Instituto Catastral y Registral del Estado de Sonora

"PLAN DE RECUPERACION DE DESASTRES"

Elaboró	Revisó	Autorizó
Ing. Javier Lagarda Antelo Jefe del Departamento de Base de Datos	**Ing. Víctor Manuel Verdugo Encinas** Jefe del Departamento de Seguridad y comunicaciones	**Ing. Víctor Hugo Rodríguez Rubio** Director General de Servicios Informáticos

Historia del Documento

Control de Cambios

Fecha de elaboración	Fecha de autorización	Versión	Elaboró	Naturaleza del cambio
1 de agosto de 2019		1.0	Javier Lagarda	Versión inicial

Revisado por

Área / Dirección	Persona
Director General de Sistemas Informáticos	Ing. Víctor Hugo Rodríguez

INTRODUCCION

Permitir restableces los servicios críticos de ICRESON y sistemas de información en case de desastres, identificar área de riesgo y la exposición a los desastres, ayudando a mitigar, contener, transferir o aceptar los riesgos en función de una escala definida en la tabla de riesgos la cual define los niveles bajo, medio y alto según el impacto generado.

I. PROPÓSITO

Reanudar con los servicios críticos en el menor tiempo posible y minimizar le impacto en la operación y servicios tecnológicos con los que cuenta ICRESON, garantizando la recuperación de los sistemas y procesos.

Evaluar los riesgos de los procedimientos de contingencia requeridos cuando se presenta una interrupción de las operaciones, de forma que solo se utilicen los recursos necesarios para restablecer el mínimo de los servicios.

Reducir el riesgo sobre la posibilidad de ocurrencia de incidentes de hardware y software, información o datos, entre otros.

II. FUNCIONES CRÍTICAS

Ante el incremento en el uso de las Tecnologías de la Información; surge la necesidad y responsabilidad de la protección de la infraestructura e información, medios de almacenamiento y ambientes de operación.

La información que se maneja en ICRESON, es de suma importancia, ya que alberga el inventario del suelo y la situación jurídica de los predios de todo el estado, es considerada como un active importante, y como tal, debe ser sujeta de custodia y protección para asegurar su integridad, confidencialidad y disponibilidad en todo momento.

La cantidad de datos guardados en los medios y equipos de almacenamiento se incrementa día con día y su integridad va relacionada con su pérdida o destrucción intencional o no intencional. Es por ello que, que los usuarios o personas directamente relacionadas con el uso y operación de los bienes informáticos, deben proponer la adopción de medidas de seguridad para proteger la información.

Con base en este plan, la Dirección General de Servicios Informáticos de ICRESON, deberá seguir los siguientes fines:

- Establecer mecanismos y procedimientos para proporcionar confidencialidad, integridad y disponibilidad de la información.
- Estimular la creación de una cultura de Seguridad de informática.
- Definir los requerimientos mínimos de seguridad de cada área, dependiendo del tipo de información que se procese: confidencial, restringida, de uso interno, general o pública, estableciendo los procedimientos para identificación y uso de cada categoría de información.

- Proveer el establecimiento de procedimientos alternos en previsión a contingencias de cualquier naturaleza que garanticen en la medida de lo posible, la continuidad del procesamiento de la información y la prestación de servicios, mismos que al incorporarse al presente documento lo irán enriqueciendo y de esta manera se logrará contar cada vez con una mejor herramienta que apoye a superar los posibles eventos que se pudieran presentar.

Funciones Críticas	Prioridad	Responsable
• Realizar un levantamiento de los servicios informáticos. • Mantener un inventario de equipo de cómputo, aplicaciones (sistemas), para determinar cuál es la información crítica que se tiene que resguardar . • Mantener un inventario de los servicios de cómputo, telecomunicaciones, internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades cotidianas.	1	Dirección General de Servicios Informáticos.
• Identificar un conjunto de amenazas. • Identificar los tipos de siniestros a los cuales esta propenso cada uno de los procesos críticos, tales como falla eléctrica prolongada, incendio, terremoto, etc. • Identificar el conjunto de amenazas que pudieran afectar a los procesos informáticos, ya sea por causa accidental o intencional.	2	Dirección General de Servicios Informáticos.
• Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados con respecto a las amenazas y vulnerabilidades identificadas.	3	Dirección General de Servicios Informáticos.
• Identificar los servicios fundamentales de ICRESON (factores críticos).	4	Dirección General de Servicios Informáticos.

