ANEXO XIII

ASPECTOS DE SEGURIDAD PARA LA CONTINUIDAD DE LA GESTIÓN

1. OBJETIVO

Responder rápidamente ante las posibles interrupciones de las actividades normales de la S.R.T.

Proteger los procesos críticos mediante acciones de recuperación.

Establecer planes de contingencia para asegurar la efectividad de las operaciones de contingencia del Organismo.

Establecer un Plan de Continuidad para la coordinación eficiente de las áreas de la S.R.T. ante situaciones que requieran acciones de recuperación de los sistemas.

2. ALCANCE

Comprende a todo el personal de la S.R.T., y las relaciones con proveedores, así como también con organizaciones externas y terceras partes involucradas con el Organismo, en caso que compartan o utilicen los activos de información pertenecientes o de propiedad de esta Superintendencia. Será de aplicación en caso de un evento real o potencial que afecte a la operatoria habitual de la S.R.T. impactando sobre la ejecución de sus procesos críticos.

3. DEFINICIONES

Análisis de Riesgos: es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratarlos. Permite comprender la naturaleza del riesgo y determinar su nivel.

Evento disruptivo: sucesos que pueden afectar la normal actividad del Organismo, como, por ejemplo, fallas en el equipamiento, ciberataques, interrupción del suministro de energía eléctrica, inundación, incendio, desastres naturales, destrucción edilicia, atentados, etc.

Plan de Continuidad de las Operaciones: Conjunto de procedimientos documentados, recursos y sistemas que conducen a una respuesta después de una interrupción. Tiene por fin dar respuestas ante una emergencia de manera adecuada, logrando así el mínimo impacto en las operaciones de la S.R.T..

Plan de Recuperación de Desastres (DRP): conjunto de procedimientos documentados que permiten ejecutar las medidas de contención y de mitigación de los incidentes en materia de ciberseguridad.

Procesos Críticos: son aquellos procesos que el Organismo no puede dejar de llevar a cabo bajo ningún escenario de emergencia mayor.

4. RESPONSABILIDADES

El Responsable de Seguridad de la Información (RSI) deberá establecer los requisitos mínimos de seguridad necesarios para mantener el nivel de continuidad de la seguridad de la información durante situaciones adversas, y establecer controles preventivos. Asimismo, deberá velar por la inclusión de estos aspectos de seguridad en el Plan de Continuidad de las operaciones implementado en el Organismo.

El RSI deberá colaborar con el desarrollo de los planes de contingencia necesarios para garantizar la continuidad de las actividades.

Por último, el RSI deberá verificar, revisar y evaluar en intervalos regulares los controles establecidos para la continuidad de la seguridad de la información.

La Subgerencia de Sistemas (S.S.), en conjunto con los Titulares de las Unidades Organizativas, abordarán la continuidad de las operaciones de la S.R.T., determinando los procesos críticos y elaborando los planes de contingencia operativos necesarios para garantizar la continuidad de las actividades.

Por otro lado, la S.S. deberá establecer la arquitectura y requerimientos necesarios, y la elaboración del Plan de Recuperación de Desastres (DRP).

Por último, la S.S. deberá implementar mecanismos que garanticen la disponibilidad de la información crítica y de las instalaciones utilizadas para su procesamiento durante situaciones adversas.

5. CONTENIDO

5.1 GESTIÓN DE LA CONTINUIDAD DE LAS OPERACIONES

Se deberá desarrollar un proceso de administración y gestión de la continuidad operativa que permita brindar respuesta ante la posible interrupción de las normales actividades de la S.R.T.. Para ello, se deberá tener en cuenta:

- Identificar los eventos disruptivos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos a establecer.

5.1.1 Planificación de la Continuidad de las Operaciones

Para accionar ante un evento disruptivo de manera adecuada y buscando reducir su impacto se deberá elaborar y documentar un conjunto de procedimientos, recursos y sistemas que conduzcan a dar respuesta inmediata después de una interrupción. Asimismo, se deberán identificar los requisitos necesarios para cumplir con todos los requerimientos de seguridad de la información, con foco en los procesos críticos y servicios esenciales que preste la S.R.T..

En ese sentido se deberá establecer un Plan de Continuidad que permita brindar respuesta y actuar ante incidentes que produzcan la interrupción de la continuidad de las operaciones en la S.R.T.. Para su elaboración deberán considerarse los siguientes aspectos:

- Priorización de los procesos críticos de la S.R.T.;
- Amenazas y eventos disruptivos identificados que puedan generar escenarios potenciales de interrupción de las actividades del Organismo;
- Controles preventivos a los diferentes eventos disruptivos identificados;
- Análisis de los impactos y ocurrencias de dichas interrupciones;
- Establecimiento de una estructura de gestión;
- Asignación de responsabilidades, estableciendo roles y funciones en equipos de trabajo específicos;
- Elaboración de los planes de contingencia operativos;
- Elaboración de un Plan de Recuperación ante Desastres (DRP);
- Comunicación y capacitación del personal, en materia de procedimientos y procesos de emergencia acordados a través de procedimientos de recuperación.

5.1.2 Procedimientos para la continuidad de las operaciones

Se deberá establecer, documentar, implementar y mantener los procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad operativa necesario, donde se incluyan los aspectos de la seguridad de la información durante situaciones adversas.

Asimismo, se deberán elaborar los procedimientos necesarios para la ejecución del Plan de Recuperación de Desastres para diferentes escenarios de contingencia.

5.1.3 Verificación del Plan de Continuidad de las Operaciones

Se deberán realizar revisiones periódicas de los Planes de Contingencia y del DRP, para evaluar la efectividad de los mismos. Dicha revisión deberá incluir la verificación y evaluación de los controles respecto a la seguridad de la información.

Estas revisiones deberán ser planificadas previamente, mediante el establecimiento de un plan de pruebas, indicando los responsables y un cronograma.

Los resultados de dichas revisiones deberán ser debidamente documentados.

5.2 REDUNDANCIA EN LAS INSTALACIONES DE PROCESAMIENTO Y TRANSMISIÓN DE LA INFORMACIÓN

Se deberán implementar componentes y/o arquitecturas redundantes en las instalaciones de procesamiento y transmisión de la información, a efectos de cumplir con los requisitos de disponibilidad operativa.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66587972-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO XIII Aspectos de Seguridad para la Continuidad de la Gestión-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 4 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:42:02 -03:00

Diego Maximiliano Segovia
Subgerente
Subgerencia de Sistemas
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:55:28 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:55:29 -03:00