Manual.

Manual para la continuidad del negocio

RT-Ma03

SISTEMA GESTIÓN DE CALIDAD

SENADO DE LA REPÚBLICA

TABLA DE CONTENIDO

INTRODUCCIÓN

Conscientes de la importancia que tiene la infraestructura de tecnologías de la información como soporte a los procesos estratégicos, operativos y de apoyo del Senado de la Republica es fundamental que el nivel de protección que tenga los activos de información de la entidad estén dentro de un nivel de riesgo aceptable, de ahí que la estrategia de recuperación de la infraestructura tecnológica del Senado debe estar alineada con la misión, visión y en general al objetivo social de la entidad; de igual forma que permita su resilencia ante eventos no deseados que amenacen la supervivencia o la continuidad de sus operaciones durante la ocurrencia de un desastre, garantizando principalmente, la preservación de tres características:

- **Integridad:** que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento.
- **Confidencialidad:** que la información sea accesible solo a las personas autorizadas.
- **Disponibilidad:** que los usuarios autorizados tengan acceso a la información y los recursos cuando lo necesiten.

El presente documento pretende ser utilizado como plan de continuidad de negocio, a través del cual se recomenda la estrategia(s) de recuperación que pueda permitir la continuidad de las funciones de la infraestructura informática critica del Senado de la Republica, tomando como punto de referencia el nivel de disponibilidad de información, tecnología actual, ventajas y desventajas; buscando adaptarla a las necesidades actuales de disponibilidad de la entidad.

Con el fin de contar con un mecanismo que permita prevenir o reaccionar ante posibles incidentes que pongan en riesgo a los activos de información, impedir la prestación y continuidad del servicio a las diferentes dependencias y soportar la planeación estratégica de la Entidad. La división de Planeación y Sistemas reúne una serie de acciones a desarrollar en el Plan de continuidad del negocio que, permitirían responder de manera eficaz ante una eventualidad y restablecer en menor tiempo posible la disposición de los servicios informáticos que se prestan y mitigar el impacto negativo que pueda ocasionar.

Así pues, este plan de continuidad del negocio tiene en cuenta lo dispuesto en el manual de políticas de seguridad de la información, el cual se encuentra publicado en el portal web del Senado, articulado a la planeación estratégica y operativa de la entidad.

El plan de continuidad adquiere mayor relevancia una vez sea apropiado por todos los funcionarios, usuarios y contratistas de manera anticipada y será actualizado y comunicado según las necesidades de la entidad.

1. OBJETIVO

1.1. Objetivo General:

- Definir las actividades preventivas y correctivas para reaccionar de manera eficiente ante una eventualidad que comprometa el desarrollo de las actividades cotidianas, la seguridad del personal o la prestación del servicio.

1.2. Objetivos Específicos:

- Determinar la vulnerabilidad en el centro de datos e instalaciones de negocios y definir las medidas preventivas que se pueden tomar para reducir al mínimo la probabilidad y el impacto en la perdida de información del Senado de la Republica
- Definir los servicios de la plataforma tecnológica, definir la criticidad y los tiempos máximos de recuperación ante fallas o eventos catastróficos.

- Definir niveles de alerta que permitan identificar posibles amenazas a la seguridad de la infraestructura tecnológica

- Asegurar una pronta recuperación en los servicios críticos para los Grupos de Valor
- Disminuir los tiempos de interrupción de la operación de los procesos

- Definir las acciones para minimizar el tiempo de inactividad y la pérdida de datos de la entidad

2. ALCANCE

El plan de continuidad del negocio inicia con la identificación y socialización de los elementos críticos del Senado de la Republica que puedan definirse como incidente o desastre que impidan continuar la operación y finaliza con el análisis y acciones de mejora identificadas de la reacción ante la situación presentada mínimo una vez al año (simulacro o realidad).

