UNIDAD DE INFORMÁTICA

Manual de **Recuperación de Desastres Informáticos** (DRP)
Unidad de informática

Índice

I. Objetivo 3

II. Alcance 3

III. Introducción 4

IV. Ámbito de aplicación 5

V. Identificación, análisis de riesgos, evaluación de riesgos, y priorización de riesgos 5

V.1 Identificación de Riesgos y Análisis de Riesgos 5

VI.2 Evaluación y priorización de riesgos 11

VI. Recursos informáticos involucrados 13

VI.1 Servidor de aplicaciones: 13

VI.2 Sistemas informáticos alojados: 14

VI.3 Firewall: 14

VI.4 Personal encargado: 14

VII. Estrategias de Recuperación 15

VII. Procesos de recuperación 16

VII.1 Servidor de aplicaciones institucionales 16

VII.2 Seguridad Perimetral de la Red de Cómputo y Comunicaciones Digitales 19

VIII. Las pruebas y mantenimiento 22

IX. Acciones preventivas 23

I. Glosario 24

Proceso de escalación de reportes de fallas 25

I. Objetivo

Establecer los mecanismos y acciones a seguir dentro de un Plan de Recuperación de Desastres (DRP), a realizar por el personal técnico del Área de Informática del CELSH en el caso de que ocurra un desastre que implique una afectación total en la operatividad y funcionamiento de los sistemas y/o aplicaciones de carácter institucional, así como, a la seguridad perimetral de la Red y Comunicaciones Digitales que afecte los servicios de conectividad externa.

II. Alcance

El alcance de este documento contempla la reactivación y restablecimiento de los activos informáticos indicados en caso de:

- Daño total del servidor de aplicaciones institucionales.
- Daño total del perímetro de seguridad de la Red.

PODER LEGISLATIVO

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

III. Introducción

Las tareas del CELSH del Estado Libre y Soberano de Hidalgo se apoyan de manera sustantiva en las Tecnologías de la Información y Comunicaciones, lo cual convierte estos recursos en activos críticos en la realización de dichas tareas.

El presente documento presenta los procedimientos y acciones a desarrollar en el caso de que suceda alguna contingencia que cause un daño total en los activos informáticos más críticos, con el fin de minimizar las afectaciones a la operación e integridad de los sistemasy aplicaciones de carácter institucional.

Asimismo, este plan establece el proceso de restablecimiento de los servicios de conectividad externa como son Internet, Videoconferencias, etc.

Dichos procedimientos y acciones serán ejecutados por el personal técnico responsable del Área de Informática y deberán seguirse antes, durante y después de que suceda alguna contingencia de este tipo.

Este plan se enfoca en el restablecimiento total del servidor de sistemas y aplicaciones institucionales en caso de un daño que deje inoperable el equipo servidor o que suceda un daño parcial o total al disco duro que aloja todos los datos de los sistemas informáticos alojados en este equipo.

También contempla el restablecimiento y operatividad del perímetro de seguridad de la red y comunicaciones digitales (servicios de conectividad local, externa y de acceso a Internet).

De antemano se cuenta con un procedimiento rutinario de respaldo total del Servidor de aplicaciones, lo cual permite tener la posibilidad de restablecer el servidor por completo.

Por otro lado, se cuenta con una póliza de mantenimiento del equipo firewall FG-1000D de Fortinet que incluye licenciamiento y soporte técnico.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

IV. Ámbito de aplicación

Este DRP informático va dirigido a la siguiente audiencia:

a) **Legisladores:** Los miembros del cuerpo legislativo, como diputados o senadores, son parte fundamental de la audiencia del DRP. Ellos deben estar informados y capacitados sobre las medidas de contingencia establecidas para hacer frente a desastres informáticos y cómo podrían afectar el funcionamiento del Poder Legislativo.

b) **Personal legislativo:** El personal encargado de la operación del poder legislativo también es una parte importante de la audiencia del DRP. Deben de estar informados sobre los protocolos y procedimientos a seguir en caso de un desastre informático, así como capacitados en las mejores prácticas de seguridad cibernética.

c) **Proveedores de servicios de infraestructura electrónica:** Es importante que estén al tanto de las medidas de contingencia establecidas y de sus roles y responsabilidades en caso de un desastre informático.

d) **Otros actores relevantes:** Incluye representantes de otras instituciones gubernamentales y ciudadanos.

V. Identificación, análisis de riesgos, evaluación de riesgos, y priorización de riesgos

El poder legislativo recopila y almacena una gran cantidad de datos confidenciales: legislativos, información financiera y datos personales. La pérdida de estos datos podría tener un impacto significativo en la capacidad del poder legislativo para llevar a cabo sus funciones.

V.1 Identificación de Riesgos y Análisis de Riesgos

Los riesgos identificados se clasifican en externos e internos.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

Riesgos Externos:

1) **Desastres naturales:** Los desastres naturales, como los incendios, las inundaciones y los terremotos, pueden causar daños físicos a la infraestructura informática.

   - **Desastres meteorológicos:** Los desastres meteorológicos son los más comunes y pueden causar una amplia gama de daños, desde inundaciones y tornados hasta huracanes y terremotos.

   - **Desastres geológicos:** Los desastres geológicos son causados por fenómenos naturales que ocurren debajo de la superficie de la Tierra, como terremotos, erupciones volcánicas e inundaciones repentinas.

   - **Desastres biológicos:** Los desastres biológicos son causados por agentes biológicos, como virus, bacterias y hongos. Estos agentes pueden causar enfermedades graves o incluso la muerte.

