Políticas de Seguridad de la Información

Medical Solutions Colombia S.A.

1. Objetivos

Los objetivos de esta Política de Seguridad de la información son establecer las políticas, prácticas y lineamientos internos de Seguridad de la Información para Medical Solutions Colombia SAcon el fin de asegurar la protección de los activos de información en todas sus formas y medios contra su modificación accidental o deliberada, utilización no autorizada, divulgación o interrupción, de modo de garantizar su confidencialidad, integridad y disponibilidad.

Medical Solutions Colombia SAestablece que ante cualquier presentación legal que se requiera y esté relacionado con los sistemas informáticos o los usuarios internos, se observarán las leyes vigentes mediante el asesoramiento legal respectivo para asegurar los requisitos regulatorios que apliquen.

2. Alcance

Este documento se deberá aplicar en todas las fases del ciclo de vida de la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y de los sistemas que la procesan (análisis, diseño, desarrollo, implementación, explotación y mantenimiento).

Aplica a todos los sectores de Medical Solutions SpA, es decir, a todo el personal, tanto interno como externo; así como a las personas que directa o indirectamente, prestan sus servicios profesionales dentro de la misma y a toda la información obtenida, creada, procesada, almacenada o intercambiada dentro y desde la Compañía.

3. Definiciones

Incidencia: Un único evento o serie de eventos de seguridad de la información inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.
Contingencia: Acción correctiva frente a una incidencia.

Procedimiento: Normas y/o pasos predefinidos para actuar frente a una situación, normalmente establecido mediante políticas internas.
Plan: Hace referencia a este documento en general y lo que afecta.

4. Vigencia

Este plan entrará en vigencia a partir del día 25 de Agosto de 2022

5. Responsabilidades

A continuación se describen los cargos de los responsables y sus roles respecto a Seguridad de Información:

Cargo	Responsabilidad
CM Chile & COO	Tomar decisiones respectos políticas y curso de acción frente a incidencias de Medical Solutions SpA
CMO	Administración de las relaciones con clientes de Medical Solutions Colombia SAy la información asociada
Controller	Responsable operacional y del área de finanzas con participación en la implementación de las políticas de seguridad de la información
DO Manager	Administrar todos los proyectos de servicio y operación médica y los procesos de ingreso, documentación, , administración de turnos y pagos del personal médico.
Operations Manager	Administrar personal médico y su disponibilidad
Project & Dev Manager	Responsable del área técnica, lo que incluye pero no se limita al desarrollo y mantención de la plataforma
Digital Health Director	Administrar al equipo médico en conjunto con todos los procesos y protocolos internos y normativos/legales para la correcta prestación telemedicina.
OSI	Asesorar en temas de seguridad de información, lo que incluye leyes de protección de datos y las mejores prácticas
CM México	Tomar acciones derivadas de las decisiones tomadas por el CM de Chile respectos políticas y curso de acción frente a incidencias de Medical Solutions Colombia SAen México

CM Colombia	Tomar acciones derivadas de las decisiones tomadas por el CM de Chile respectos políticas y curso de acción frente a incidencias de Medical Solutions Colombia SAen Colombia

6. Autoridad de emisión, revisión y publicación

Esta Política fue confeccionada en base a los requerimientos de Medical Solutions Colombia SAy ha sido aprobada por el Comité de Seguridad de la Información, acordando que se revisará de manera anual a partir de la fecha de vigencia.

Éste documento y los que se generen de él, deberán ser publicados y comunicados a toda la compañía y a todos los niveles de la organización.

7. Reglas de aplicación

7.1. Designación de un Oficial de Seguridad de Información

El OSI u Oficial de Seguridad de Información es designado por sus cualidades profesionales y conocimiento específico en leyes y prácticas de protección de datos.

La empresa debe asegurar y proveer al área de seguridad de información con todos los recursos apropiados para realizar sus labores y mantener su conocimiento a un nivel de experto en la materia.

El OSI reporta directamente al nivel más alto de la gerencia y no tiene otras responsabilidades que resulten en un conflicto de intereses.

