SICHF

Plan de Respaldo de datos

Samuel tejero

Sofia linares

Página de control de revisiones

Fecha	Resumen de cambios realizados	Cambios realizados por (Nombres y Apellidos)

Propósito

El propósito de este plan de respaldo de datos es garantizar que sichf pueda respaldar de manera segura datos, sistemas, bases de datos y otra tecnología de misión crítica para que estén disponibles en caso de una interrupción que afecte las operaciones comerciales. Se espera que todas las ubicaciones de sichf implementen medidas de respaldo de datos siempre que sea posible para minimizar las interrupciones operativas y recuperarse lo más rápido posible cuando ocurre un incidente.

El plan abarca operaciones de respaldo de datos de sichf en todas las ubicaciones.

Alcance

El alcance de este plan se limita a las actividades de respaldo de datos y no es un documento de procedimientos de resolución de problemas diarios.

Objetivos del plan

Sirve como guía para los equipos de respaldo de datos de TI de sichf
• Referencias y puntos a la (s) ubicación (es) de los datos, sistemas, aplicaciones y otros recursos de datos de misión crítica respaldados
• Proporciona procedimientos y recursos necesarios para realizar copias de seguridad de datos, sistemas y otros recursos.
• Identifica proveedores y clientes que deben ser notificados en caso de una interrupción que pueda requerir la recuperación de datos respaldados y otros recursos.
• Minimiza las interrupciones operativas al documentar, probar y revisar los procedimientos de respaldo de datos.
• Identifica fuentes alternativas para actividades de respaldo de datos
• Documenta el almacenamiento de datos, las copias de seguridad y los procedimientos de recuperación de registros vitales y otros datos relevantes.

Supuestos

• Los empleados clave de respaldo de datos de TI (por ejemplo, administrador principal de respaldo de datos, líderes de equipo, técnicos y suplentes) estarán disponibles luego de un desastre.
• Este plan y los documentos relacionados se almacenan en un lugar seguro fuera del sitio y no solo sobrevivieron al desastre, sino que son accesibles inmediatamente después del desastre.
• La organización de TI tendrá planes de recuperación ante desastres (DR) de tecnología que se alineen con este plan de respaldo de datos.

Definición de desastre

Un desastre es cualquier evento catastrófico o disruptivo (por ejemplo, corte de energía, clima, desastre natural, vandalismo) que causa una interrupción en la tecnología relacionada con datos, bases de datos, sistemas, datos archivados y otros recursos proporcionados por las operaciones de TI de sichf.
Copia de seguridad de datos y equipos relacionados
• Equipo de respaldo de datos
• Equipo de soporte técnico de TI
Consulte el Apéndice A para obtener detalles sobre las funciones y responsabilidades de cada equipo.

Responsabilidades de los miembros del equipo

• Cada miembro del equipo designará un suplente / suplente.
Todos los miembros del equipo deben mantener una lista de contactos actualizada de los números de teléfono del trabajo, del hogar y del celular de los miembros del equipo, tanto en el hogar como en el trabajo.
• Todos los miembros del equipo deben mantener este plan como referencia en casa en caso de que ocurra una interrupción después del horario normal de trabajo.
• Todos los miembros del equipo deben familiarizarse con el contenido de este plan.

Política de respaldo

Las copias de seguridad completas e incrementales protegen y preservan la información de la red corporativa y deben realizarse con regularidad para los registros del sistema y los documentos técnicos que no se reemplazan fácilmente, tienen un alto costo de reemplazo o se consideran críticos. Los medios de respaldo deben almacenarse en un lugar seguro, geográficamente separado del original y aislado de los peligros ambientales. Los componentes de la red de respaldo, el cableado y los conectores, las fuentes de alimentación, las piezas de repuesto y la documentación relevante deben almacenarse en un área segura en el sitio, así como en otras ubicaciones corporativas.
Las políticas de retención de datos y documentos se establecen para especificar qué registros deben conservarse y durante cuánto tiempo. Todos los departamentos son responsables de especificar su gestión de datos, retención de datos, destrucción de datos y requisitos generales de gestión de registros. El soporte técnico de TI sigue estos estándares para la copia de seguridad y el archivo de datos:

Bases de datos del sistema

Se debe realizar una copia de las bases de datos de misión crítica más actualizadas al menos dos veces al mes, o según la frecuencia de los cambios realizados.
• Las copias de seguridad deben almacenarse fuera del sitio.
• El administrador de datos principal es responsable de esta actividad.

