DIRECCIÓN DE INNOVACIÓN,
PLANIFICACIÓN Y
NUEVAS TECNOLOGÍAS

PLAN DE CONTINGENCIA PARA EL

FUNCIONAMIENTO PARLAMENTARIO REMOTO

AISLAMIENTO SOCIAL, PREVENTIVO Y OBLIGATORIO CORONAVIRUS COVID-19

Objetivo

General

Generar una herramienta de prevención, mitigación, control y respuesta a posibles contingencias surgidas durante la realización de una sesión de parlamento remoto.

Específicos

- Determinar los riesgos potenciales que podrían generar una falla en la infraestructura informática durante una sesión de parlamento remoto, ya sea por fallas en los diferentes elementos involucrados o por acciones realizadas por agentes externos.
- Definir mecanismos de prevención y control, y en el caso de presentarse una contingencia, activar los mecanismos del plan.
- Identificar los equipos, tanto internos como externos que puedan ofrecer sus servicios de apoyo logístico, para ser vinculados al Plan de Contingencia.
- Definir el grupo de respuesta con sus respectivos procedimientos operativos.

Alcance

El alcance de este plan guarda relación con la infraestructura informática necesaria para el funcionamiento del parlamento remoto.

Entenderemos como infraestructura informática al hardware, software y elementos complementarios que soportan la información o datos críticos para la función del parlamento remoto.

Un Plan de Contingencia considera una "planificación de la contingencia" así como un conjunto de "actividades" las que buscan definir y cumplir metas que permitan controlar el riesgo asociado a una contingencia.

Elementos de la infraestructura informática

A continuación, se identifican los diferentes elementos que forman parte de la infraestructura informática desplegada para el funcionamiento del parlamento electrónico en la HCDN. Para cada uno de estos elementos se describen las posibles fallas y las acciones necesarias para eliminar o mitigar dichas fallas.

Dividiremos los elementos en dos grandes grupos, elementos de cliente y elementos de centro de datos.

Elementos de cliente

Red eléctrica

Red eléctrica de hogar sin sistema de respaldo. Cabe aclarar que los dispositivos móviles cuentan con baterías. Si bien se recomienda el uso de PC para realizar las reuniones virtuales, también es recomendable tener los dispositivos móviles configurados y con carga completa para que sirvan de contingencia en caso que falle la red eléctrica.

Vínculo de internet

Único vínculo de internet sin garantía de calidad de servicio. Como alternativa a la conexión a internet vía banda ancha, también es posible crear una red wifi mediante los dispositivos móviles con conexión a la red de datos 3g/4g.

Plataforma de cómputo

Puede utilizarse Notebook, Tablet o celular o una combinación de ellos. El dispositivo/s debe tener la VPN configurada. Se recomienda la utilización de PC y auriculares para una mejor calidad de audio y video.

Plataforma de videoconferencia

La plataforma de videoconferencia del lado del cliente requiere solamente el acceso a una página web pero también cuenta con un cliente disponible para dispositivos móviles y pc, siendo esta última la recomendada.

Plataforma de identificación

Para la identificación, se debe tomar una serie de fotos del rostro (selfie) y enviarlas al sistema mediante la plataforma de la HCDN. El sistema demora aproximadamente 5 segundos en dar una respuesta.

Elementos del centro de datos

Red eléctrica

El centro de datos de la HCDN cuenta con un sistema de red eléctrica compuesto por dos UPS (sistemas de alimentación ininterrumpida) dos entradas de línea diferentes y dos grupos electrógenos. Para que el sistema falle, deberían fallar las dos UPS o las dos entradas de línea y los dos grupos electrógenos.

Vínculo de internet

Está compuesto por un Sistema Autónomo, dicho sistema mantiene las tablas de ruteo independientemente del proveedor de internet. Actualmente, la HCDN cuenta con 2 proveedores de internet: IPLAN y Metrotel. Para que el vínculo de internet falle, debe haber una falla simultánea de los dos proveedores de internet.

Plataforma de cómputo

La plataforma de cómputo de la HCDN está compuesta por un sistema de ingeniería de máquinas virtuales (Oracle). Dicho sistema cuenta con componentes redundantes y su ingeniería permite mantener los servicios activos de forma automatizada si alguno de los componentes falla. Esto permitió en el último año, llegar al 99.95% de disponibilidad de la plataforma.