III. FUNCIONES NORMATIVAS Y REFERENCIAS

FUNCIONES

Desarrollar e implementar sistemas computacionales que permitan realizar las operaciones catastrales, registrales y de administración del Impuesto predial de manera eficaz, fácil y segura. Sirviendo como un recurso experto a todos nuestros usuarios.

Facilitar y coordinar la implementación de proyectos de mantenimiento y desarrollo de software, para hacer más eficiente el acceso a la información, procesos y sistemas del Instituto Catastral y Registral del Estado de Sonora.

Controlar el acceso y Salvaguardar la información de las bases de datos y en general el acervo digital con el que cuenta el instituto.

IV. AMENAZAS

La identificación de amenazas se extraen como principales las siguientes:

- SISMO
- INCENDIO
- NEGLIGENCIA
- FALLAS DE ENERGIA ELECTRICA
- INUNDACIONES
- VIRUS Y ATAQUES INFORMATICOS

La operación de ICRESON pueden ser afectadas en menor o mayor medida por los distintos siniestros tanto naturales, accidentales o incidentales.

- **SISMO**

SIN PERDIDA O DAÑOS MENORES DEL EDIFICIO: EL siniestro puede afectar únicamente parte de la infraestructura del edificio, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera del inmueble, lo que provocaría en ICRESON una afectación que sería menor, puesto que las actividades se interrumpirían por unas horas o hasta por días completes.

CON PERDIDA DEL EDIFICIO: la pérdida de las instalaciones afectaría gravemente a las operaciones de ICRESON y los datos pueden verse seriamente dañados. Para tal efecto ICRESON consideraría un sitio alterno, este sitio debe estar preparado para tener una comunicación con el ambiente de producción y realizar una réplica de la información y de las aplicaciones más críticas. Ésta replica y el tiempo que tarde en hacerse, dependerá del tipo de enlace con que se trabaja y el tamaño de la información que se requiere.

En esta parte de la contingencia es en donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

- **INCENDIO**

Un incendio en el centro de datos es poco probable, sin embargo en caso de ocurrir, estos incendio son de desarrollo lento y de muy baja velocidad en la liberación del calor.

Sin embargo, un incendio y sobre todo la producción de humo dentro de una instalación de este tipo podrían ser catastróficos.

Se tiene gran impacto en la información ya que la información crítica reside en los servidores y dispositivos de comunicación ubicados en el Centro de Datos y en caso de sufrir algún daño, se requerirá adquirir un nuevo equipo, así como de instalar nuevamente el Sistema operativo en los equipos dañados, configurar los servidores y restaurar los respaldos para continuar trabajando, y en caso de ser necesario trasladarse al sitio alterno.

Un incendio dependiendo de su magnitud, puede afectar desde los servidores y dispositivos de comunicación localizados en el Centro de Datos e incluso la infraestructura del mismo.

- **NEGLIGENCIA**

El error humano siempre es latente, por lo que es necesario contar con mecanismos de respaldo de información y listos para reactivarse en caso de pérdida involuntaria de información, así mismo la capacitación constante del personal involucrado en las actividades de administración y mantenimiento de equipos y sistemas es de alta prioridad.

- **FALLAS DE ENERGIA ELECTRICA**

Los servidores necesitan de una fuente de alimentación eléctrica fiable para que funcionen adecuadamente, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias.

Las caídas, altas de tensión y los picos tienen un impacto negativo en todo tipo de aparato eléctrico, entre los que se incluyen los servidores, unidades de respaldo, monitores, etc. Y como consecuencia de ello posible pérdida en la integridad de la información.

Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolonga por tiempo indefinido se provocará un trastorno en las operaciones ya que esto impactaría en la pérdida de información y tiempos de proceso.

Para ello se cuenta con equipos de respaldo de energía eléctrica (UPS por sus siglas en inglés) los cuales proporcionan de forma directa la protección de los equipos servidores y de telecomunicaciones que operan en las instalaciones de ICRESON.

- **INUNDACION**

Un inundación en el Centro de Datos es poco probable, Sin embargo debido a que se tienen instalaciones sanitarias en pisos superiores al Centro de Datos, así mismo lluvias intensas por temporadas propias de la región, podría ocurrir un siniestro de este tipo que pudiera ser catastrófico.

