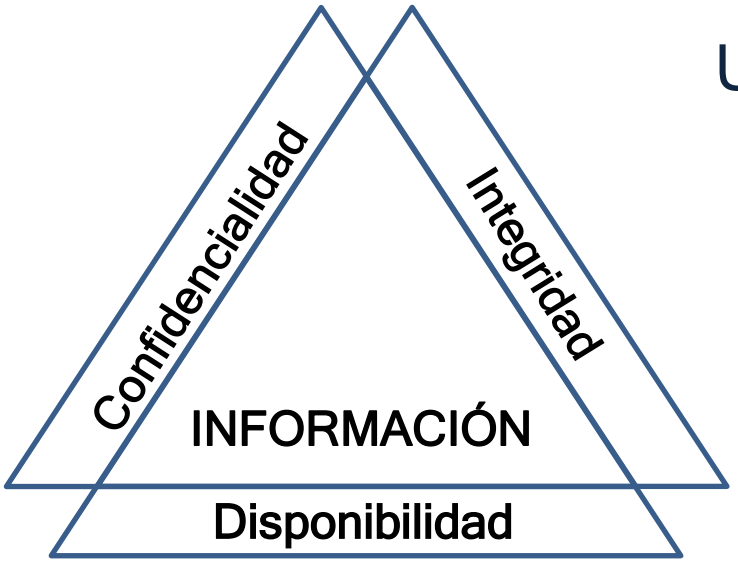
- Términos y abreviaciones
- Seguridad de la información
- Continuidad vs. Recuperación
- Medidas de continuidad
- Medidas de recuperación
- Caso de estudio
- Lecciones Aprendidas
- Criterios para desarrollar un DRP

Términos y abreviaciones

- **BIA** (Business Impact Analysis) – Análisis de impacto al negocio
- **BCP** (Business Continuity Plan) – Plan de continuidad del negocio
- **DRP** (Disaster Recovery Plan) – Plan de recuperación ante desastres
- **SLA** (Service Level Agreement) – Acuerdo de nivel de servicios

Seguridad de la información

- Preservación de la **confidencialidad**, **integridad**, y **disponibilidad** de la información.



UNIT-ISO/IEC 27000:2016

Continuidad vs. Recuperación

- Continuidad de la seguridad de la información: procesos y procedimientos para garantizar la continuidad de las operaciones de seguridad de la información.

  UNIT-ISO/IEC 27000:2016

- El foco de la recuperación ante desastres se orienta a la vuelta a condiciones estipuladas ante un incidente de seguridad de la información que afecte la provisión de los servicios en los niveles estipulados, principalmente enfocados a tecnología.

¿Cuáles son los principales problemas que identifican en sus organizaciones en aspectos de continuidad y recuperación de las operaciones?

Medidas de continuidad

- Política de Seguridad de la Información.
- Plan de continuidad de las operaciones (BCP).
- Sitios de trabajo alternativo (oficinas).
- Entre otras.

Medidas de recuperación

- Política de Seguridad de la Información.
- Plan de recuperación ante desastres (DRP).
- Respaldos de información.
- Sitios de procesamiento alternativo.
- Entre otras.

Caso de estudio

HACKEO DEL PORTAL INSTITUCIONAL

- Escenario de desastre que afecta la operativa habitual de la organización.
- ¿Qué harían en este caso?
- Considerar aspectos de imagen pública, contractuales, legales, regulatorios y técnicos.

Caso de estudio

Instrucciones:

- El caso consta de tres fases.
- Escuche atentamente las situaciones que se van a presentar en el caso.
- Tenga a su mano su dispositivo móvil para las fases I y II del caso.
- La fase III se realizará un ejercicio grupal.

Caso de estudio | Fase I

El Ministerio de Tecnología actualmente proporciona servicios a los usuarios de manera ágil y fácil por medio de su portal oficial. La infraestructura que soporta estos servicios se compone de un solo servidor físico con suficiente capacidad de procesamiento, memoria y almacenamiento de disco, para alojar todas las aplicaciones que el Ministerio ofrece a los usuarios. En este equipo se encuentran aplicaciones como: seguimiento de expedientes (trámites cuya disponibilidad es fundamental), contenido de difusión, agenda de eventos y noticias de interés.