7.2. Gestión de Activos y Clasificación de la Información

La Gestión de Activos y Clasificación de la Información tiene como objetivo garantizar que los activos, constituidos por información y los recursos que le dan soporte, sean identificados, inventariados y clasificados en función de los requerimientos del negocio.

El Comité de Seguridad de la Información debe establecer los procesos y procedimientos necesarios para una adecuada gestión de activos de acuerdo con las necesidades del negocio, los cuales deberán asegurar:

- La identificación y el mantenimiento del inventario de activos de Información.
- Establecer los mecanismos para la designación de Propietarios de Activos de Información.

- Establecer los criterios de clasificación de la información en función de las dimensiones de confidencialidad, integridad y disponibilidad, de acuerdo con el nivel de criticidad que la información tenga para el negocio.
- Establecer los procedimientos necesarios para la clasificación de la información y todos los activos de información que le dan soporte.
- Establecer los niveles mínimos de tratamiento de seguridad que deberá dar a la información de acuerdo con el nivel de clasificación de confidencialidad asignada, en términos de su ciclo de vida, generación, transmisión, utilización, almacenamiento y destrucción.
- Los Propietarios de los Activos de Información deberán identificar, categorizar, modificar y dar de baja los activos de información en el inventario; como así también, determinar la clasificación de la información bajo su responsabilidad, en función de los criterios definidos por el Comité de Seguridad de Información.

Sólo se clasifica información que sea estrictamente necesaria para el funcionamiento de la empresa. También se limitan los accesos a los datos sólo para aquellos que lo requieran en el desempeño de sus tareas. La información se divide en categorías, para asegurar que está protegida de forma adecuada y que se están asignando los recursos de seguridad de forma pertinente.

No clasificado: Es información que se puede hacer pública, sin que implique consecuencias negativas para la empresa, como es la información que es de conocimiento público.

Confidencial de los empleados: Esto incluye información como ficha con los datos personales de los colaboradores, registros médicos, liquidación de remuneraciones, entre otros.

Confidencial de la compañía: Como contratos, códigos fuente, contraseñas para sistemas críticos de TI, contratos de clientes, cuentas, etc.

Confidencial del cliente: Esto incluye información de identificación como nombre, dirección, claves de acceso al sistema de clientes, acuerdos comerciales, planes de negocio, información de nuevos productos, información sensible del mercado, etc.

Hemos categorizado la información que tenemos en la siguiente tabla:

Tipo de Información	Sistemas Involucrados	Nivel de clasificación	Propietario de la Información
Registro de clientes de Medismart	Enroll Medismart	Confidencial de la compañía	Project & Dev Manager
Operación médica	Plataforma Medismart	Confidencial de la compañía	Operations Manager
Ficha clínica e información médica	Plataforma Medismart	Confidencial de los clientes	Digital Health Director
Contratos de	Google Drive	Confidencial de la	CMO

clientes		compañía	
Información contable de Medismart	SAP Business	Confidencial de la compañía	Controller
Repositorio de servicios web y enroll	Atlassian Bitbucket	Confidencial de la compañía	Project & Dev Manager
Repositorio de plataforma	Gitlab	Confidencial de la compañía	Project & Dev Manager
Registro de actividades internas	Google Suite	Confidencial de la compañía	Project & Dev Manager
Registro de clientes	Hubspot	Confidencial de la compañía	CMO
Registro de personal médico	Plataforma Medismart	Confidencial de la compañía	Operations Manager
Registro de personal operacional (no médico)	Google Suite	Confidencial de los empleados	DO Manager
Registro de atención al cliente	Adere.so	Confidencial de la compañía	CMO

7.3. Gestión de Riesgos

La Gestión de Riesgos tiene como objetivo ayudar a identificar y medir posibles eventos de pérdida (operativa y tecnológica) futuros y a establecer y priorizar planes de tratamiento sobre los riesgos que desafían sus objetivos estratégicos y prácticas operativas cotidianas de la empresa.