3. TÉRMINOS Y DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la entidad, y en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: documento en el que los funcionarios del Senado o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Amenaza: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Directorio Activo: Servicios de directorio es una base de datos distribuida que permite almacenar información relativa a los recursos de una red con el fin de facilitar su localización y administración.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Evaluación del Riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de Seguridad de la Información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión del Riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de Seguridad de la Información: un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

Resilencia: La capacidad para adaptarse positivamente a situaciones adversas**.**

Sistema de Información (SI): Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Seguridad de la Información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Sistema de Gestión de la Seguridad de la Información SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Plan de Continuidad del Negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

Tratamiento del Riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

Valoración del Riesgo: proceso global de análisis y evaluación del riesgo.

4. DESARROLLO DEL CONTENIDO

4.1. ROLES, MECANISMOS Y RESPONSABILIDADES

ROL	RESPONSABLE	MECANISMOS
Jefe de División	Jefe División de Planeación y Sistemas	Generar las directrices para la Creación, implementación y actualización del plan de continuidad del negocio
Coordinador de Sistemas	Asesor II División de Planeación y Sistemas	Coordinar la implementación del plan de continuidad del negocio
		Realizar seguimiento a los lineamientos estratégicos dispuestos en el plan
Profesionales de apoyo	Profesional universitario Profesionales de apoyo (contratistas)	Mesas de trabajo
		Gestor de información
		Análisis de la información
		Metodología de riesgos
		Inclusión en el plan de acción anual de las actividades
Aprobación	Comité de Calidad	Sesiones ordinarias y extraordinarias del Comité
Socialización y pruebas del plan de continuidad,	Profesionales de apoyo	Campañas de divulgación
	Equipo de comunicaciones internas	
Activación del Plan de emergencia y Plan de restablecimiento	Administradores de servicios tecnológicos - Grupo de trabajo Seguridad de la Información - Grupo de trabajo de Control de Cambios	Mesas de trabajo, Análisis y pruebas, Inspección y verificación
Restablecer prestación de servicio		Comunicación con los grupos

4.2 GENERALIDADES DEL PLAN DE CONTINUIDAD

El Plan de Continuidad reúne un conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento de la entidad y la prestación de sus servicios tecnológicos, para lo cual se establecen los siguientes aspectos:

- **Preventivo:** Dentro de este aspecto se involucran los recursos humanos, quienes deben estar preparados en caso de presentarse un evento inesperado, y las acciones anticipadas que se puedan articular a la gestión de los diferentes procesos.

- **Reactivo:** Este aspecto va dirigido a fortalecer las políticas internas de restauración y comunicarlas oportunamente para ponerlas en marcha una vez detectada la contingencia.

- **Recuperación:** Este aspecto está enfocado en las actividades a desarrollar en el momento de atender una contingencia.

4.3 ANÁLISIS DEL ENTORNO INSTITUCIONAL

Teniendo en cuenta las funciones y obligaciones normativas de la entidad, que se consolidad y apoyan las actividades legislativas que se manejan en el Senado de la República y que podrían ocasionar un inadecuado desarrollo en la prestación de los servicios, se pretenden mitigar con un plan de continuidad representado en los siguientes aspectos:

Aspectos Externos

- **Económicos:** Disminución presupuestal, demoras o dificultades para el traslado de recursos de inversión o de funcionamiento, cambios de gobierno en la priorización y traslado de recursos.
- **Políticos:** Cambio de mesa directiva, nuevas prioridades del Senado, jornada electoral.
- **Sociales:** Manifestaciones y protestas frecuentes en el centro de la ciudad, dificultad de acceso para el grupo técnico y los usuarios de los sistemas, daños intencionados a la infraestructura de la Entidad.
- **Tecnológicos:** Deficiencia en la interoperabilidad de los sistemas de administración, monitoreo y gestión, diferencia en las plataformas tecnológicas del negocio, ataques externos e internos a la información y las herramientas tecnológicas.
- **Medio Ambientales:** Ubicación de la entidad cerca a los cerros, incendios, terremotos, Inundaciones, desastres naturales.