El portal acaba de ser hackeado y el ataque produjo la destrucción del contenido oficial del Ministerio y sus aplicaciones, reemplazando la portada con una imagen de índole política acompañada de una proclama.

Caso de estudio | Fase I

Instrucciones:

- Conéctese a la red WIFI (agesic2018) con la clave (agesic2018).
- Ingrese a su dispositivo móvil a la siguiente dirección web: https://kahoot.it
- Espere que el moderador indique cual es el número de PIN en pantalla.
- Ingrese el numero PIN y escoja la ruleta para que le asigne un nombre.

Caso de estudio | Fase II

Los administradores no cuentan con acceso al servidor web, pues la contraseña de administración ha sido cambiada por el atacante (que obtuvo acceso de administrador) y tiene secuestrado el equipo. El personal de Tecnología evalúa solicitar asistencia a personal externo para solucionar la situación.

El Ministerio además está presente en redes sociales como Twitter y Facebook, cuyos perfiles están siendo sobrecargados con solicitudes de información y quejas de los usuarios, quienes manifiestan que es increíble que le ocurra esto al Ministerio de Tecnología.

Recientemente, el Ministerio de Tecnología, para dar cumplimiento a lo especificado en el decreto 92/014 y siguiendo los lineamientos del Marco de Ciberseguridad de AGESIC, ha contratado el servicio de colocación instalando servidores propios en uno de los centros de procesamiento de Antel. Los equipos que se instalaron en el centro de procesamiento alterno son equipos que anteriormente fueron usados en producción, por lo que no son idénticos ni cuentan con la capacidad de la infraestructura instalada en el ambiente de producción actual.

Caso de estudio | Fase II

Instrucciones:

- Conéctese a la red WIFI (agesic2018) con la clave (agesic2018).
- Ingrese a su dispositivo móvil a la siguiente dirección web: https://kahoot.it
- Espere que el moderador indique cual es el número de PIN en pantalla.
- Ingrese el numero PIN y escoja la ruleta para que le asigne un nombre.

Caso de estudio | Fase III

A las 15:00h el área de Tecnología informa que, según el análisis primario del CERTuy, la causa del ataque se debió a la explotación de una vulnerabilidad por falta de parches de seguridad del software base del servidor. Esto no solo generó que se comprometiera la administración y contenido del portal, sino que adicionalmente el atacante borró la base de datos, por lo cual ahora los datos son inaccesibles. Las autoridades han solicitado que el portal sea dado de baja y se restaure lo antes posible (menos de 4 horas), dado que se están recibiendo muchas consultas y exigencias desde organismos externos.

La recomendación del CERTuy es que el servidor sea desconectado de la red y no apagarlo, a fin de no perder las trazas de información que dejó el ataque. Dado que recientemente se pusieron en producción nuevos servicios que no estuvieron contemplados en la gestión de capacidad, el ministerio no cuenta con el suficiente espacio en disco para poder levantar un nuevo equipo en la infraestructura del centro de datos primario. Se le solicita al grupo que ordene las acciones o procedimiento para restablecer los servicios, debiendo considerarse las comunicaciones pertinentes para mantener informada a la ciudadanía y autoridades. Una estimación del área de Tecnología indica que la restauración de la base de datos y portal puede llevar al menos 3 horas. Este procedimiento nunca ha sido probado.

Caso de estudio | Fase III

Orden Sugerido: Equipo de Comunicación

- Establecer contacto con área de Tecnología para conocer cuáles serán las próximas acciones que se realizarán.
- Se le informa al personal del Ministerio que las autoridades han autorizado al área de Tecnología a realizar las acciones para restablecer los servicios en el centro de datos alterno.
- Se le solicita al personal que trabaja en el Ministerio que cuente con disponibilidad para ayudar en las acciones de verificación y prueba de los sistemas afectados una vez que estén restablecidos.
- Se genera un nuevo comunicado a la ciudadanía indicando que los servicios estarán disponibles en menor tiempo posible y se difunde por las redes sociales.
- En redes sociales se atienden preguntas y comentarios de los usuarios, dando respuestas generales a planteos repetitivos.
- Se promueven mensajes por las redes sociales donde se indique que se sigue trabajando en la solución del incidente. Se indica que se trabaja en forma conjunta con otros organismos para el restablecimiento de las funcionalidades que se ofrecen por el sitio web público del Ministerio.