2) **Fallas de infraestructura:** Las fallas de infraestructura en luz e internet pueden interrumpir el funcionamiento de los sistemas informáticos.

   Fallas de luz.

   a) **Interrupción de actividades:** Una falla de luz puede causar una interrupción inmediata de las actividades legislativas. Las sesiones, reuniones y debates pueden suspenderse temporalmente, lo que puede afectar la productividad y retrasar la toma de decisiones.
   b) **Pérdida de datos:** Información importante relacionada con proyectos de ley, informes, votos y otros documentos legislativos. La pérdida de estos datos puede afectar la eficiencia y la transparencia del Poder Legislativo.
   c) **Problemas de seguridad:** Las fallas de luz pueden crear brechas en la seguridad física y digital.

   Fallas de Internet

   a) **Limitaciones en la comunicación:** Los legisladores y el personal legislativo pueden tener dificultades para comunicarse entre sí, lo que puede afectar la coordinación de actividades y la toma de decisiones. Además, la falta de acceso a internet puede dificultar la comunicación con el público, otras instituciones gubernamentales, organizaciones y otros actores relevantes.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

b) **Retraso en el acceso a información:** Limitar el acceso a documentos legislativos, datos estadísticos, informes, estudios y otras fuentes de información que son necesarias para llevar a cabo investigaciones y tomar decisiones informadas.

c) **Limitaciones en la participación ciudadana:** Dificultar la participación ciudadana en consultas, audiencias públicas virtuales, presentación de propuestas y expresión de opiniones sobre temas legislativos. Esto puede generar una falta de inclusión y representatividad en la toma de decisiones.

3) **Ataques cibernéticos:** Los ataques cibernéticos, como los ataques de denegación de servicio (DDoS) o los ataques de ransomware, pueden comprometer la seguridad de los sistemas informáticos.

- **Acceso no autorizado a información confidencial:** un ataque cibernético podría permitir que los atacantes accedan a información confidencial y sensible, como registros legales, datos personales de litigantes, pruebas, decisiones judiciales, entre otros. Esto podría comprometer la confidencialidad y la privacidad de las partes involucradas en los casos judiciales, generar un riesgo de robo de identidad o de extorsión.

- **Manipulación de registros y evidencias:** los atacantes podrían manipular registros judiciales y evidencias digitales, lo que podría conducir a decisiones judiciales erróneas o injustas. Esta alteración de pruebas o registros podría socavar la confiabilidad y la integridad del sistema judicial.

- **Interrupción de servicios:** un ataque cibernético sofisticado podría paralizar los sistemas informáticos del CELSH, lo que afectaría la prestación de servicios. Esto podría resultar en la suspensión o retraso en los sistemas institucionales, red inalámbrica y correo institucional principalmente.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

Riesgos Internos

4) **No poder realizar votaciones electrónicas:** La interrupción de los sistemas informáticos podría dificultar al poder legislativo realizar votaciones en sistema de votación biométrico, originando que el panel histórico de resultados, no sea exacto en tiempo real conteniendo la cantidad de votos a favor, en contra, abstinencia, ausentes, fecha y hora del cierre de votaciones.

5) **Falta de acceso a la información electrónica:** La interrupción de los sistemas informáticos podría dificultar al poder legislativo acceder a la información necesaria para tomar decisiones en las siguientes dimensiones:

- **Legislación:** Puede analizar y utilizar datos electrónicos para tomar decisiones sobre la creación, reforma o derogación de leyes y reglamentos. Estos datos pueden incluir estadísticas, informes técnicos, estudios de impacto, resultados de consultas ciudadanas, entre otros.

- **Investigaciones y análisis legislativo:** El CELSH puede utilizar datos electrónicos para realizar investigaciones y análisis sobre temas específicos, que sirvan como base para la toma de decisiones. Estos datos pueden incluir informes de expertos, estudios académicos, estadísticas, entre otros.

- **Presupuesto:** El CELSH puede utilizar datos electrónicos para tomar decisiones relacionadas con la asignación de recursos y elaboración del presupuesto estatal. Estos datos pueden incluir información sobre ingresos, gastos, deudas, programas y proyectos gubernamentales, entre otros.

- **Políticas públicas:** El CELSH puede utilizar datos electrónicos para tomar decisiones relacionadas con la implementación de políticas públicas. Estos datos pueden incluir estudios demográficos, análisis de necesidades sociales, resultados de evaluaciones de programas, entre otros.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

6) **Fallas de comunicación:** La interrupción de los sistemas informáticos podría dificultar al poder legislativo comunicarse con el público y con otras partes interesadas.

- **Sitio web institucional:** El CELSH del Estado de Hidalgo tiene su propio sitio web donde se publica información sobre legislación, sesiones, comisiones, diputados, noticias y eventos. Este sitio web proporciona un medio para que el público acceda a información legislativa y se comunique con el CELSH a través de formularios de contacto.

- **Redes sociales:** el CELSH está presente en diferentes redes sociales, como Facebook, Twitter, Instagram y YouTube. A través de estas plataformas, el CELSH comparte información legislativa, noticias, eventos y responde a consultas y comentarios de los ciudadanos.

- **Correo electrónico y formularios en línea:** el CELSH puede recibir comunicaciones y consultas a través de correo electrónico y formularios en línea disponibles en su sitio web. Estos canales permiten a los ciudadanos y otras partes interesadas enviar mensajes o hacer preguntas directamente al CELSH.

