PLAN DE TRATAMIENTO O GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - IFINORTE 2.022

Tabla de contenido

INTRODUCCION

El Instituto Financiero Para el Desarrollo de Norte de Santander IFINORTE entiende que existen amenazas significativas ante la posibilidad de la ocurrencia de un incidente o desastre que afecte la operación, como también la necesidad de recuperarse en el menor tiempo posible, garantizando la continuidad en el funcionamiento del instituto.

La realización de un análisis de los procesos que componen el Instituto en relación a la Seguridad y Privacidad de la Información servirá para priorizar qué procesos son críticos para el negocio y establecer una política de recuperación ante un desastre, definiendo un plan que permita continuar con la actividad empresarial en caso de una interrupción, para responder organizadamente a eventos que interrumpen la normal operación y que pueden generar impactos sensibles en el logro de los objetivos.

El Plan de Tratamiento o Gestión de Riesgos de Seguridad y Privacidad de la Información de IFINORTE es una herramienta que buscar reducir, mitigar y/o controlar el riesgo, reduciendo la no disponibilidad de los recursos necesarios para el normal desarrollo de las operaciones ofreciendo como elementos de control la prevención y atención de emergencias, administración de la crisis y capacidad de retorno a la operación normal.

1. OBJETIVOS

1.1 Objetivo general

Establecer un Plan de Tratamiento o Gestión de Riesgos de Seguridad y Privacidad de la Información del Instituto Financiero para el Desarrollo de Norte de Santander IFINORTE, que permita identificar y analizar cuáles podrían ser los riesgos que se pueden presentar dentro del Instituto y con base en esto se tomen las acciones y medidas necesarias que ayuden a mitigar las consecuencias y permitan la normal operación de la entidad.

1.2 Objetivos específicos

- ✓ Garantizar que IFINORTE esté preparado para responder a emergencias, recuperarse de ellas y mitigar los impactos ocasionados, permitiendo la continuidad de los servicios para la atención de sus clientes.
- ✓ Lograr un nivel de preparación frente a incidentes que permita garantizar la seguridad y privacidad de la información y bienes de la entidad en forma adecuada, realizando una buena administración de la crisis.
- ✓ Minimizar la frecuencia de interrupciones de la operación.
- ✓ Asegurar una pronta restauración de las operaciones afectadas por el evento.
- ✓ Minimizar las decisiones a tomar en caso de contingencia para evitar cometer errores.

2 PROPOSITO

El propósito del Plan de Tratamiento o Gestión de Riesgos de Seguridad y Privacidad de la Información de IFINORTE es permítele al Instituto continuar ofreciendo sus servicios cuando ocurra un desastre que provoque una interrupción de sus actividades en lo relacionado con el manejo de la información, minimizando de esta forma sus consecuencias.

A través del Plan de Tratamiento o Gestión de Riesgos de Seguridad y Privacidad de la Información se busca planificar las acciones necesarias a nivel informático y tecnológico para responder de forma adecuada ante un incidente de trabajo, desde el momento en que se declare la contingencia hasta la vuelta a la normalidad, de forma que se reduzca al mínimo su impacto sobre el negocio.

El Plan de Tratamiento o Gestión de Riesgos de Seguridad y Privacidad de la Información está orientado a la protección de la información, así como al restablecimiento oportuno de los procesos, servicios informáticos y tecnológicos críticos, frente a eventos de interrupción o desastre. Todo el personal de la Entidad debe estar entrenado y capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que le competen, mediante actividades periódicas de formación, divulgación y prueba del Plan de Tratamiento o Gestión de Riesgos de Seguridad y Privacidad de la Información.

El Plan de Tratamiento o Gestión de Riesgos de Seguridad y Privacidad de la Información debe mantenerse actualizado, para lo cual se deben desarrollar, probar y de ser necesario mejorar de forma periódica o ante cambios significativos en políticas, personas, procesos, tecnología; siendo necesario que en dicha revisión participen las áreas involucradas.

3 ALCANCE

Este Plan de Tratamiento o Gestión de Riesgos de Seguridad y Privacidad de la Información, se proyecta para poder continuar operando durante un incidente a nivel informático, incluye las acciones y procedimientos individuales, así como a los responsables de dar respuesta y recuperación de la operación normal de los servicios en el caso de presentarse un incidente externo que pudiera causar una interrupción de los servicios de cómputo por un tiempo prolongado, como un corte en el servicio de Comunicaciones o fallas en el suministro eléctrico.