Plataforma de videoconferencia

La plataforma seleccionada es Cisco Webex, la cual ha sido utilizada para el desarrollo de las videoconferencias de más de 20 reuniones de comisión. En dichas reuniones se realizaron pruebas de seguridad, funcionalidad y facilidad de uso. La plataforma utiliza una infraestructura de nube independiente de la HCDN y de probada confiabilidad con cifrado de punta a punta respecto de los clientes y la nube. Cuenta con centros de cómputos distribuidos globalmente que permitirían la continuidad de la operación, aunque un evento crítico interrumpiera las operaciones en el centro de cómputos de la HCDN. Para que esta plataforma falle, debería fallar el servicio a nivel de Cisco a nivel global.

Plataforma de identificación

La plataforma de identificación funciona en el centro de datos del RENAPER. Con respecto a la Infraestructura el ReNaPer, cuenta con dos centros de datos independientes que funcionan de forma sincronizada. Actualmente existen decenas de organismos públicos, bancos públicos y privados que utilizan este servicio las 24 horas al día, los 7 días de la semana.

Análisis de riesgos

Proceso Metodológico

Para la evaluación de los diferentes factores de riesgo, se debe considerar el siguiente proceso metodológico:

- Valoración de la sensibilidad a fallos de los diferentes elementos que integran el sistema.
- Identificación de los elementos de mayor sensibilidad y vulnerabilidad.
- Evaluación de los diferentes factores de riesgo.

Matriz de riesgo: El proceso de evaluación ejecutado bajo los tres ítems anteriores arrojó una calificación de riesgo de Nivel Bajo/Medio, que se corresponde con la capacidad de respuesta de la estructura con la cual se implementa el Protocolo de Funcionamiento Parlamentario Remoto.

		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA	MUY BAJO	BAJO	MEDIO
	MEDIA	BAJO	MEDIO	ALTO
	ALTA	MEDIO	ALTO	MUY ALTO

Valoración

Elementos del cliente

Red eléctrica		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA		BAJO	
	MEDIA			
	ALTA			

Vínculo de internet		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA		BAJO	
	MEDIA			
	ALTA			

Plataforma de cómputo		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA		BAJO	
	MEDIA			
	ALTA			

Plataforma de video conferencia		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA		BAJO	
	MEDIA			
	ALTA			

Plataforma de identificación		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA		BAJO	
	MEDIA			
	ALTA			

Elementos del centro de datos

Red eléctrica		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA			MEDIO
	MEDIA			
	ALTA			

Vínculo de internet		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA			MEDIO
	MEDIA			
	ALTA			

Plataforma de cómputo		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA			MEDIO
	MEDIA			
	ALTA			

Plataforma de video conferencia		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA			MEDIO
	MEDIA			
	ALTA			

Plataforma de identificación		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD	BAJA			MEDIO
	MEDIA			
	ALTA			

Identificación de los elementos de mayor sensibilidad y vulnerabilidad.

Para la valoración del riesgo, se tuvo en cuenta que todos los elementos analizados tienen una contingencia. Es por eso que la **probabilidad de falla** es baja. En el Anexo I puede verse el detalle técnico de los sistemas de contingencia.

Los elementos del centro de datos tienen alto **impacto** dado que su falla dejaría el sistema inoperativo para todos los clientes. En cambio, una falla en un cliente, no evita que el resto del sistema continúe en funcionamiento.

De las matrices de valoración surge que el riesgo de falla es BAJO/MEDIO.

Contingencia ante la falla.

A continuación, se describe las diferentes acciones que se seguirán ante alguna contingencia prevista en este documento.

Elementos de cliente

Red eléctrica

Ante una falla de la red eléctrica, utilizar un dispositivo móvil con acceso a la red de datos 3g/4g. Dichos dispositivos deben tener instalados y configuradas las aplicaciones de VPN, cliente Cisco Webex y cliente Microsoft Teams.

Vínculo de internet

Ante perdida o degradación de la conexión de banda ancha, utilizar un dispositivo móvil con acceso a la red de datos 3g/4g. Dichos dispositivos deben tener instalados y configuradas las aplicaciones de VPN, cliente Cisco Webex y cliente Microsoft Teams. También se puede compartir la red de datos de un dispositivo móvil en forma de red wifi y conectar la PC a dicha red.