Ayudar al Comité de Seguridad de Información a identificar y medir amenazas y vulnerabilidades que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información de la Compañía, en especial aquella más crítica para el desarrollo confiable e ininterrumpido de sus actividades; como así también, establecer y priorizar los planes de tratamiento para reducir riesgos.

El CTO o Project & Dev Manager deberá establecer un proceso formal que permita a la Alta Gerencia:

- Identificar los riesgos estratégicos que pueden afectar negativamente al logro de los objetivos estratégicos de la Compañía.
- Definir y aprobar el alcance del proceso de gestión de riesgos y las modificaciones eventuales al mismo.
- Definir el umbral de tolerancia y aceptación de riesgos de la organización.
- Aprobar el nivel de riesgo residual de la organización.

- Identificar activos críticos, amenazas y vulnerabilidades.
- Establecer los criterios de evaluación y medición de riesgos.
- Definir la planificación de los análisis de riesgos.

El análisis y evaluación de riesgos se realizará, como mínimo, una vez al año o cuando ocurran cambios significativos en el entorno, lo que suceda primero.

7.4. Gestión de Accesos y Perfiles

La Gestión de Accesos y Perfiles tiene como objetivo establecer los lineamientos para un adecuado control de los usuarios y perfiles utilizados por el personal de la Compañía o terceros que accedan a los activos informáticos.

Internamente, en la medida de lo posible, operamos bajo la política de la "necesidad de compartir" y no la "necesidad de saber", esto es con respecto a la información confidencial de la empresa. Esto significa que nuestra parcialidad e intención es compartir la información para ayudar a la gente a realizar su trabajo y no para aumentar innecesariamente las barreras de acceso a la información.

En cuanto a la información del cliente, operamos bajo "El derecho de acceso" de GDPR. Esto hace referencia al derecho de los dueños de la información a confirmar el procesamiento de sus datos, donde se procesa y con qué propósito. De forma adicional, tenemos que proporcionar, si es que nos solicitan, una copia de sus datos personales, sin cobrar por ello y en un formato electrónico.

Se permite que los interesados transmitan sus propios datos a otros controladores.

Adicionalmente, los privilegios de administrador de los sistemas de la empresa son restringidos a individuos específicos y autorizados, para las siguientes funciones que le permiten desarrollar su trabajo de forma correcta. Esta información se encuentra en la "Matriz de control de accesos" de la compañía.

Como medidas de precaución para la preservación de la información se adopta los siguientes lineamientos:

- Todo usuario de sistemas o plataformas tecnológicas está asociado a una persona física de manera unívoca y en los casos que se requiera la utilización de usuarios genéricos, estos tengan un responsable asociado.
- Se establece una gestión de las altas y asignación de credenciales de usuarios considerando la identificación de los mismos y las autorizaciones necesarias para su gestión.
- Ante un cambio de funciones se eliminan los accesos relacionados con la función anterior y se asignan los accesos necesarios para la nueva función.
- Toda desvinculación de personal implica el retiro de los accesos otorgados y/o la eliminación o inhabilitación de los ID de usuarios asociados a la persona.
- Se asegura la adecuada segregación de funciones evitando la asignación de permisos incompatibles con las funciones de los usuarios.

- La generación/acceso a los usuarios de privilegios especiales en los sistemas y plataformas se encuentre limitado a personal debidamente identificado y bajo una adecuada justificación de necesidad, como así también que su utilización sea monitoreada y controlada.
- Implementación de una adecuada custodia de las credenciales de usuarios de privilegios especiales y usuarios genéricos que asegure la identificación del personal que las utilice y el registro de la justificación para su utilización.
- En vistas de mantener la asignación de manera correcta, se realiza la revisión de derechos de accesos, la cual está a cargo del CTO o del Project & Dev Manager.

7.5. Gestión de Seguridad de Entornos, Plataformas y Aplicaciones

La Gestión de seguridad de entornos, plataformas y aplicaciones tiene como objetivo establecer los lineamientos para la definición, implementación y control de una adecuada seguridad en todos los entornos y plataformas que soportan los servicios de negocio.