Datos de misión crítica

Los datos y bases de datos de misión crítica actuales deben respaldarse de acuerdo con los objetivos de punto de recuperación (RPO) establecidos, y deben reflejarse o replicarse para asegurar ubicaciones de respaldo dentro de los plazos de RPO.
• Las copias de seguridad deben almacenarse fuera del sitio en una o más ubicaciones seguras en la nube o en oficinas o centros de datos alternativos de la empresa, o una combinación de estos.
• El administrador de datos principal es responsable de esta actividad.

Datos que no son de misión crítica

Los datos y bases de datos actuales que no son de misión crítica deben respaldarse de acuerdo con los RPO establecidos, y pueden duplicarse o replicarse en ubicaciones seguras de respaldo dentro de los plazos de RPO.
• Alternativamente, se deben realizar copias de los datos y bases de datos actuales al menos dos veces por semana, o según las métricas de RPO o la frecuencia de los cambios realizados.
• Las copias de seguridad se pueden almacenar en el sitio en instalaciones de almacenamiento seguras, o se pueden almacenar fuera del sitio en una o más ubicaciones seguras en la nube o en centros de datos u oficinas alternativos de la empresa, o una combinación de estos.
• El equipo de administración de datos es el responsable de esta actividad.
Los medios de respaldo se almacenan en ubicaciones que son seguras, aisladas de los peligros ambientales y geográficamente separados de la ubicación que alberga los componentes de la red.

Procedimientos de almacenamiento fuera del sitio

Las cintas, discos y otros medios adecuados se almacenan en instalaciones ambientalmente seguras.
• La rotación de cintas o discos se produce en un horario regular coordinado con el proveedor de Almacenamiento.

Realización de copias de seguridad de datos

Las copias de seguridad de datos se programarán diaria, semanal y mensualmente, según la naturaleza de la copia de seguridad. Los administradores de datos deben utilizar la tecnología de respaldo de datos aprobada para preparar, programar, ejecutar y verificar respaldos. Las copias de seguridad se pueden realizar en recursos de almacenamiento local (por ejemplo, USB, github, disco local, nube) localmente o en ubicaciones seguras fuera del sitio (por ejemplo, proveedores de servicios de copia de seguridad de

datos en la nube, proveedores de copia de seguridad como servicio) aprobados por la administración de TI.

Actividades de la copia de seguridad de datos
La siguiente tabla enumera las actividades de respaldo de datos que se realizarán de manera programada regularmente.

	Acción	Responsable(s)
1.	Revisar el programa con la gerencia de TI; aprobaciones seguras según sea necesario.	Administrador principal de respaldo de datos, Jefe de Operaciones de TI.
2.	Identificar y categorizar los datos que se respaldarán.	Administrador de respaldo principal; equipo de respaldo.
3.	Identificar y categorizar los sistemas que se respaldarán.	Administrador de respaldo principal; equipo de respaldo.
4.	Identificar y categorizar otros recursos para respaldar.	Administrador de respaldo principal; equipo de respaldo.
5.	Programe actividades de respaldo, por ejemplo, fecha, hora, frecuencia, tipo de recurso para respaldar, destino para respaldos.	Administrador de respaldo principal; equipo de respaldo.
6.	Programe los sistemas y recursos de respaldo de acuerdo con el cronograma y la política.	Administrador de respaldo principal; equipo de respaldo.
7.	Programe actividades de rotación y copia de seguridad en medios magnéticos.	Administrador de respaldo principal; equipo de respaldo.
8.	Ejecute copias de seguridad de datos, sistemas y otros recursos.	Administrador de respaldo principal; equipo de respaldo.
9.	Asegúrese de que los medios magnéticos estén asegurados para su recogida y estén debidamente etiquetadas; verificar recogida.	Administrador de respaldo principal; equipo de respaldo.
10.	Verifique que las copias de seguridad se hayan completado y que todos los recursos de la copia de seguridad no hayan cambiado.	Administrador de respaldo principal; equipo de respaldo.
11.	Preparar y distribuir informes de respaldo.	Administrador de respaldo principal; equipo de respaldo.
12.	Programar y realizar pruebas de copias de seguridad de datos.	Administrador de respaldo principal; equipo de respaldo.
13.	Programar y aplicar parches a los recursos de respaldo.	Administrador de respaldo principal; equipo de respaldo.
14.	Actualice los sistemas y tecnologías de respaldo según sea necesario.	Administrador de respaldo principal; equipo de respaldo.