Aspectos Internos

- **Financieros:** Dificultad para la priorización de recursos, cambios frecuentes en el plan de adquisición, comunicación inoportuna de los cambios, demoras en la apropiación de recursos, fallas en los sistemas de registro SIIF.
- **Personal:** Planta de personal insuficiente, nuevas exigencias de competencias del personal en el nuevo modelo de operación, tiempo insuficiente para el desarrollo de habilidades, falta de motivación e involucramiento del personal, alta rotación de personal.
- **Procesos:** nuevos procesos, desconocimiento de las características de los procesos, desconocimiento del nivel de responsabilidad y autoridad de los procesos, baja apropiación del nuevo modelo, baja asistencia a las capacitaciones de socialización y las mesas de creación de los procesos.

- **Tecnología:** Desconocimiento de un Plan estratégico de TI, desarticulación de las herramientas y aplicativos internos, fallas en la infraestructura tecnológica, fallas en el sistema de seguridad de la información, desconocimiento de los niveles de responsabilidad y autoridad frente a los sistemas.
- **Estratégicos:** Cambios en la gestión institucional sin planificación y comunicación oportuna, fallas en la comunicación y solicitud de información a las dependencias, ausencia de ANS concertados, fallas en la comunicación interna, solicitud de información múltiple, fallas en los sistemas de información.
- **Comunicación Interna:** Desconocimiento en los temas gestionados por parte del Senado de la Republica, Inapropiada distribución de canales internos, Inoportunidad en la entrega de información, falta de registros de información y contactos actualizados y protegidos.

4.4 RIESGOS ASOCIADOS A LA CONTINUIDAD DEL NEGOCIO

El Senado de la Republica contempla implícitamente en la gestión de sus procesos la identificación y administración de los riesgos como práctica para impedir que eventualidades internas o externas impidan cumplir sus metas institucionales, por lo cual, al desarrollar el plan de continuidad del negocio se integra la metodología de riesgos aplicada y el control preventivo, detectivo y correctivo de dicho plan estaría asociado al mapa de riesgos institucional.

Para el monitoreo preventivo del ejercicio de continuidad del negocio y del servicio el Senado cuenta con los siguientes riesgos existentes:

Clasificación del Riesgo	**Nombre del Riesgo**	**Descripción del Riesgo**
Información	Perdida de información institucional	Se asocia con la pérdida de información física y digital de los archivos, bases de datos, servidores y Sistemas de Información de la Entidad
Disponibilidad	No restablecimiento de los servicios tecnológicos de la entidad	Contempla la disponibilidad para uno de la información y de los servicios que tiene la entidad con sus usuarios.
Imagen	Pérdida de credibilidad y confianza en la entidad.	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la Entidad.
Información	No restauración de la información respaldada	Se asocia con la pérdida de información física y digital de los archivos, bases de datos, servidores y Sistemas de Información de la Entidad.
Operativo	Daño o deterioro de los activos tangibles.	Comprende el daño o deterioro de los bienes muebles o inmuebles de la Entidad.

Tecnológico	Accesos no autorizados.	Se asocia con el acceso a los sistemas de información, aplicativos, bases de datos o servidores sin autorización previa.
Tecnológico	Afectación de la infraestructura tecnológica.	Está relacionado con el daño, pérdida, siniestro o deterioro a nivel de hardware, networking y enlaces de datos.
Tecnológico	Inadecuados servicios de Tecnologías de la Información.	Contempla la pertinencia, calidad y oportunidad de los servicios de tecnología y las deficiencias en la prestación de los mismos.

Estos riesgos se integrarán a la matriz de riesgos del proceso de gestión de recursos tecnológicos, que maneja el Senado de la República, para el periodo inmediatamente posterior y serán monitoreados a través del sistema de gestión de calidad con que cuenta la corporación de acuerdo a su periodicidad su periodicidad.

4.5 PRUEBAS Y REVISIONES

Las acciones preventivas se llevarán a cabo en toda la entidad según la planificación de la División de Planeación y Sistemas en conjunto con la División de Recursos Humanos y Dirección General Administrativa; durante la definición de la planificación institucional se definirán y aprobarán los simulacros, interrupción del servicio, evacuación de emergencia o pruebas aleatorias del plan de continuidad, según los recursos económicos con los que se cuente en cada vigencia; de igual manera el seguimiento se realizará una vez al año por la División de Planeación y Sistemas.