- **Transmisiones en vivo y archivos de sesiones:** El CELSH transmite en vivo las sesiones legislativas a través de su sitio web y redes sociales. Además, proporciona acceso a archivos de sesiones anteriores que se pueden consultar en línea. Esto permite al público mantenerse informado sobre el trabajo legislativo y acceder a las discusiones que se han llevado a cabo.

- **Boletines legislativos:** el CELSH puede enviar boletines legislativos por correo electrónico, publicarlos en su sitio web o en las distintas redes sociales oficiales. Estos boletines contienen información sobre proyectos de ley, eventos, actividades legislativas y otro tipo de actualizaciones relevantes para el público en general.

7) **Daño a la Imagen institucional:** El poder legislativo tiene la responsabilidad de proteger la seguridad de los datos y la privacidad de los ciudadanos. La reputación del poder legislativo podría verse dañada si se produjera un desastre informático que provocara la pérdida de datos o la interrupción de las operaciones.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

- **Pérdida de datos:** Un desastre informático, como un ciberataque o una falla de hardware, puede resultar en la pérdida de datos importantes y confidenciales. Esto puede tener un impacto negativo en la reputación del CELSH, ya que muestra una falta de seguridad y protección de la información.

- **Divulgación de información sensible:** Si ocurre un desastre informático, es posible que se vea comprometida la información sensible o confidencial del CELSH la organización, como datos personales de los ciudadanos o deliberaciones internas. Esto podría afectar la confianza del público y la percepción de que no está protegiendo adecuadamente los datos institucionales.

- **Interrupción de servicios:** Un desastre informático puede provocar la interrupción de servicios electrónicos clave, como la transmisión en vivo de sesiones, la comunicación con el público a través de canales electrónicos o la publicación de documentos legislativos. Esta interrupción en la prestación de servicios puede generar frustración y descontento entre los ciudadanos y otras partes interesadas, lo que puede afectar negativamente la reputación del CELSH.

- **Difusión de noticias falsas:** En el contexto de un desastre informático, es posible que se generen noticias falsas o desinformación que afecten la reputación del CELSH. Esto podría suceder si los atacantes difunden información falsa a través de los canales oficiales del CELSH o si los medios de comunicación malinterpretan o informan de manera inexacta sobre el incidente.

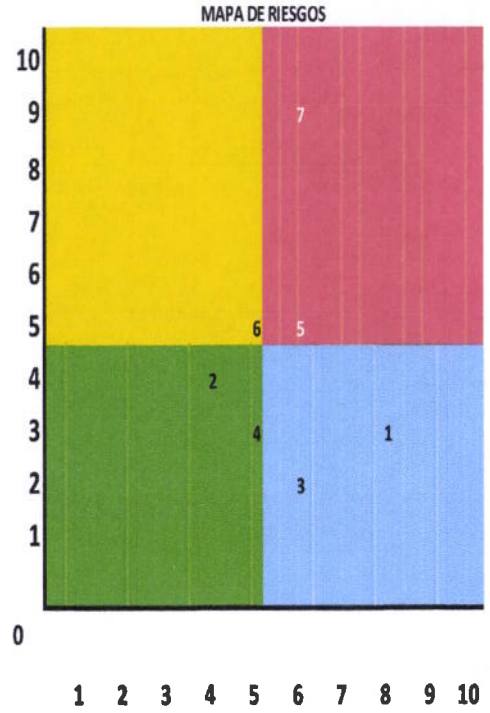
- **Falta de respuesta adecuada:** La manera en que el CELSH responda a un desastre informático también puede afectar su reputación. Si no se toman medidas rápidas y efectivas para mitigar el impacto del incidente, comunicar de manera transparente con el público y tomar medidas para evitar futuros incidentes, esto podría generar desconfianza y dañar la imagen del CELSH.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.

www.congreso-hidalgo.gob.mx
(771) 71.744.00

VI.2 Evaluación y priorización de riesgos

NO. RIESGO	DESCRIPCIÓN DEL RIESGO	IMPACTO	OCURRENCIA	Cuadrante	
1	Desastres naturales	8	3	SEGUIMIENTO	III
2	Fallas de infraestructura	4	4	CONTROLADO	IV
3	Ataques cibernéticos	6	2	SEGUIMIENTO	III
4	No poder realizar votaciones electrónicas	5	3	CONTROLADO	III
5	Falta de acceso a la información electrónica	6	5	CRITICO	I
6	Fallas de comunicación	5	5	PERIODICO	III
7	Daño a la reputación	9	6	CRITICO	I



Metodología de ejecución localización

El presente DRP será ejecutado dentro de las instalaciones del CELSH, ubicado en Carretera México-Pachuca Km. 84.5 S/N, Col. Carlos Rovirosa, Pachuca de Soto, Hidalgo. Tel. 7717174400