Recuperación de datos

Se deben establecer, documentar y probar periódicamente procedimientos para recuperar datos, bases de datos, sistemas, aplicaciones y otros activos de información si ocurre un evento disruptivo que requiera la recuperación de esos activos y recursos.

Revisión y mantenimiento del plan

Este plan de copia de seguridad de datos debe revisarse periódicamente y los procedimientos deben validarse (y actualizarse según sea necesario) para garantizar que las copias de seguridad se realicen según sea necesario y cuando sea necesario. Como parte de esta actividad, es recomendable revisar las listas del personal del equipo de respaldo de datos, proveedores de servicios de respaldo de datos y proveedores de respaldo de datos en la nube, y actualizar los datos de contacto según sea necesario. La versión impresa de este plan de respaldo de datos se almacenará en una ubicación común donde el personal de TI, como los administradores de datos, pueda verlo. Las versiones electrónicas estarán disponibles a través del Soporte técnico de TI.

Apéndices

Apéndice A: Equipos

Equipo de respaldo de datos
Actividades de apoyo

Equipo de soporte técnico de TI (ITS)

Actividades de apoyo

Apéndice B: Listas de contactos del equipo de respaldo de datos

Equipo de respaldo de datos (EBD)

Empresa/Nombres y Apellidos	Contacto	Dirección Domicilio	Numero de Celular/Fijo

Equipo de soporte técnico de TI (EST)

Empresa /Nombres y Apellidos	Contacto	Dirección Domicilio	Numero de Celular/Fijo

Apéndice C: Lista de contactos de proveedores aprobados

Empresa	Contacto (Nombres y Apellidos)	Dirección Domicilio	Numero de Celular/Fijo
Proveedor de respaldo 1			
Proveedor de respaldo 2			
Proveedor de respaldo 3			

Apéndice D: Ubicaciones de respaldo de datos

Recurso de copia de seguridad 1 – <Nombre de la ubicación>

Primaria: Dirección
Teléfono
Ciudad, Localidad, Estado, Barrio
Nombres y Apellidos de Contacto

Alternativa Dirección
Teléfono
Ciudad, Localidad, Estado, Barrio
Nombres y Apellidos de Contacto

Recurso de copia de seguridad 2 – <Nombre de la ubicación>

Primaria: Dirección
Teléfono
Ciudad, Localidad, Estado, Barrio
Nombres y Apellidos de Contacto

Alternativa Dirección
Teléfono
Ciudad, Localidad, Estado, Barrio
Nombres y Apellidos de Contacto

Instalaciones de almacenamiento de datos (por ejemplo, USB, disco, nubes, NAS, SAN, RAID)

Nombre de la Empresa	Contacto (Nombres y Apellidos)	Dirección Domicilio	Numero de Celular/Fijo

Apéndice E: Inventario de recursos de datos, bases de datos para respaldar

Proporcionar una lista de recursos

Apéndice F: Inventario de hardware y software para realizar copias de seguridad

Proporcionar una lista de recursos

Apéndice G: Inventario de equipos y servicios de red para respaldar

Proporcionar una lista de recursos