DESCRIPCIÓN DEL PROCEDIMIENTO

GOBIERNO DE EL SALVADOR	INSTITUTO NACIONAL DE PENSIONES DE LOS EMPLEADOS PÚBLICOS	*MANUAL DE PROCEDIMIENTOS*

1. **NOMBRE DEL PROCEDIMIENTO:** GESTION PARA LA CONTINUIDAD DEL NEGOCIO
2. **OBJETIVO DEL PROCEDIMIENTO:** Cumplir adecuadamente con las diversas actividades relacionadas a la Gestión de la Continuidad del Negocio, conforme a la normativa aplicable.
3. **FORMATOS UTILIZADOS:** N /A
4. **NORMAS ESPECIFICAS:** Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio "NRP-24"
5. **FRECUENCIA DE USO:** Mensual, Semestral, Anual
6. **PARTICIPANTES DEL PROCEDIMIENTO:** Junta Directiva, Comité de Riesgo, Comité de Continuidad del Negocio, Unidad de Riesgos y todas las Unidades Organizativas del INPEP.
7. **DESCRIPCIÓN DEL PROCEDIMIENTO:**

Nº ACT.	RESPONSABLE	DESCRIPCIÓN
0		Inicio del procedimiento
1	Gestor de la Continuidad del Negocio y Jefe Unidad de Riesgos	Elabora el plan anual de trabajo para la Gestión de la Continuidad del Negocio, con el apoyo del Jefe de la Unidad de Riesgos, para posteriormente presentar a Comité de Riesgos, quien revisa y analiza la documentación para ser remitida a Junta Directiva para su aprobación respectiva.
2	Gestor de la Continuidad del Negocio y áreas determinadas como críticas	Ejecuta la Gestión de Continuidad del Negocio, mediante el desarrollo de cada una de las etapas, conforme a lo indicado en la Normativa, de acuerdo a lo siguiente: ANALISIS El Gestor de la Continuidad del Negocio, realiza la actividad de análisis institucional en las áreas determinadas como críticas, por medio de: a) Análisis del impacto del negocio (BIA): • Inicialmente solicita los manuales de procesos y los planes de contingencia a cada área determinada como critica; • Posteriormente coordina una entrevista • Completa el cuestionario de información preliminar de procesos, • Completa el formato de estructura de respuesta y finalización de eventos, para determinar los tiempos objetivos de respuesta y los tiempos máximos de contingencia.

1. **NOMBRE DEL PROCEDIMIENTO:** GESTION PARA LA CONTINUIDAD DEL NEGOCIO		
2	Gestor de la Continuidad del Negocio y áreas determinadas como críticas	b) Para el análisis de escenarios de riesgos; el Gestor de la Continuidad del Negocio, inicialmente trabaja en conjunto con el Comité de Seguridad y Salud Ocupacional y las áreas determinadas como críticas, para logística y las simulaciones futuras, a fin de documentar debidamente la identificación, cuantificación y calificación de los eventos disruptivos en términos, financieros, reputacionales, operativos, legales y de tiempo.
3	Gestor para la Continuidad del Negocio y áreas determinadas como críticas	ESTRATEGIAS El Gestor de la Continuidad del Negocio realiza: • Reuniones con las áreas determinadas como áreas críticas, para llevar a cabo por medio de: entrevistas, mesas de trabajo y reuniones del personal directamente involucrado en los procesos institucionales identificados como críticos; • Determina el tratamiento y las acciones que se implementaran o se llevaran a la práctica para hacer frente a los posibles eventos disruptivos; para poder seguir brindando los servicios institucionales mínimos requeridos • El Gestor para la Continuidad del Negocio, plasmara en el documento de Análisis de Escenarios de Riesgos Críticos, las acciones y tratamiento determinados