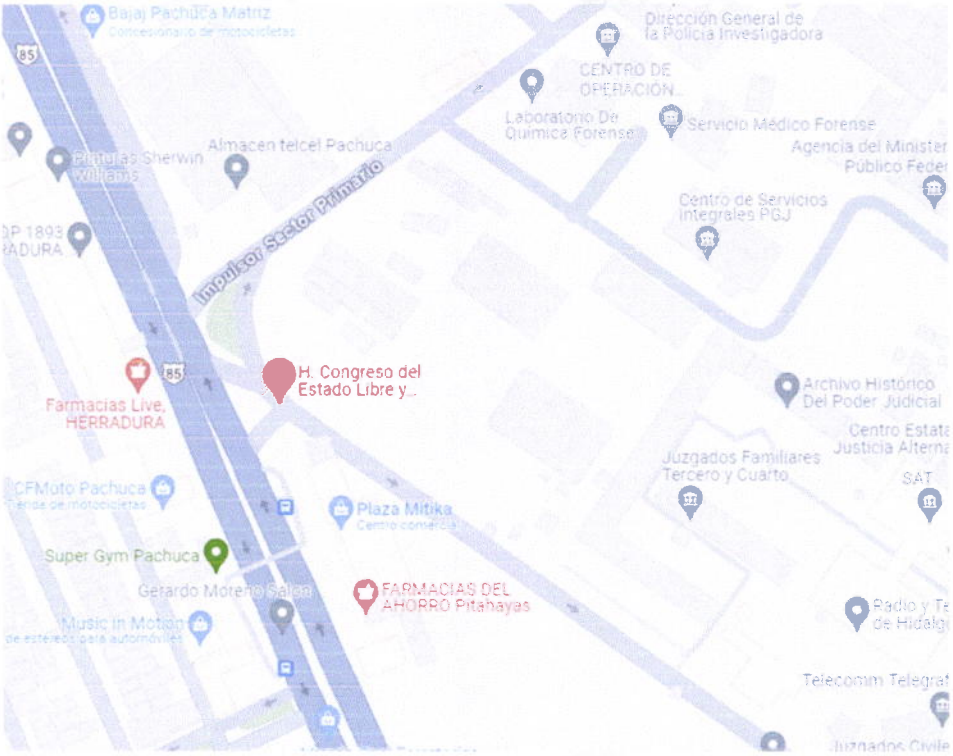


Figura 1. Ubicación del CELSH.

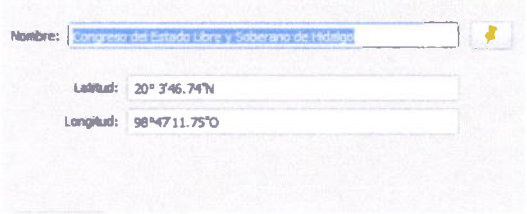


Figura 2. Coordenadas de ubicación del CELSH.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

VI. Recursos informáticos involucrados

En este apartado nos enfocaremos en los recursos involucrados en el DRP, elementos indispensables para garantizar la pronta recuperación y continuidad de los sistemas informáticos. Uno de los componentes clave es el servidor de aplicaciones, en este caso, un potente servidor HP DL-160 Gen 9, equipado con un procesador Intel Xeon y una amplia capacidad de memoria y almacenamiento. Este servidor, con su sistema operativo Windows Server 2012 R2 Standard, permite alojar y ejecutar diversos sistemas y aplicaciones.

Entre los sistemas informáticos alojados en este servidor, encontramos una amplia gama de funciones vitales para el funcionamiento de una organización. Desde la página web oficial del CELSH (**www.congreso-hidalgo.gob.mx**) hasta sistemas de resguardos, inventarios, coffee break, votaciones, archivo, planeación, turnos, parque vehicular, declaración patrimonial y nómina integral. Todos estos sistemas, con sus respectivas funciones y bases de datos, deben ser protegidos y recuperados en caso de un desastre informático.

Para asegurar la seguridad de la red y de los sistemas informáticos, se cuenta con un firewall Fortigate 1000D Fortinet, una solución de seguridad de alto rendimiento. Este firewall se encarga de proteger la infraestructura tecnológica de posibles amenazas externas y ataques cibernéticos.

Por último, pero no menos importante, el personal encargado desempeña un papel crucial en el éxito del DRP. Este equipo de profesionales capacitados y responsables se encargará de implementar y mantener el DRP, así como de ejecutar las acciones necesarias en caso de una situación de emergencia.

VI.1 Servidor de aplicaciones:

- Servidor HP DL-160 Gen 9.
- Procesador Intel Xeon E5-2603 v3 @ 1.60 Ghz.
- 64 Gb de memoria RAM.
- Disco duro de 1 TB.
- Sistema operativo Windows Server 2012 R2 Standard.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

VI.2 Sistemas informáticos alojados:

- Página web oficial: **www.congreso-hidalgo.gob.mx**
- Sistema de resguardos.
- Sistema de inventarios.
- Sistema de coffee break.
- Sistema de votaciones.
- Sistema de archivo.
- Sistema de planeación.
- Sistema de turnos.
- Sistema de parque vehicular.
- Sistema de declaración patrimonial.
- Sistema de nómina integral (NOI).

VI.3 Firewall:

- Fortigate 1000D Fortinet.

VI.4 Personal encargado:

- **Ernesto Armando Sánchez López**; director de la Unidad de Informática.
  - Ext. 1502
  - Correo electrónico: informatica@CELSH-hidalgo.gob.mx

- **Juan Ramón Dimas**; encargado de la red y comunicaciones digitales.
  - Ext. 1503
  - Correo electrónico: redes@CELSH-hidalgo.gob.mx

VII. Estrategias de Recuperación

Servidor de Aplicaciones Institucionales

- Incidente menor o parcial:

- Se realiza un diagnóstico del problema y se corrige la causa.
- Se restaura la aplicación o el sistema afectado a partir de la última copia de seguridad.

- Incidente mayor:

- Se reemplaza el servidor o el componente dañado.
- Se restaura el servidor o el componente dañado a partir de la última copia de seguridad.

Seguridad Perimetral de la Red de Cómputo y Comunicaciones Digitales

- Incidente menor o parcial:

- Se realiza un diagnóstico del problema y se corrige la causa.
- Se restaura la configuración del Firewall a partir de la última copia de seguridad.