Plataforma de cómputo

Si el dispositivo utilizado falla por alguna razón y la mesa de ayuda no puede solucionarlo, utilizar un dispositivo alternativo, el cual debe estar previamente configurado con las aplicaciones de VPN, cliente Cisco Webex y cliente Microsoft Teams.

Plataforma de videoconferencia

Si un cliente no puede conectarse a la reunión o tiene algún inconveniente con el cliente de videoconferencia, debe contactar a la Mesa de Ayuda de la HCDN para recibir asistencia.

Plataforma de identificación

Para realizar la verificación de identidad, el sistema requiere de una fotografía (autorretrato o selfie) del usuario, la cual debe cumplir al menos con los siguientes requisitos:

- expresión neutra del fotografiado,
- fondo uniforme detrás del rostro,
- ausencia de anteojos,
- un plano tal que el rostro cubra la mayor proporción posible de la captura fotográfica.

Si se tuvieron en cuenta las recomendaciones anteriores y no es posible identificarse o no es posible acceder a la plataforma de identificación, comunicarse con la Mesa de Ayuda de la HCDN, quien deribará el caso a ReNaPer.

Centro de datos

Red eléctrica

Ante una falla de alimentación eléctrica en el anexo A, el sistema está preparado para responder de forma automática y tomar electricidad del anexo C sin interrupción de servicio. El Dpto. de Ingeniería Tecnológica de DGIS, verifica que la contingencia para este elemento funcione correctamente (para más detalle ver el Anexo I) y da aviso a la Mesa de Ayuda de la situación.

Si la contingencia automática falla, el Dpto. de Ingeniería Tecnológica, identifica la falla de la contingencia. Si la falla se debe al tablero de distribución que se encuentra en el centro de datos, realiza el pase manual a la toma de tensión del anexo C. Si la falla es de alimentación en dicho tablero, se notifica a la Dirección de Servicios Generales. Se cuenta con 20 minutos aproximadamente de autonomía de batería de las UPS. Si no se resuelve la falla en ese lapso, se producirá una caída total del centro de cómputo y solo estará disponible la plataforma de teleconferencia, dado que la misma se encuentra por fuera de la infraestructura de la HCDN.

Vínculo de internet

Como se mencionó anteriormente, el vínculo de Internet, cuenta con una redundancia basada en dos proveedores diferentes y el Sistema Autónomo. Ante la falla de uno de los proveedores, el Dpto. de Ingeniería Tecnológica de DGIS se comunica con el proveedor e informa de la situación a la Mesa de Ayuda. Si se produce la falla de los dos proveedores de forma simultánea, los servicios del centro de datos no podrán ser alcanzados desde fuera de la red de la HCDN y solo estará disponible la plataforma de teleconferencia dado que la misma se encuentra por fuera de la infraestructura de la HCDN.

Plataforma de cómputo

Ante la falla de algún servidor físico, del sistema de ingeniería de cómputo de la HCDN, los servicios asociados al Parlamento Remoto pueden migrarse de forma automática a otro servidor físico sin perder servicio. Lo mismo pasa con la conectividad y el sistema de almacenamiento, todo cuenta con hardware redundante. Ante la falla completa la plataforma de cómputo, solo estará disponible la plataforma de teleconferencia dado que la misma se encuentra por fuera de la infraestructura de la HCDN.

Plataforma de videoconferencia

Ya se explicó la fortaleza de la plataforma de videoconferencia utilizada y que es independiente del centro de datos de la HCDN. Ante la falla de dicha plataforma, la HCDN cuenta con Microsoft Teams montada sobre la nube Microsoft Azure y de similares características y funcionamiento que Cisco Webex. Ante la falla de la plataforma de Cisco Webex, la Dirección de Sistemas Electrónicos de DGIS, notifica a la Mesa de Ayuda y a la Dirección de Diputados TV, genera una reunión en Microsoft Teams y envía los datos de la nueva reunión. Los participantes deben ingresar a la nueva reunión.

Plataforma de identificación

Ante la falla del sistema de identificación, el Dpto. de Ingeniería Tecnológica de DGIS notifica del problema al RENAPER para identificar y evaluar la falla y si es posible la restauración del servicio, de no ser posible, el servicio de identificación no estará disponible.