4 PLAN DE RIESGOS EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Es responsabilidad del área de Sistemas de la Entidad el preparar y actualizar periódicamente el Plan de Riesgos en Seguridad y Privacidad de la Información previendo la continuidad de los procesos críticos para el Instituto en el evento de presentarse una interrupción o degradación del servicio a nivel tecnológico.

4.1 Análisis de Riesgos

El análisis de riesgos supone más que el hecho de observar la posibilidad de que ocurran cosas negativas. Se deben tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles, de esta forma se pueden priorizar los problemas y su costo potencial desarrollando un plan de acción adecuado, teniendo en cuenta la frecuencia con que puede ocurrir un desastre, nivel de daños y las consecuencias generales.

En la fase de evaluación de riesgos tecnológicos se debe priorizar, que se va a proteger y que situaciones se pueden enfrentar: fallas en el servidor, fallas en los dispositivos y equipos tecnológicos, eliminación accidental de archivos, virus, fallas eléctricas. Como también determinar el nivel de riesgo: bajo, muy bajo, medio, alto y muy alto.

Una vez presentada la contingencia o falla, se deberá ejecutar las siguientes actividades, planificadas previamente:

- ✓ Plan de Emergencias: En el cual se establecen las acciones a realizar cuando se presente una falla o contingencia, así como la coordinación y comunicación de las mismas. Es muy conveniente prever los posibles escenarios de ocurrencia de la contingencia, la cual se puede dar en horario diurno, como nocturno.

- ✓ Entrenamiento: Establecer un programa de prácticas periódicas de todo el personal de la institución frente a las diferentes contingencias informáticas y tecnológicas que se puedan presentar, de acuerdo a los roles que manejen dentro de la entidad.

Después de ocurrida la contingencia es necesario realizar:

- ✓ Evaluación de Daños: Inmediatamente después de concluida la contingencia, de deberá evaluar la magnitud del daño producido, equipos no funcionales, cuales se pueden recuperar y estimación del tiempo.

- ✓ Ejecución de Actividades: La recuperación y puesta en marcha del servicio afectado, se realizará en dos fases, la primera restablecer el servicio usando los recursos propios (Equipos de respaldo) y la segunda con el apoyo de proveedores y entes tanto gubernamentales como no gubernamentales.

- ✓ Evaluación de Resultados: Finalizada las fases de recuperación, se debe evaluar objetivamente las actividades realizadas, porcentaje de eficiencia y efectividad, tiempo, inconvenientes, colaboración y apoyo.

4.2 Elaboración del Mapa de Riesgo

Efectuar estudios de análisis de Riesgos de Seguridad y Privacidad de la Información para identificar oportunamente los eventos o situaciones de fallos en los accesos o en el manejo de la información presentados en la Entidad, estableciendo planes de acción que incluyan controles para contrarrestarlos y reducir el riesgo a un nivel aceptable.

5 NORMAS DE GESTIÓN DE EMERGENCIAS INFORMATICAS Y TECNOLOGICAS

5.1 Políticas de copias de seguridad de datos

Las políticas de copias de Seguridad de datos tienen como finalidad proteger adecuadamente los activos tecnológicos y la información resguardada en IFINORTE con el objetivo de asegurar su disponibilidad y mitigar los riesgos en caso de desastres.

Teniendo en cuenta que la información es quizás el activo intangible más importante del Instituto, las copias de seguridad son realizadas por:

- ✓ La empresa contratista proveedora del servicio de internet realiza una copia de seguridad de la información almacenada en los servidores con una frecuencia de 4 horas, en la nube de google drive.
- ✓ La empresa contratista del servicio del software institucional (OPE) realiza una copia de seguridad de las bases de datos cada hora.
- ✓ El área de las TIC´s de IFINORTE realiza una copia física en forma semanal.