Para proteger los datos, sistemas, usuarios y clientes se usan los siguientes sistemas:

1	**Anti-malware sugerido para computadoras portátiles y de escritorio**			
	Prestador	Windows Defender	**Validez**	Indefinido
2	**Email spam, malware y filtrado de contenido alojados en la nube**			
	Prestador	GSuite Business	**Validez**	Indefinido
3	**Archivos y continuidad de correos electrónicos**			
	Prestador	GSuite Business	**Validez**	Indefinido

Dada la naturaleza de la plataforma, los sistemas que la soportan recurren a medios de protección propios, los que en conjunto otorgan protección al servicio. Los principales sistemas utilizados con medios de protección son:

- Azure
- Google Suite
- Vonage
- Medipass
- Vultr

Adicionalmente, se desarrollan estándares que deberán contemplar como mínimo las definiciones necesarias para las siguientes categorías de entornos, plataformas, sistemas o aplicativos:

- Sistemas operativos.
- Redes y dispositivos de Red.
- Estaciones de trabajo y dispositivos móviles.
- Sistemas de almacenamiento.
- Sistemas de virtualización.
- Bases de datos.
- Correo electrónico e internet.
- Aplicaciones en general.
- Aplicaciones web.
- Soluciones de seguridad.

Todo cambio de arquitectura, infraestructura o definiciones de seguridad deben ser acordados con el Comité de Seguridad de Información a fin de no generar problemas de seguridad.

Es por esto, que se deben considerar los siguientes lineamientos:

Gestión de la seguridad de redes

- Las redes deben gestionarse y controlarse adecuadamente para proteger la información en los sistemas y aplicaciones.
- Restringir las conexiones entre redes no confiables y cualquier componente del sistema en los entornos críticos.
- Se prohíbe el acceso público directo entre Internet y todo componente del sistema en los entornos críticos.
- Las políticas y los procedimientos operativos para administrar los equipos de red deben estar documentados, implementados y ser de conocimiento para todas las partes afectadas.

Intercambio de información con partes externas

- Medical Solutions Colombia SAdebe implementar políticas, procedimientos y controles formales para proteger el intercambio de información por medio del uso de cualquier tipo de recurso de comunicación, en coherencia con las políticas de clasificación de los activos de Información.

7.6. Gestión de Vulnerabilidades

La Gestión de Vulnerabilidades tiene como objetivo detectar las exposiciones de posibles vulnerabilidades que puedan encontrar y aprovechar personas malintencionadas. Una correcta ejecución y detección temprana ayuda a reducir el riesgo de exposición.

Dado esto, se dictamina lo siguiente:

- Se realizará Ethical Hacking 2 veces al año (cada 6 meses), un proceso que tiene como objetivo llevar a cabo la revisión de vulnerabilidades mediante pruebas en ambientes controlados, ya sea de forma interna o contratando los servicios de empresas externas capacitadas para llevar a cabo este proceso de forma segura.

- Se debe establecer un proceso formal de gestión de vulnerabilidades que contemple:

    a. La realización periódica de escaneos de vulnerabilidades y pruebas de intrusión.
    b. La verificación periódica de la publicación de vulnerabilidades por parte de los fabricantes de tecnología.
    c. Se definan plazos para reaccionar ante las notificaciones de vulnerabilidades técnicas potencialmente relevantes de resolución que contemple, como máximo, 1 mes.
    d. El análisis de aplicabilidad de las vulnerabilidades detectadas o identificadas y la definición de su remediación.
    e. Generación de un plan de remediación con plazos establecidos y su seguimiento.

7.7. Gestión de Incidentes (de seguridad)

La Gestión de Incidentes tiene como objetivo establecer lineamientos para un adecuado registro, análisis y tratamiento de los incidentes de seguridad que puedan afectar a la compañía.