Anexo I: Especificaciones técnicas

Red eléctrica

El suministro eléctrico del centro de datos de la HCDN es asegurado mediante dos UPS (Sistema de Alimentación Ininterrumpida) “en línea”, es decir que las baterías alimentan directamente el equipamiento y el suministro eléctrico de red las mantiene cargadas.

Estos dos UPS funcionan en paralelo alimentado sendas fuentes de energía que proveen redundancia al sistema de cómputo, almacenamiento y comunicaciones. La falla de un UPS no afectaría el funcionamiento del equipamiento del centro de cómputos.

Por otro lado, el centro de cómputos posee dos líneas de suministro eléctrico: una propia del Anexo A y otra desde el Anexo C, conectadas a los grupos generadores de dichos anexos. Ante la interrupción del suministro eléctrico de uno de ellos, el tablero conmuta al otro mientras los UPS permiten el funcionamiento normal del hardware del centro de cómputos. Su batería tiene una duración de 20 minutos, tiempo suficiente para que, en caso de una interrupción simultanea de las dos líneas de suministro eléctrico, los generadores de los anexos entren en funcionamiento.

Por último, cabe destacar que todo el equipamiento del centro de cómputos cuenta con contratos de mantenimiento y soporte, y toda la plataforma de la HCDN es monitoreada mediante una herramienta que permite tener una visión general del estado de la red y estadísticas de uso.

Vínculo de internet

La HCDN cuenta con un segmento IP propio y un sistema autónomo (ASN) lo que permite dotar de redundancia el vínculo a Internet de la HCDN. Dicha redundancia hoy está siendo provista por dos vínculos a Internet de 1 Gbps c/u pertenecientes a las empresas Metrotel (CPS Comunicaciones SA) y IPlan (NSS SA).

En caso de presentarse la eventualidad de la caída de uno de los vínculos, el tráfico es re direccionado automáticamente y sin interrupciones hacia el otro vínculo.

Además, es posible re direccionar de manera manual el tráfico hacia un vínculo específico en caso de que el proveedor del servicio de Internet presente problemas de ruteo. La operación de conmutación manual de un enlace hacia otro, demanda un tiempo no superior a los 10 minutos. Asimismo, se informa que existe un SLA acordado entre la HCDN y los ISP que prevé la atención de reclamos 24 horas, todos los días de la semana, con un esquema de escalamiento en caso de incidentes críticos.

VPN (Red Privada Virtual)

El organismo dispone de un sistema de VPN que permite interconectarse remotamente a la red del organismo utilizando un vínculo cifrado. El protocolo de VPN utilizado en la HCDN se denomina IPsec/IKE2. Dicho protocolo es el que mayor nivel de seguridad y performance provee a esta clase de conexiones. Considerando la posibilidad de que puedan presentarse problemas de bloqueo de VPNs por parte de proveedores de internet, se diseñó un esquema de URL ofuscadas y segurizadas.

Firewall

La HCDN cuenta con un firewall (equipo que tiene por función proveer seguridad controlando el tráfico entre las distintas redes de datos del organismo e Internet) Fortinet Fortigate 1500D con redundancia

de componentes críticos (fuentes de alimentación e interfaces de red), por lo que la falla en uno de sus componentes críticos no afecta la operación del sistema.

Plataforma de cómputo

La HCDN cuenta con un centro de datos propio con equipamiento de moderna tecnología y contratos de mantenimiento vigentes. El centro de datos alcanza un nivel de virtualización superior al 90% ello significa que “los servidores” donde se ejecutan las aplicaciones no son equipos físicos, sino que son VMs (máquinas virtuales) que corren dentro de un sistema de ingeniería (Oracle en nuestro caso) con 6 nodos de cómputos que proveen capacidad dinámica en función de cargas de trabajo. Además, cada nodo de cómputo cuenta con componentes que son redundantes entre sí. Las máquinas virtuales pueden moverse de un nodo de cómputo a otro en caso de falla o necesidad de mantenimiento de un nodo.