2. **NOMBRE DEL PROCEDIMIENTO:** GESTION PARA LA CONTINUIDAD DEL NEGOCIO

4	Gestor para la Continuidad del Negocio y Jefe de la Unidad de Riesgos	PLAN DE CONTINUIDAD • Elabora el documento que plasme las estrategias • Identifica los diversos escenarios y las diferentes respuestas a dicho evento disruptivo • Identifica los tiempos de respuesta • los tiempos de recuperación; • Brinda una guía a seguir al personal clave involucrado en relación a canales de comunicación, recursos e infraestructura dentro de los periodos de tiempo y capacidad establecida. El plan de continuidad será elaborado con el apoyo del Jefe de la Unidad de Riesgos para ser presentado a Comité de Continuidad del Negocio previa a presentación a Comité de Riesgos quien revisará y analizará su remisión a Junta Directiva para su aprobación respectiva.
5	Gestor para la Continuidad del Negocio, Comité de Seguridad y Salud Ocupacional y Comité de Continuidad del Negocio	PRUEBAS • En Coordinación con el Comité de Seguridad y Salud Ocupacional y el Comité de Continuidad del Negocio, se activa los planes de continuidad del negocio, mediante formas simuladas, para verificar: o el nivel de stress, incluyendo pruebas remotas con personal clave desde casa, sobre las actividades en "X" situación; estas pruebas pueden ser parciales, temporales y no anunciadas; • A medida que la maduración del sistema lo permita se incluirá pruebas completas de escenarios de interrupción que involucren la participación de agentes externos, principalmente de los proveedores de servicios críticos • La ejecución de pruebas completas debe ser validados por el Comité de Continuidad del Negocio, para posteriormente presentar a Comité de Riesgos, quien evalúa los resultados y los remite a Junta Directiva para su aprobación.

1. **NOMBRE DEL PROCEDIMIENTO:** GESTION DE LA CONTINUIDAD DEL NEGOCIO

6	Gestor para la Continuidad del Negocio,	COMUNICACIÓN DE PRUEBAS A SUPERINTENDENCIA DEL SISTEMA FINANCIERO Toda prueba denominada como no anunciada y completa, debe ser informada por el Gestor para la Continuidad del Negocio a la Superintendencia del Sistema Financiero con 30 días de anticipación a su ejecución, indicando tipo y fecha de ejecución, de conformidad a lo estipulado en Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio "NRP-24"
7	Gestor para la Continuidad del Negocio, Comité de Continuidad y Comité de Riesgos	REVISION, MANTENIMIENTO Y SEGUIMIENTO Solicita a los encargados de las áreas críticas el informe correspondiente, posterior a la realización de pruebas, para presentar de manera integral en el Comité de Continuidad del Negocio y posteriormente al Comité de Riesgos, para que se implementen las mejoras de manera oportuna y se informe posteriormente a Junta Directiva.
8	Gestor para la Continuidad del Negocio	MONITOREO Y COMUNICACIÓN Elabora y emite los informes en relación al lanzamiento de nuevos productos o servicios, cambios significativos de procesos o infraestructura tecnológica y que puedan afectar de manera relevante las actividades y procesos críticos de la entidad; así como de las acciones adoptadas luego del resultado de las pruebas y/o incidentes disruptivos; para conocimiento de las diferentes unidades de la institución, presentar a Comité de Riesgos que informa a la Junta Directiva sobre las acciones y/o ejecuciones realizadas a nivel institucional
9		Fin de proceso

DESCRIPCIÓN DE PROCEDIMIENTO

GOBIERNO DE EL SALVADOR	INSTITUTO NACIONAL DE PENSIONES DE LOS EMPLEADOS PÚBLICOS	*MANUAL DE PROCEDIMIENTOS*

1. NOMBRE DEL PROCEDIMIENTO: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.
2. OBJETIVO DEL PROCEDIMIENTO: Cumplir adecuadamente con las funciones de la Gestión de Seguridad de la Información, conforme a lo establecido en las normas aplicables.
3. FORMATOS UTILIZADOS:N /A
4. NORMAS ESPECIFICAS: Normas Técnicas para la Gestión de la Seguridad de la información "NRP-23", ISO 27001.
5. FRECUENCIA DE USO: Mensual, Semestral, Anual
6. PARTICIPANTES DEL PROCEDIMIENTO: Junta Directiva, Comité de Riesgo, Comité de la Seguridad de la Información, Unidad de Riesgo y Unidades organizativas según estructura organizacional.
7. DESCRIPCIÓN DE PROCEDIMIENTO:

NºACT	RESPONSABLE	DESCRIPCIÓN
0		Inicio de procedimiento
1	Gestor de la Seguridad de la Información/ Jefe de Unidad de Riesgos.	Desarrolla la Gestión de la Seguridad de la información, mediante cada una de las etapas conforme a las Normas Técnicas para la Gestión de la Seguridad de la Información "NRP-23" conforme a lo siguiente: <u>PLANEAR:</u> El Gestor de la Seguridad de la Información en esta etapa realiza lo siguiente: • Elabora el plan anual de trabajo para la Gestión de la Seguridad de la Información, con el apoyo del Jefe de la Unidad de Riesgos y posteriormente se remite a Comité de Riesgos para su revisión y validación, para la aprobación de Junta Directiva. • Documenta el Sistema para la Gestión de la Seguridad de la Información por medio de: alcance, las políticas y los controles específicos de Seguridad de la Información.