- Incidente mayor:

- Se solicita al proveedor un equipo de reemplazo.
- Se instala la última configuración respaldada en el nuevo equipo.

En ambos casos, las estrategias de recuperación se basan en la restauración de los datos y sistemas afectados a partir de copias de seguridad. Esto permite que la organización pueda reanudar sus operaciones lo antes posible.

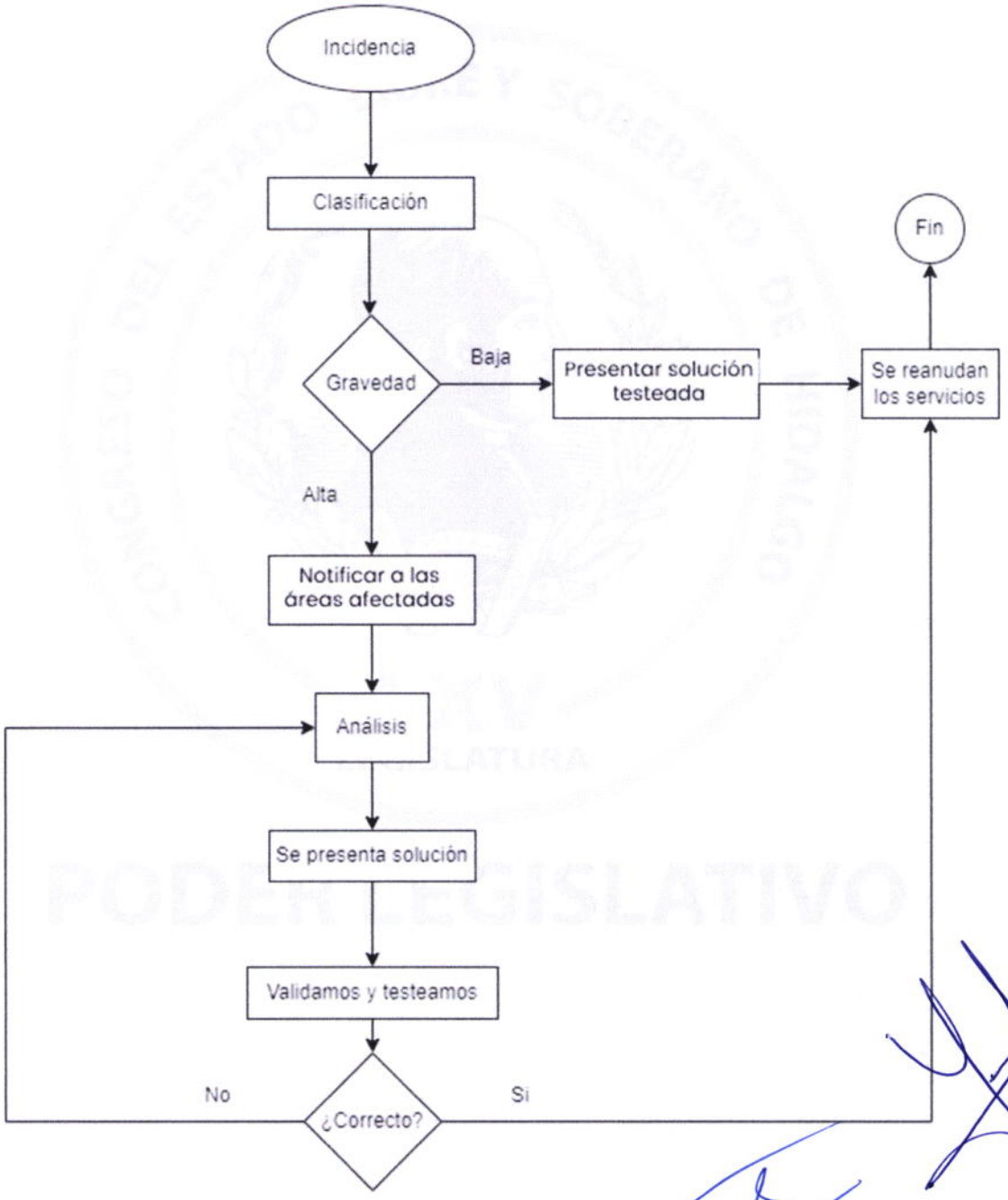
PODER LEGISLATIVO

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.

www.congreso-hidalgo.gob.mx
(771) 71.744.00

VII. Procesos de recuperación

VII.1 Servidor de aplicaciones institucionales



Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

Descripción

1. **Incidencia:** Se considera un incidente a un suceso que provoca una falla en el servidor de aplicaciones institucionales y que impide su correcta operación. Este suceso provoca que las aplicaciones informáticas del CELSH no puedan serutilizadas.

2. **Clasificación:** se realiza con el objetivo de dar la respuesta prioritaria.

3. **Gravedad.** Una vez que se ha recibido la notificación, el personal responsable analiza el problema y determina el tipo y criticidad del incidente:

    a. **Baja:** Este tipo de incidente sucede cuando:
        I. Se presenta una falla en uno o varias aplicaciones, pero el servidorse encuentra operable.
        II. Hay una falla en el suministro eléctrico sin daño al servidor.
        III. Hay un problema de conectividad sin representar un daño delservidor.
        IV. Una infección de virus.
        V. Una afectación al sistema operativo que sea posible corregir que norepresente una falla total del servidor.

    b. **Alta:** Este tipo de incidente se refiere a:
        I. Un daño a cualquier componente físico o lógico que deje inoperablee inutilizable al servidor.
        II. Un daño a la integridad del Disco Duro que no represente un dañofísico del servidor pero que impida su operatividad.