Por tal, se considera lo siguiente:

- Se debe registrar, analizar y definir mitigantes, si correspondiera, para todo incidente de seguridad reportado o detectado.
- Todo el personal debe informar al área de Seguridad de la Información todo evento que pueda considerarse un incidente de seguridad.
- El área de Seguridad de la Información debe establecer un proceso formal de gestión de incidentes de seguridad que permita un adecuado registro de los mismos, su priorización, análisis y seguimiento hasta su cierre.
- Ante un incidente detectado, existe un equipo experto en remediar los mismos, así como otras vulnerabilidades detectadas.
- También, se debe analizar los incidentes de seguridad ocurridos, el impacto ocasionado, su frecuencia y forma de resolución aplicada, con el objeto de tener estadísticas de comportamiento de respuesta ante incidentes, aprender de lo ocurrido y establecer mejoras en las acciones de control y las políticas cuando sea necesario.

- Tener en cuenta los incidentes ocurridos en los futuros planes de concientización y capacitación.

7.8. Gestión del Ciclo de Vida, Puesta en Producción y Entornos

La Gestión del ciclo de vida, puesta en producción y entornos tiene como objetivo establecer los lineamientos para un adecuado control de los cambios, la puesta en producción y la segregación de ambientes.

Se debe establecer, documentar e implementar un proceso formal para el control de los cambios en producción y el pasaje de desarrollos al ambiente productivo, este proceso deberá contemplar:

- Autorizar la instalación de todo nuevo producto o modificaciones a sistemas aplicativos.
- Verificar que se hayan cumplido con todos los puntos de control existentes para los desarrollos/mantenimientos/adquisiciones de sistemas aplicativos de acuerdo con las metodologías de desarrollo, mantenimiento y adquisición de la compañía.
- Minimizar la posibilidad de modificaciones a los sistemas de aplicación durante los procesos de control y una vez aprobados e instalados en producción.
- Llevar un registro de todas las instalaciones efectuadas en el ambiente de producción. En la misma se debe indicar, mínimamente, fecha, hora, ambiente de procesamiento, identificación, activo de información y responsable interviniente.
- La seguridad correspondiente a todo nuevo desarrollo/modificación se debe adecuar a lo establecido por las normas y estándares de seguridad definidos.
- Establecer un procedimiento de emergencia para dejar sin efecto en forma rápida los cambios efectuados y poder recuperar las versiones autorizadas anteriormente en el caso de generarse problemas no solucionables durante la instalación y período de control que afecten a la continuidad operativa.
- Las aplicaciones existentes en el ambiente de producción deben estar debidamente documentadas.
- Los ambientes están segregados en entornos de desarrollo, testing y producción.

7.9. Gestión de Capital Humano

El área responsable de RRHH, en este caso el área de “People & Clients”, debe establecer todos los lineamientos y procesos necesarios para asegurar la gestión de la seguridad relacionada con la incorporación, permanencia y desvinculación del personal que realizará tareas como colaborador de la Compañía, debiendo tener en cuenta los siguientes requerimientos:

- Formalización de los roles y responsabilidades de cada puesto dentro de la compañía, mediante los cuales se realizará una evaluación de idoneidad y aplicabilidad del personal a incorporar en colaboración con la jefatura asociada.

- Aceptación por parte del colaborador de los términos y condiciones de contratación y las políticas y Normas de Seguridad de la compañía que debe cumplir.
- Formalización de un compromiso de confidencialidad y lealtad de acuerdo con lo que se establece en este documento.
- Formalización de un proceso para la desvinculación del colaborador considerando que permita un adecuado retiro y/o devolución de todos los activos provistos por la compañía y el retiro de todos los privilegios de acceso a los sistemas informáticos o físicos.
- Inducción a los colaboradores (internos y/o externos) sobre temas específicos de Seguridad de la Información. En caso de no brindar inducción o capacitación directa al colaborador externo, se debe exigir lo mismo a la empresa tercerizadora de personal.
- Formalización del código de conducta de la organización donde se detallen los valores, pautas y conductas que los colaboradores (internos y/o externos) deben respetar.
- Todos los empleados de la organización deben al menos una vez al año hacer una declaración de que leyeron y entendieron las políticas de Seguridad de la Información.
- Realizar un plan anual de capacitación y concientización sobre Seguridad de la información para colaboradores (internos y/o externos).