5.2 Políticas Específicas

- ✓ Se realizarán copias de seguridad diarias de aquella información que IFINORTE actualiza frecuentemente, y son de alto valor para la institución.
- ✓ Se realizarán copias de seguridad física semanal de los servidores.
- ✓ Se conservarán al menos una semana la copia diaria, y al menos un mes la copia semanal. De esta forma, se va rotando el medio físico de almacenamiento
- ✓ Se conservará una copia de cada mes, al menos durante un año.
- ✓ Se conservará una copia del último mes de cada año como históricos.
- ✓ Se realizará cada seis meses simulación de recuperación de las copias de seguridad.
- ✓ En el caso de que no se puedan realizar los respaldos por algún problema con los Servidores (Virus o falla en unidad de almacenamiento) se procede a realizarlos una vez sea superada la falla.
- ✓ Todas las copias de seguridad serán etiquetadas con las siguientes especificaciones: tipo de copia (semanal, mensual, diaria).

- ✓ Se almacenarán las copias de seguridad mensuales en un lugar localizado fuera de las instalaciones de la institución, a través de una empresa especializada en seguridad que garantice la salvaguarda de la Información.

5.3 Políticas De Almacenamiento De Dispositivos Físicos

IFINORTE adopta un sitio para ubicar los recursos informáticos físicamente sólido, y protegido de accesos no autorizados, que cuente con las mejores condiciones climáticas lejos del calor, la humedad y la oxidación. Para el adecuado almacenamiento y conservación de los dispositivos, IFINORTE define como Responsable del proceso de supervisión de copias de seguridad, como garante de los datos digitales, al Ingeniero de Sistemas del Instituto, por tanto, debe hacer revisión periódica que permita detectar las fallas a las que podrían estar expuestos los dispositivos de almacenamiento de datos, e incluso de la verificación de que las copias se han realizado correctamente. También será el encargado de guardar las copias de seguridad en el compartimiento de seguridad del Instituto, ideado con el fin de que su apertura sea muy difícil a personas no autorizadas y de esta manera guardar todos los elementos de valor, esta caja de seguridad consta de un sistema de cierre que solo se puede abrir mediante clave secreta y están claves son cambiadas con frecuencia para garantizar y preservar más aun la seguridad, para que, en caso de que se produzca algún desastre como un incendio, los datos se encuentren protegidos y a su vez debe asegurarse que los dispositivos de almacenamiento cumplan con las siguientes condiciones mínimas para su conservación.

También se debe tener en cuenta:

- ✓ No exponer los discos al polvo.
- ✓ No tocar los discos con los dedos en el área del surco, se deben tomar por los bordes o por la etiqueta.
- ✓ No exponerlos por tiempos largos a la luz directa del sol o artificial, devuélvalos a su respectivo empaque lo más rápido posible.
- ✓ No guardar juntos discos de diferentes tamaños.
- ✓ Guardar los discos en ambientes a temperatura constante, si los va a guardar por largo tiempo trate de colocarlos en un ambiente fresco y oscuro.
- ✓ En caso de tener que aplicar una limpieza rápida a la cara de datos, se hace desde el centro del disco hacia afuera. Nunca limpiar moviendo en círculos, pues las rayas de desgaste que pudieran producirse tienen más posibilidades de estropear el proceso de lectura.
- ✓ No colocar pegatinas en la superficie del disco.

- ✓ Al marcarlos usar un rotulador de punta suave. Los objetos puntiagudos pueden dañar los datos. No se deben exponer al agua, a las caídas ni los golpes.

5.4 Procedimientos De Almacenamiento Externo

IFINORTE, realizo un contrato de servicios de almacenamiento con una entidad privada, independiente y plenamente asegurada, para la salvaguarda y conservación total de la Información considerada de mayor valor para el Instituto, como la opción más segura para el almacenaje de datos en forma virtual, donde los datos son guardados en la nube y de forma física, por medio de otro servidor alternativo que se encuentra ubicado en una locación externa.

5.5 Interrupción prolongada de electricidad.

En el caso de falta de energía eléctrica en todo el Instituto por un periodo mayor de 24 horas se recomienda suplir la energía eléctrica mediante sus sistemas de emergencia (UPS y generador). En sus instalaciones, se habilitarán espacios de trabajo temporales para realizar las funciones esenciales.

Actualmente los equipos están conectados a la UPS y éste a su vez está conectado al generador de electricidad para IFINORTE. La UPS nos permite hasta 15 minutos de funcionamiento en lo que se activa el generador. De haber problemas con la activación del generador se hará lo siguiente: El Subgerente Financiero o persona encargada solicitará información al Ingeniero de Sistemas de IFINORTE sobre la falla, Se evaluará la situación y de ésta prolongarse se tomará la decisión de moverse a otras instalaciones mientras se retoma el normal desarrollo de las actividades.