Caso de estudio | Fase III

Orden Sugerido: Equipo de Tecnología

- El área de Tecnología comunica a las diferentes áreas, indicando que se realizarán los procedimientos para comenzar el cambio al centro de datos alterno y restaurar servicios.
- Se establece contacto con los encargados del centro de datos alterno donde se encuentra la solución de contingencia.
- Se solicitan los servicios de manos remotas para la asistencia con el despliegue de la solución de contingencia y la asignación de tarjetas de acceso al personal que está registrado en las listas de autorización para ingresar al centro alterno de datos.
- El área de Tecnología indica al proveedor que comience el levantamiento del respaldo para ganar tiempo, mientras que parte del equipo de tecnología se dirige al centro alterno de datos.
- Desde el área de Tecnología se le solicita al área de Comunicaciones que avise al personal que requerirá de su apoyo una vez que los servicios se restablezcan para probar los sistemas.
- Se contacta al CERTuy para la verificación y asistencia antes de volver a publicar el sitio web.

Lecciones Aprendidas

- No estar preparado es siempre el peor escenario
- La improvisación nunca debe ser la estrategia a seguir de cara a la recuperación
- La gestión de un incidente no es exclusivamente un problema tecnológico
- El compromiso de las autoridades debe estar formalizado

Lecciones Aprendidas

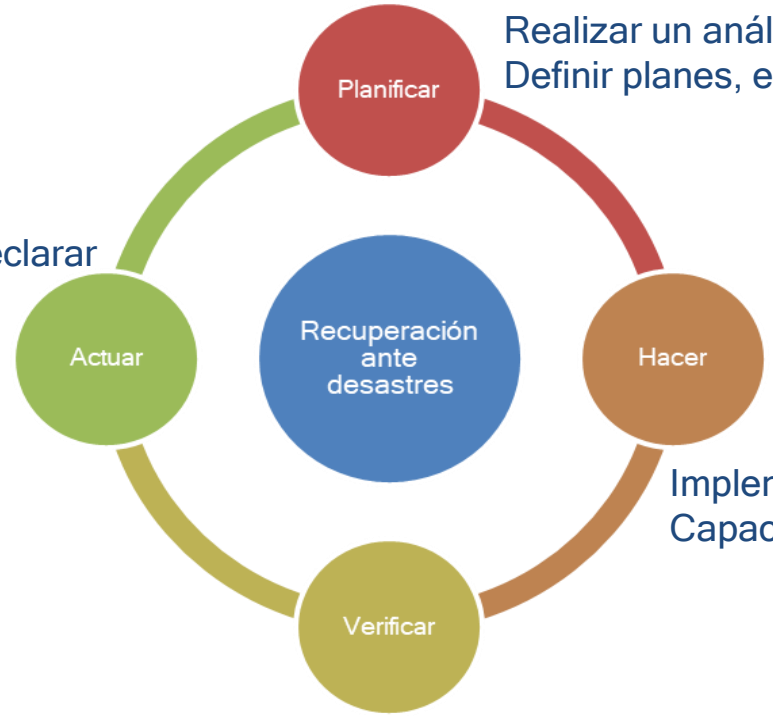
- Identificar los actores críticos
- Desarrollar pruebas sobre las estrategias
- Realizar revisiones o auditorías
- Incorporar un sistema de control de cambios
- La falta de monitoreo siempre es un grave error

Criterios para desarrollar un DRP

1. Generación de equipos y designación de responsable
2. Establecer análisis de riesgos
3. Definir la estrategia de recuperación
4. Formar los equipos de respuesta ante desastre
5. Pruebas del DRP

Criterios para desarrollar un DRP

Realizar un análisis de impacto (BIA)
Definir planes, equipos



Ante un incidente, decidir si declarar
Crisis Ejecutar la estrategia
Recuperar servicios críticos
Emitir comunicaciones

Implementar la estrategia
Capacitar al personal

Probar y actualizar la estrategia regularmente

encuentro agesic 2018

CONTINUIDAD DE LA TRANSFORMACIÓN: aprendizaje permanente

+info:

Centro de Recursos de Agesic

https://centroderecursos.agesic.gub.uy/

Contacto

seguridad.informacion@agesic.gub.uy

agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
República Oriental del Uruguay