Se tiene gran impacto en la información ya que la información crítica reside en los servidores y dispositivos de comunicación ubicados en el Centro de Datos y en caso de sufrir algún daño, se requerirá adquirir un nuevo equipo, así como de instalar nuevamente el Sistema operativo en los equipos dañados, configurar los servidores y restaurar los respaldos para continuar trabajando, y en caso de ser necesario trasladarse al sitio alterno.

Una inundación dependiendo de su magnitud, puede afectar desde los servidores y dispositivos de comunicación localizados en el Centro de Datos e incluso la infraestructura del mismo.

- **VIRUS Y ATAQUES INFORMÁTICOS**

Esta amenaza se vincula con la actividad humana, es decir, existe generalmente una finalidad específica (robo de información, robo de identidad, etc.) motivo por el cual también existe uno o varios autores intelectuales y se tipifica también como un delito. Bajo todos estos antecedentes es necesario contar con un buen Sistema de seguridad perimetral y de seguridad interna(Firewall y Antivirus por mencionar algunos), lo que hace necesario validar correctamente la correcta actualización de dicho software.

V. IMPLEMENTACIÓN

El plan debe ser mantenido en un alto nivel de preparación y debe estar listo para aplicaciones sin previo aviso. Asegurando que pueda activarse plenamente durante cualquier crisis o emergencia en la que las operaciones e información de ICRESON se vean amenazadas o no sean accesibles.

- Listado con nombre y cargo del personal clave y personal de apoyo que ejecutará las actividades del plan.

Nombre	Puesto
Ing Victor Hugo Rodriguez Rubio	Director General
Ing Javier Armando Lagarda Antelo	Servidores y BD
Ing Victor Manuel Verdugo Encinas	Infraestructura TI y REDES
Ing David Benitez Acuña	Mantenimiento y Soporte Técnico

Una situación de emergencia puede requerir la evaluación de las instalaciones de ICRESON con poco o ningún aviso previo. La evacuación del edificio, en caso necesario, se logra a través de la aplicación de Planes de Emergencia.

FASE I: ACTIVACION

El presente Plan de Recuperación se establece en el mes de Septiembre del 2018 como un documento de uso interno en la Dirección General de Servicios Informáticos de ICRESON.

Los desastres son eventos que pueden inhabilitar los servicios relacionados con las tecnologías de información, por lo que deben identificarse, analizar su nivel de riesgo y tomarse las medidas necesarias de prevención.

I. Alertamiento, Notificación y Puesta en Marcha

El alertamiento podrá darse por los medios cotidianos de protección civil o los mecanismos que para tal efecto se hayan destinado (alarmas audibles y/o visuales) o bien por la comunicación directa de cualquier persona perteneciente a ICRESON.

Para lo cual se buscará la forma inmediata de hacerlo del conocimiento del Director General de Servicios Informáticos o de quien en la línea de mando le suceda. Quién dará instrucciones o en su caso efectuará las tareas de contingencia descritas en este Plan de Recuperación de Desastres.

II. Proceso de toma de decisiones

Actividades vinculadas a la toma de decisiones de los responsables de la aplicación del Plan de Recuperación de Desastres.

Responsable	Actividades
Director General de Servicios Informáticos	• Analizar la gravedad de la contingencia y tomar acciones y coordinar las actividades que realizará el personal a su cargo. • Gestionar la compra emergente de equipos indispensables para la continuidad de operaciones. • Validar la disponibilidad del servidor alterno con el propósito de reiniciar operaciones. • Control y seguimiento del Plan de Recuperación de Desastres.
Servidores y BD	• Validar la disponibilidad de los respaldos de datos, programas, manuales y claves en el servidor alterno. • Una vez restaurada la información realizar pruebas de funcionalidad y de integridad de los datos. • Instalar aplicaciones y bases de datos actualizadas. • Restaurar la información de las bases de datos y/o programas.
Infraestructura TI y REDES	• Realizar las configuraciones necesarias para la interconexión de los equipos de manera local. • Verificar el restablecimiento de los enlaces WAN y VPNs

	hacia las oficinas remotas. • Restablecimiento de Active Directory
Mantenimiento y Soporte Técnico.	• Evaluar las condiciones operativas de los equipos una vez concluido y controlado el siniestro. • Proceder a tramitar la garantía de los equipos dañados y/o proporcionar las características técnicas para comprar los equipos indispensables para la continuidad de las operaciones.

III. Directorio de Emergencias.

La siguiente tabla presenta el directorio de emergencias para la activación del Plan.