4. **Notificar a las Áreas Afectadas:** Una vez diagnosticado el problema y las medidas de solución, se notifica a las áreas afectadas para establecer un tiempo estimado de recuperación y el alcance de los daños.

5. **Análisis de la Falla:** Se realiza una revisión exhaustiva del problema que se presenta en el servidor para poder determinar la causa del fallo y establecer las medidas correctivas adecuadas.

6. **Iniciar acciones de recuperación:** De acuerdo a las casusas del fallo se inician las acciones de recuperación que pueden ser:

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

a. **Reemplazo del equipo servidor:** En el caso de un daño físico del servidor que sea irreparable se deberá reemplazar el equipo servidor y se deberá iniciar la recuperación del sistema total del servidor a partir del último respaldo inmediato realizado en el caso de que el disco duro haya sido afectado en su integridad física y lógica.

b. **Reemplazo del o los componentes dañados:** En el caso de que uno o más componentes del servidor presenten daño, que no sea el disco duro, se deberán reemplazar y una vez corregida la falla se debe proceder a su restablecimiento.

c. **Daño parcial o total del disco duro:** En el caso de que la falla se presente en el disco duro, se deberá reemplazar e iniciar el proceso de recuperación a partir del último respaldo inmediato realizado.

7. **Restablecer operación de sistemas y aplicaciones Institucionales:** Una vez que se ha restablecido la operación del servidor se debe establecer la operación de los sistemas y aplicaciones a partir de la recuperación realizada.

8. **Validar Integridad de sistemas y aplicaciones institucionales:** Se debe validar con cada área usuaria involucrada la integridad de la información y operatividad de los sistemas y aplicaciones en el servidor.

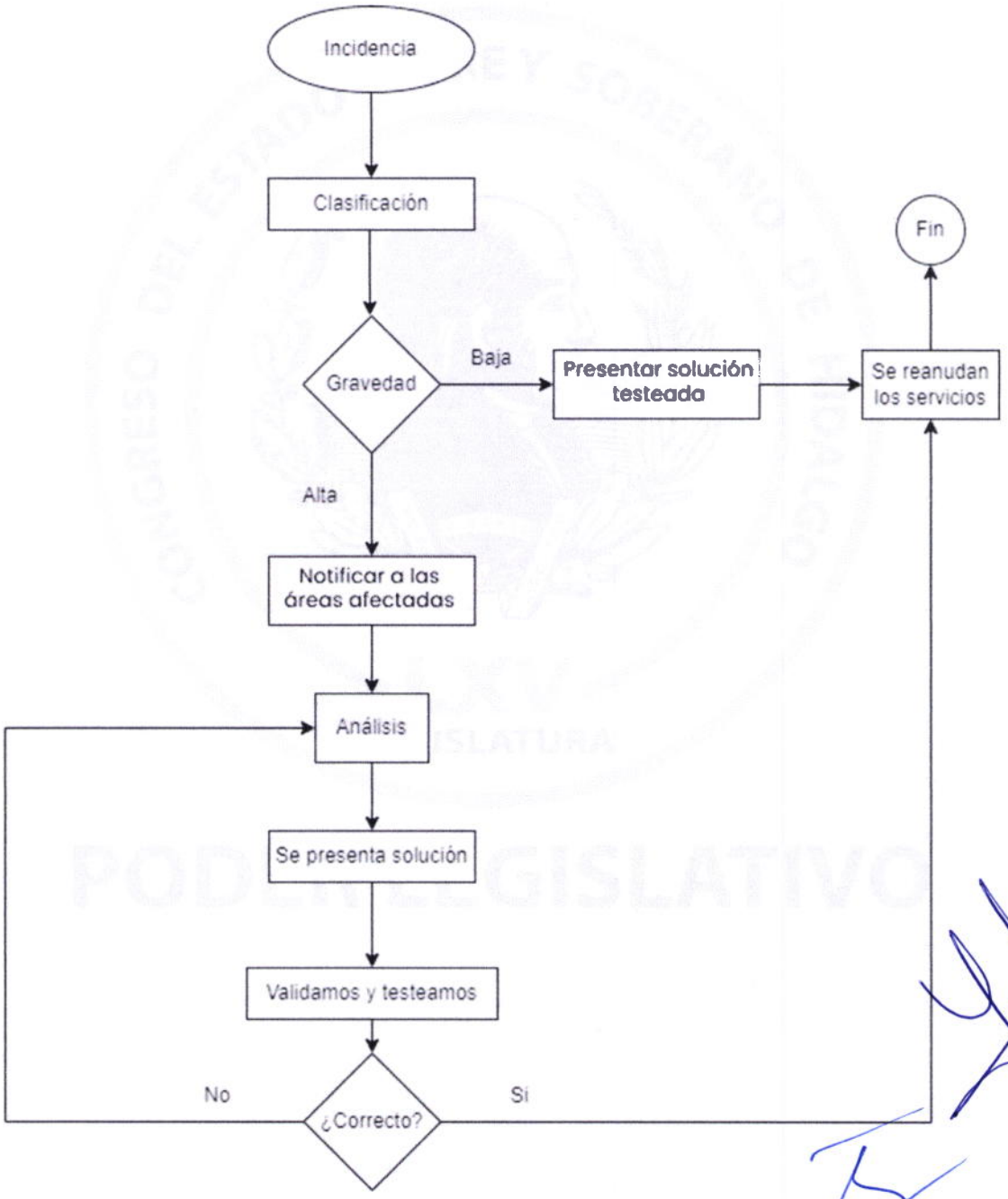
9. **Restablecimiento correcto:** Si el restablecimiento de los sistemas y el servidor se ha realizado con éxito se puede proceder a dar acceso a los usuarios para poder reanudar sus actividades en el uso de los sistemas y aplicaciones. En caso contrario se debe proceder nuevamente a partir del punto 4.