Se realiza entrenamiento a todo el personal de Medical Solutions SpA, lo que incluye a las nuevas incorporaciones, y se entrega apoyo al personal existente para implementar esta política. Esto incluye:

- Una introducción inicial a la seguridad TI, cobertura de riesgos, medidas básicas de seguridad, políticas de la compañía y dónde encontrar ayuda.
- Entrenar como se usan los sistemas de la empresa y los softwares de seguridad de forma apropiada.
- Si se requiere, una revisión de salud de seguridad en sus computadores, tablets o teléfonos previo al ingreso del empleado.

Teletrabajo

El apartado de teletrabajo tiene como objetivo establecer los lineamientos de trabajo remoto para una adecuada utilización de los activos de información de la compañía por parte de personal interno y externo.

Esto incluye:

- El suministro de equipo adecuado y mobiliario de almacenamiento para las actividades críticas que se realicen mediante teletrabajo, donde no se permite el uso de equipo de propiedad privada que no se encuentra bajo control de la organización.
- Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede realizar y los sistemas y servicios internos a los que el teletrabajador se encuentra autorizado a acceder.
- El suministro de equipo adecuado de comunicación, incluyendo los métodos para facilitar el acceso remoto seguro.

Sanciones

Puede ocurrir el caso en que personal interno, externo o proveedor incurra en alguna desviación o incumplimiento de esta política, lo cual puede ser motivo de sanciones administrativas e incluso legales que deben quedar explícitas en los contratos celebrados.

7.10. Gestión y Protección del uso de los dispositivos

La Gestión y protección del uso de los dispositivos tiene como objetivo establecer los lineamientos para una adecuada utilización de los activos de información de la compañía por parte de los usuarios incluyendo colaboradores, proveedores y terceros contratados.

Por lo que se toman las siguientes medidas:

- Remover softwares que no se usen o necesiten en los computadores.
- Actualizar el sistema operativo y aplicaciones de forma regular.
- Mantener el firewall del computador encendido.
- Para los usuarios de Windows, asegurar la instalación de un software anti-malware o utilizar Windows defender, y mantenerlo actualizado. Para usuarios Mac considerar usar un anti-malware.
- Guardar documentos en espacios de almacenamiento oficiales de la empresa para que estén respaldados de forma apropiada y disponibles ante cualquier emergencia.
- Mantener encendido el cifrado de disco.
- Tener cuentas separadas para otros usuarios como familiares, en el caso de que utilicen el computador que se utiliza para actividades de la Compañía. Idealmente, tener computadores separados para el trabajo y para uso de la familia u otros.
- No usar un administrador de cuentas en el computador de uso diario.
- Asegurar que el computador y teléfono cierren sesión después de 15 minutos y soliciten contraseña para volver a ingresar.
- No compartir bajo ningún concepto las credenciales de acceso a los diferentes sistemas, plataformas y aplicativos como así tampoco escribir las contraseñas en lugares donde otras personas puedan visualizarlas.
- No abandonar el puesto de trabajo sin antes desconectarse del sistema o de activar el salvapantallas con contraseña, de forma tal de impedir la utilización de los perfiles, por personal no autorizado.
- Proceder a cambiar la contraseña en forma inmediata cuando sospeche que se encuentra comprometida.

7.11. Gestión de Claves y Criptografía

La Gestión de Claves y Criptografía tiene como objetivo establecer lineamientos para garantizar una adecuada gestión de las claves (incluida su criptografía) de acuerdo a las

mejores prácticas de seguridad de la industria y a los requerimientos normativos que aplican a la compañía.