	Nombre	Puesto	Teléfono
	Ing Victor Hugo Rodriguez Rubio	Director General	6621120629
	Ing Javier Armando Lagarda Antelo	Servidores y BD	6621414208
	Ing Victor Manuel Verdugo Encinas	Infraestructura TI y REDES	6621744096
	Ing David Benitez Acuña	Mantenimiento y Soporte Tecnico	6621387520

Nota: la información y orientación a los empleados suele ser trasmitida por la red de mensajes, correo electrónico o por teléfono. Dependiendo de la situación la información actual disponible también podrá difundirse a través de anuncios hechos por las autoridades locales, estaciones de radio y televisión.

IV. Ejecución

La ejecución del Plan se efectuará acorde a las actividades y responsabilidades mencionadas en el proceso de toma de decisiones, según el grado de afectación que se tenga derivado del siniestro experimentado.

Así mismo deberá considerar la recuperación de los sistemas prioritarios y su información, de tal forma que permitan la reanudación de la operación en los tiempos mínimos posibles, para ello a continuación se enlista los sistemas críticos.

BD RPP	Alto
Sistema de Gestión RPP (Escritorio y WEB)	Alto
Servidor de Aplicaciones (pase a caja, consultas de inscripciones, Servicios Web)	Alto
Pagina de Internet (Consultas en linea)	Medio
Directorio Activo	Alto

Imágenes digitalizadas (registro público)	Medio
BD CATASTRO	Alto
Sistema de Gestión Catastral	Alto
Imágenes digitalizadas(Catastro)	Medio
Cartografía	Alto

FASE II: OPERACION EN INSTALACIONES ALTERNAS

Derivado de la funcionalidad con la que cuenta el servidor alterno que permite su administración remota, no se considera específicamente necesario contar con una sede alterna y en virtud de que las aplicaciones se pueden configurar para que opera bajo un esquema de acceso via web, los usuarios también pueden hacer uso de ellas desde cualquier ubicación únicamente contando con equipo de cómputo con acceso a internet.

FASE III: RESTABLECIMIENTO DE OPERACIONES NORMALES

El restablecimiento de las operaciones normales comienza cuando la persona autorizada , comprueba que la situación de emergencia ha terminado y es poco probable que vuelva a surgir. Sin embargo, una vez que la Dirección General de servicios informáticos de ICRESON determina oficialmente que la situación de emergencia ha terminado; es menester de éste con apoyo de los proveedores correspondientes restablecer las operaciones normales.

Para ello y dependiendo de la situación, una de las siguientes opciones debe considerarse para el restablecimiento:

- Continuar con la operación alterna
- Comenzar un retorno ordenado a las instalaciones, restableciendo las funcionalidades operativas de los sitios restantes oficinas u otros recursos.

VI. PRUEBAS, ENTRENAMIENTO Y EJERCICIOS DEL PLAN

El entorno cambiante de las amenazas y los acontecimientos recientes hacen hincapié en la necesidad de que el plan se encuentre operando en amplio espectro de situación de emergencia. Las pruebas, entrenamiento y ejercicio del Plan incrementarán esta capacidad.

Para ello será necesario realizar eventos tipo simulacro que permitan garantizar su actualidad y funcionalidad. Así mismo se debe hacer del conocimiento de todos los integrantes de la Dirección General de Servicios Informático de ICRESON.

VII. ACTUALIZACIONES ANUALES DE LA ESTRATEGIA Y DEL PLAN

Este plan deberá revisarse de forma anual y en su caso actualizarse al entorno a los riesgos que sean identificados en su momento.

VIII. MANTENIMIENTO DEL PLAN

Describir los requerimientos esenciales y los recursos, a corto y largo plazo, las metas y los objetivos, las previsiones de necesidades presupuestales, anticipar y abordar las cuestiones y los obstáculos potenciales y la planeación, llevando un listado de las actividades necesarias para controlar la dinámica de los elementos y la ejecución del Plan.

Actividad	Tareas	Frecuencia de revisión
Actualización y Validación	• Incorporar las lecciones aprendidas y los cambios en la política y filosofía. • Difusión	Anual
Sucesión y Delegación de Autoridad	• Identificar a los actuales titulares. • Actualizar información de contacto.	Anual
Condiciones de sede alterna	• Supervisar todos los sistemas operables, • Verificar accesibilidad. • Verifique disponibilidad de suministros y equipos necesarios	Semestral
Bases de Datos, Archivos y documentación esencial	• Supervisar el volumen del material. • Actualizar/borrar archivos respaldo	Mensual