10. **Reanudar servicio a los usuarios:** Una vez validada la operatividad y funcionalidad del servidor, sistemas y aplicaciones se debe dar acceso nuevamente a los usuarios para que reanuden sus actividades normales.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.

www.congreso-hidalgo.gob.mx
(771) 71.744.00

VII.2 Seguridad Perimetral de la Red de Cómputo y Comunicaciones Digitales



Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.

www.congreso-hidalgo.gob.mx
(771) 71.744.00

Descripción

1. **Incidencia:** Se considera un incidente a un suceso que provoca una falla en la conectividad perimetral de la Red de Cómputo y Comunicaciones Digitales del CELSH.

2. **Clasificación:** se realiza con el objetivo de dar la respuesta prioritaria.

3. **Gravedad.** Una vez que se ha recibido la notificación, el personal responsable analiza el problema y determina el tipo y criticidad del incidente:

    a. **Baja.** Este tipo de incidente sucede cuando:
        I. Se presenta una falla en uno o más usuarios que no pueden acceder a servicios de información externos como páginas WEB, servicios Online, servicios electrónicos de Información, etc.
        II. Hay una falla en el suministro eléctrico sin daño al Firewall.
        III. Hay un problema de conectividad sin representar un daño del Firewall.
        IV. Una falla en la operación del Firewall por saturación de memoria, disco o CPU.
        V. Una falla de los servicios de conectividad aplicable al proveedor del servicio.

    b. **Alta.** Este tipo de incidente se refiere a un daño a cualquier componente físico o lógico que deje inoperable e inutilizable al Firewall.

4. **Análisis de la Falla.** Se realiza una revisión exhaustiva del problema que se presenta en el Firewall para poder determinar la causa del fallo y establecer las medidas correctivas adecuadas.

5. **Notificar a las Áreas Afectadas.** Una vez diagnosticado el problema y las medidas de solución, se notifica a las áreas afectadas para establecer un tiempo estimado de recuperación y el alcance de los daños.

6. **Iniciar acciones de recuperación.** De acuerdo a la póliza Forticare y RMA contratada se procede a solicitar al proveedor:

Plaza Cívica Miguel Hidalgo, "Centro Cívico", Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa, C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

a. Préstamo de un equipo de acuerdo al RMA para restablecimiento inmediato de los servicios y restauración de la última versión de la configuración respaldada.

7. **Restablecer Servicios de Conectividad.** Una vez que se ha reemplazado o reparado el Firewall se procede a instalar la última versión de la configuración respaldada y restablecimiento de los servicios de conectividad externa.

8. **Validar Servicios de Conectividad.** Se debe validar la funcionalidad de las políticasy reglas de seguridad y permisos establecidos en el Firewall antes del fallo.

9. **Restablecimiento correcto.** Si el restablecimiento de los servicios se ha realizado con éxito, se puede proceder a dar acceso a los usuarios para poder reanudar sus actividades. En el caso contrario se debe proceder nuevamente a partir del punto 4.

10. **Reanudar servicio a los usuarios.** Una vez validada la operatividad y funcionalidad del Firewall y los servicios se debe dar acceso nuevamente a los usuarios para que reanuden sus actividades normales.

PODER LEGISLATIVO

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.

www.congreso-hidalgo.gob.mx
(771) 71.744.00

VIII. Las pruebas y mantenimiento

Deben cubrir las siguientes áreas:

- **La eficacia de las estrategias de recuperación**. Las pruebas deben garantizar que las estrategias de recuperación descritas en el DRP sean efectivas para restaurar los datos y sistemas críticos en caso de un desastre.
- **La disponibilidad de los recursos necesarios**. Las pruebas deben verificar que los recursos necesarios para la recuperación, como las copias de seguridad, el hardware y el software, estén disponibles y sean funcionales.
- **La coordinación de los equipos involucrados**. Las pruebas deben garantizar que los equipos involucrados en la recuperación, como el personal de TI, los usuarios finales y los proveedores externos, estén coordinados y preparados para actuar en caso de un desastre.

Las pruebas del DRP deben realizarse periódicamente, al menos una vez al año. Las pruebas deben ser lo suficientemente exhaustivas para identificar cualquier problema o deficiencia en el plan.

En el caso de los procedimientos descritos, las pruebas y mantenimiento podrían incluir las siguientes actividades:

- **Seguridad Perimetral de la Red de Cómputo y Comunicaciones Digitales**

- Realizar pruebas de restauración de la configuración del Firewall a partir de las copias de seguridad.
- Verificar que el hardware y el software necesarios para la recuperación estén disponibles y sean funcionales.
- Realizar simulaciones de incidentes menores y mayores para evaluar la respuesta del personal de TI y los usuarios finales.