Plataforma de almacenamiento

El centro de cómputos de la HCDN cuenta con un sistema de almacenamiento de última tecnología compuesto por cajones de discos de estado sólido y componentes críticos redundantes (fuentes de alimentación, controladoras, interfaces de red, etc.). Por sus características (contar con componentes sin partes mecánicas como son los discos de estado sólido) la fiabilidad y rendimiento del sistema cumplen con los estándares más exigentes de centro de datos de alta performance en cuanto a este equipamiento.

Plataforma de backup

Pese a que el equipamiento anterior cuenta con componentes redundantes y el sistema de almacenamiento es extremadamente fiable, con objeto de asegurar el resguardo de datos se dispone de un esquema de copias de seguridad en cintas denominadas LTO efectuadas de forma automatizada y de manera diaria que son almacenadas en una caja fuerte fuera del ámbito de la Dirección General de Informática y Sistemas. Se utiliza un esquema denominado GFS con backups diarios-semanales-mensuales con un histórico de un año. Por lo que en caso de un evento catastrófico que afectara el centro de cómputos del organismo, permitiría la restauración de todos los datos que allí se alojaban, en una nueva infraestructura.

Plataforma de videoconferencia

Cisco Webex utiliza una infraestructura de nube independiente de la HCDN y de probada confiabilidad con cifrado de punta a punta respecto de los clientes y la nube. La plataforma cuenta con centros de cómputos distribuidos globalmente que permiten la continuidad de la operación de la plataforma, aunque un evento crítico interrumpa las operaciones con el centro de cómputos de la HCDN.

Como contingencia contamos con la plataforma Microsoft Teams montada sobre la nube Microsoft Azure disponible por el acuerdo empresarial entre la firma Microsoft y la HCDN.

Figure 1. Magic Quadrant for Meeting Solutions

Source: Gartner (September 2019)

Plataforma de identificación

Existen distintas instancias de verificación de identidad:

- conexión a la VPN de la HCDN,
- ingreso a www.recinto.hcdn.gob.ar con usuario y contraseña,
- verificación de identidad por ReNaPer.

Para realizar la verificación de identidad, el Registro Nacional de las Personas (RENAPER) precisa el número de DNI, el sexo (información contenida en la base de datos de la HCDN) y la fotografía (autorretrato o selfie) del usuario, la cual debe cumplir con los siguientes requisitos:

- expresión neutra del fotografiado,
- fondo uniforme detrás del rostro,
- ausencia de anteojos,

- un plano tal que el rostro cubra la mayor proporción posible de la captura fotográfica.

Con los datos enviados, el Sistema Automatizado de Identificación Biométrica (ABIS) del RENAPER realiza la verificación de identidad y devuelve como resultado un valor entre 0 y 100, donde cualquier valor superior a 60 puntos determinará que la persona fotografiada es quien dice ser. El tiempo de verificación que efectúa el sistema es de entre 3 y 5 segundos en línea.

La fotografía selfie capturada es transmitida de manera cifrada y en formato base64, junto al DNI y el sexo al centro de datos del RENAPER a través de la Interfaz de Programación de Aplicaciones (API) expuesta para tal fin.

La API recibe la fotografía, la convierte a imagen binaria y mediante el DNI y el sexo recibido, ejecuta una consulta sobre la base de datos DNI/Pasaporte de RENAPER y recopila la mejor fotografía asociada a un trámite firmado digitalmente y emitido por dicho organismo.

Luego, la API presenta ambas fotografías al monitor biométrico. El monitor ejecuta la comparación utilizando el algoritmo específico para tal fin, devuelve el resultado a la interfaz, y la interfaz arroja el resultado al requirente.

La tecnología empleada para el reconocimiento facial es una herramienta denominada 'NeoFace Watch' de la empresa NEC, implementada e integrada en la República Argentina por personal del RENAPER y reconocida por el National Institute of Standards and Technology (NIST) en sus informes oficiales (ver en referencia:

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf)

La acción de verificación cuenta con un número de transacción único llamado TCN, que identifica a esta operación con fecha y hora y el resultado. Toda esta información está trazada en el sistema por lo que se puede generar un reporte cuando sea necesario.

Con respecto a la Infraestructura el RENAPER cuenta con dos centros de datos independientes que funcionan de forma sincronizada.

Existen decenas de organismos estatales, Bancos Públicos y Privados que utilizan este servicio las veinticuatro horas del día, los siete días de la semana.