1. NOMBRE DEL PROCEDIMIENTO: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.		
2	Gestor de la Seguridad de la Información/ Jefe de la Unidad de Ciberseguridad/ Unidades Organizativas.	<u>ÁNALISIS</u> • Solicita a las áreas requeridas dentro de la institución según estructura organizativa, los manuales de procedimientos, activos de información y lineamientos que rigen sus actividades; para el análisis de riesgos asociados a la Seguridad de la Información. • Revisa la información obtenida e identifica los riesgos asociados con los activos de información para dar seguimiento en la ejecución de la Gestión de la Seguridad de la Información. • En caso de ser activos de información El Gestor de Seguridad de la Información los clasifica en el Registro de control de activos. • Posteriormente coordina una entrevista con el jefe inmediato del área requerida, para un diagnóstico y completa matriz de riesgos de la Seguridad de la Información con la información brindada. • Informa al Jefe de la Unidad de Ciberseguridad en caso de ser necesario, para el seguimiento de los riesgos de la Seguridad de la Información. • Elabora un informe detallando los riesgos de la Seguridad de la Información de las áreas requeridas. • Presenta informe a Comité de Riesgos para su evaluación y validación para ser posteriormente remitidos a Junta directiva para su aprobación.

1. NOMBRE DEL PROCEDIMIENTO: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

	Gestor de la Seguridad de la Información/ Jefe de la Unidad de Riesgos.	HACER: • Para la ejecución de la Gestión de la Seguridad de la Información el Gestor de la Seguridad de información realiza lo siguiente: • Realiza diagnósticos de Seguridad de la Información en las diferentes áreas de la institución, mediante acciones de monitoreo y encuestas, documentando fallos encontrados en relación a la Seguridad de la Información, posteriormente comunica a la Jefatura de Ciberseguridad, y Elabora un plan de acción para el tratamiento de amenazas asociadas a la Seguridad de la Información. • Elabora un plan mediante el cual se dará tratamiento a los riesgos asociados a la Seguridad de la Información con sus respectivos controles, con el apoyo del Jefe de la Unidad de Riesgos, el cual será propuesto a Comité de Riesgos para su evaluación y validación y posteriormente ser remitido a Junta Directiva para su aprobación. • Comunica a las áreas correspondientes los controles a implementar.
4	Gestor de la Seguridad de la Información	MONITOREO Y REVISIÓN. • Revisa la efectividad del Sistema de Gestión de la Seguridad de la Información en las áreas donde se ha implementado garantizando dando seguimiento al cumplimiento de políticas y controles de la Seguridad de la Información.
5	Gestor de la Seguridad de la Información	ACTUAR: • Documenta las mejoras encontradas en el Sistema de Gestión de la Seguridad de la Información mediante un informe, y ejecuta un plan de acción que incluya acciones correctivas y preventivas; el cual se comunicará a las áreas correspondientes para para eliminar o mitigar fallos en la Seguridad de la Información.

UNIDAD DE RIESGOS inpêp JUNTA DIRECTIVA

GERENCIA inpêp

PRESIDENCIA inpêp

1. NOMBRE DEL PROCEDIMIENTO: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.		
6	Gestor de la Seguridad de la Información.	RESPUESTA A INCIDENTES: • Solicita información a las áreas requeridas sobre los incidentes relacionados a la Seguridad de la Información. • Verifica que los reportes de incidente presenten la información necesaria para la elaboración del informe técnico. • Presenta a Comité de Riesgos el informe realizado con sus respectivas acciones de respuesta para para su revisión y validación para posteriormente ser aprobado por Junta Directiva.
7	Gestor de la Seguridad de la Información	COMUNICACIÓN: • Comunica a Comité de Riesgos los aspectos relevantes de la Gestión de la Seguridad de la Información para una oportuna toma de decisiones. • Informa a la Alta Gerencia y Superintendencia del Sistema Financiero sobre los incidentes materializados de la Seguridad de la Información en la institución, mediante un informe técnico, considerando un máximo de 10 días calendario para su remisión y comunicación. • Desarrolla un programa de divulgación y capacitación de la Seguridad de la Información para todas las áreas de la institución según estructura organizativa.
8		Fin de proceso

Ambos procedimientos entrarán en vigencia a partir del 14 de diciembre de 2021.