- **Servidor de Aplicaciones Institucionales**

- Realizar pruebas de restauración de los datos y sistemas críticos a partir de las copias de seguridad.
- Verificar que el hardware y el software necesarios para la recuperación estén disponibles y sean funcionales.
- Realizar simulaciones de incidentes menores y mayores para evaluar la respuesta del personal de TI y los usuarios finales.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

IX. Acciones preventivas

Con el fin de minimizar los riesgos y mitigar los posibles efectos de un daño mayor a losactivos informáticos indicados en este plan, se realizan las siguientes acciones preventivas:

IX.1 Servidor de sistemas y Aplicaciones Institucionales

- Alojamiento del servidor en el SITE que es un espacio adecuado con las condiciones físicas, ambientales y de seguridad de acceso adecuadas.
- Utilización de un Sistema de Suministro Ininterrumpido de Energía Eléctrica (UPS).
- Montaje en Gabinete.
- Restricción de cuentas de administración.
- Uso de aplicación antivirus.
- Actualizaciones puntuales del Sistema Operativo.
- Mantenimiento preventivo periódico físico y lógico.
- Respaldo mensual de la integridad total del Servidor en un disco duro externo.

IX.2 Seguridad perimetral de la red informática y comunicaciones digitales

- Alojamiento del Firewall en el SITE que es un espacio adecuado con las condicionesfísicas, ambientales, de seguridad de acceso y conectividad adecuadas.
- Utilización de un Sistema de Suministro Ininterrumpido de Energía Eléctrica (UPS).
- Montaje en Rack de Aluminio.
- Restricción de cuentas de administración.
- Monitoreo permanente de la operación y funcionalidad del Firewall.
- Actualizaciones puntuales del Sistema Operativo.
- Mantenimiento preventivo periódico.
- Actualización y pago de la licencia Forticare.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

I. Glosario

CELSH: Congreso del Estado Libre y Soberano de Hidalgo.

Usuario: es una persona que utiliza una computadora o un servicio de red.

Software: comprende el conjunto de los componentes lógicos necesarios que hace posible la realización de tareas específicas.

Hardware: son todas las partes físicas, tangibles, de un sistema informático, sus componentes eléctricos, electrónicos y electromecánicos.

DRP: recuperación de desastres informáticos.

FortiGate: Es un firewall de próxima generación y es una gran amenaza contra los ataques cibernéticos. A través de capacidades avanzadas de inspección y filtrado de tráfico, FortiGate protege las redes empresariales de intrusiones y ataques garantizando un rendimiento óptimo de la red.

Servidor: es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red.

Recursos: cualquier componente físico o virtual de disponibilidad limitada en un sistema informático.

Internet: es una red de computadoras interconectadas entre sí a nivel mundial con el objetivo de hacer común información de acceso público.

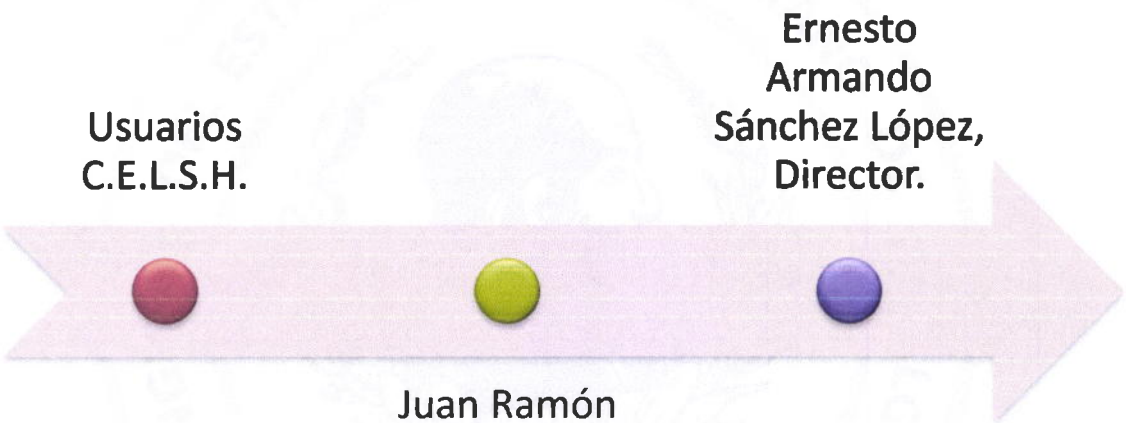
Site: proveen el espacio para albergar el equipo de telecomunicaciones y cómputo de una organización.

Almacenamiento: consiste en la conservación de información empleando una tecnología específicamente desarrollada para mantener los datos y que se encuentren accesibles siempre que sean necesarios.

Seguridad: se encarga de mantener la confidencialidad de los datos de tu organización y de recuperar el control mediante el uso de recursos de gestión de riesgos en el caso de que se haya producido algún incidente.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

Proceso de escalación de reportes de fallas



Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00

Fecha de elaboración	**25/Enero/2024**
Proyecto	**DRP Informáticos**
Asunto	**DRP**
Versión	**CELSH-DRP-2023-02**
Responsable	**Juan Ramón Dimas**
Cargo	**Encargado de la Red de Cómputo y Comunicaciones Digitales**

Elaboró	Revisó	Autorizó
Ing. Juan Ramón Dimas *Encargado de la Red de Cómputo y Comunicaciones Digitales*	**Ing. Ernesto Armando Sánchez López** *Director de la Unidad Informática*	**Héctor Adrián Terán Castelán** *Director General de Servicios Administrativos*

Vo. Bo.
Dip. Jesús Osiris Leines Medécigo Presidente de la Junta de Gobierno del Congreso del Estado Libre y Soberano de Hidalgo.

Plaza Cívica Miguel Hidalgo, "Centro Cívico",
Carretera México-Pachuca Km. 84.5, Col. Carlos Rovirosa,
C.P. 42082, Pachuca de Soto, Hidalgo, México.
www.congreso-hidalgo.gob.mx
(771) 71.744.00