4.6. GESTIÓN DEL PLAN DE CONTINUIDAD

El Senado de la República deberá emprender las acciones necesarias para comunicarlo a todos los funcionarios, contratistas y terceros de la entidad y de esta manera estar preparados para enfrentar situaciones de emergencia y restablecer en el menor tiempo posible el servicio, para lo cual se seguirá el siguiente protocolo:

OBJETIVO	ACCIÓN	RESPONSABLE	EVIDENCIA

Determinar la vulnerabilidad en el centro de datos e instalaciones de negocios y definir las medidas preventivas que se pueden tomar para reducir al mínimo la probabilidad y el impacto en la perdida de información del Senado de la Republica	Registro de la emergencia presentada	Personal mesa de servicio	Registro plataforma Aranda
	Convocar grupo de trabajo seguridad de la información	Gestor de la información	Acta de reunión
Definir los servicios de la plataforma tecnológica, definir la criticidad y los tiempos máximos de recuperación ante fallas o eventos catastróficos.	Revisión de la afectación de la información	Equipo de sistemas.	Acta de reunión
Definir niveles de alerta que permitan identificar posibles amenazas a la seguridad de la infraestructura tecnológica	Revisión de la afectación de la información	Equipo de sistemas.	Registro plataforma Aranda
Asegurar una pronta recuperación en los servicios críticos para los Grupos de Valor	Analizar daños	Equipo de Trabajo seguridad de la información.	Lista de los servicios afectados por cada administrador
	Contacto con sistemas de soporte	Equipo de sistemas	Registro plataforma Aranda
	Llamado al equipo de restablecimiento	Jefe de División de Planeación y Sistemas	Registro plataforma Aranda - acta de reunión
Disminuir los tiempos de interrupción de la operación de los procesos	Restablecimiento de los sistemas de información	Jefe de División de Planeación y Sistemas	Registro plataforma Aranda
Definir las acciones para minimizar el tiempo de inactividad y la pérdida de datos de la entidad	Análisis de la situación	Equipo de Trabajo seguridad de la información	Informe de situación - Plan de mejoramiento
	Establecer plan de mejoramiento a partir del análisis	Equipo de sistemas	

4.7. BASE LEGAL

- NTC 5722: Gestión de Continuidad del negocio: Esta norma específica los requisitos para planificar, establecer, implementar, operar, supervisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de los incidentes perjudiciales que puedan surgir.

- ISO 31000:2009: norma internacional para la Gestión de Riesgos. Proporciona principios y guías para que las organizaciones lleven a cabo su análisis y evaluación de riesgos.

- ISO 17799:2000: estándar para la administración de la seguridad de la información, publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

- COBIT: Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC

- ITIL: "Information Technology Infraestructura Library", es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la Office of Jovenmente Commerce, una entidad independiente de la tesorería del gobierno británico.

- ISO Serie 27000: es una serie de estándares, que incluye, definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información), (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoria y certificación de SGSI (ISO 27006), una guía de auditoria de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario

5. ANEXOS

N/A

6. FORMATOS

N/A

7. DOCUMENTOS RELACIONADOS

Relacione en este campo los documentos

8. CONTROL DE CAMBIOS

Control de Cambios

- Ver. 001// Rev. 1

  Cambios:

  Justificación: Se crea el presente documento con el fin de cumplir con lo establecido en el Manual de políticas de seguridad de la información. De otra parte como acción frente al hallazgo identificado por la Contraloría en la auditoria vigencia 2016.

  Responsable: Mary Alexandra Rodriguez Bernal

  Fecha: 2017-11-30

ELABORÓ	REVISÓ	APROBÓ
Nombre:Aldair Suarez - Wilmer Amaya	Nombre:Jorge Enrique Carbonell	Nombre: Grupo Evaluador de documentos -SGC
Cargo: Profesional Universitario - Contratista - División Planeación y Sistemas	Cargo: Jefe División Planeación y Sistemas	No. Acta y Fecha: Acta No. 100 del 30 de noviembre de 2017.

Mary Alexandra Rodriguez Bernal @2017-11-30, 16:03:59