Por tal, se dictamina:

- Las contraseñas generadas por equipo deben poseer como mínimo una longitud de 8 caracteres y contener minúsculas , mayúsculas, números y símbolos. Un ejemplo de esto puede verse en el siguiente texto: "7_#{P>_[4M(5UpA\FpRuy>+5"
- Los integrantes del equipo no deben compartir contraseñas, si un miembro del equipo requiere un usuario y/o contraseña para acceder a un servicio, el mismo debe solicitarlo al Jefe de Área, el cual se encargará de darle los accesos solicitados.
- Evitar compartir credenciales en texto plano por medios no seguros (incluido medio impreso, escrito o grabado).
- No escribir PINs ni contraseñas al lado de computadores o teléfonos.

Adicionalmente se incentiva a todos los miembros de Medical Solutions Colombia SAa cumplir con las siguientes medidas de buenas prácticas:

- Cambiar las contraseñas de forma regular, cada 90 días.
- Se recomienda a los integrantes del equipo utilizar un gestor para generar y/o almacenar contraseñas de forma segura.
- Todas las aplicaciones utilizadas por el equipo deben ser configuradas con segundo factor de autenticación (2FA) y los códigos de Backup deben ser almacenados de forma segura en un gestor de contraseñas.
- No utilizar la misma contraseña para diferentes sistemas críticos.
- Considerar el uso de criptografía sólida en todos los aplicativos que estén sometidos a normativas que regulan el negocio.

7.12. Gestión de Respaldo, Recuperación y Continuidad

La Gestión de Respaldo, Recuperación y Continuidad tiene como objetivo establecer lineamientos tendientes a la preservación de los datos, operatoria y poder asegurar la continuidad del negocio.

Para esto, es necesario:

- Asegurar un inventario de los soportes de resguardo existentes, su contenido y lugar de almacenamiento, así como también fijar los responsables de mantener esos inventarios y mantener una copia actualizada del mismo en una locación remota.
- Realizar pruebas periódicas de recuperación de información desde los soportes almacenados con el fin de asegurarse del adecuado funcionamiento de los procesos de generación de las copias y de la disponibilidad de la información en tiempo y forma.
- Realizar un análisis de riesgo para determinar cuáles son las amenazas y escenarios de desastre a las que se encuentran expuestos los procesos críticos, cuál es su probabilidad de ocurrencia y cuál es su impacto económico en caso que ocurra una contingencia.

- Establecer los medios para que todo el personal clave involucrado en el Plan de Recuperación de Datos o DRP por sus siglas en inglés (*Data Recovery Plan*) pueda ser contactado y ubicado en forma inmediata, como así también establecer los procedimientos de Comunicación de Crisis necesarios durante la contingencia y hasta que sea normalizada la operación.
- Definir, documentar, ejecutar y controlar un plan de pruebas anual para la evaluación de la eficiencia del plan de continuidad del negocio y la detección de mejoras a implementar y necesidades de capacitación.
- Elaborar, revisar, actualizar y documentar el BIA como fuente de información y respaldo a las decisiones del negocio relacionadas con nuestro alcance del plan de continuidad del negocio.

También, se consideran las respuestas a las potenciales interrupciones al negocio:

- Interrupción severa del transporte.
- Incapacidad de acceder a la oficina por inundaciones, fuego, desorden civil, incidentes terroristas, etc.
- Pérdida de internet y/o conexión telefónica.
- Pérdida o robo de sistemas críticos.

Los planes de contingencia se probarán, al menos, una vez al año.

7.13. Gestión de Cumplimiento

La Gestión de Cumplimiento tiene como objetivo establecer lineamientos tendientes a estar alineados con las diferentes regulaciones y normativas a las que la empresa esté sujeta.

Para esto, es necesario:

- Verificar que los acuerdos con clientes internos (empleados), clientes externos (clientes) y proveedores cumplan con las pautas de las regulaciones e incluyan aspectos relacionados a los riesgos de seguridad de información derivados del servicio prestado.
- Determinar puntos de control con los terceros subcontratados en cuanto al cumplimiento de las mejores prácticas y normativas.
- Establecer las políticas y procedimientos necesarios para establecer el marco de adherencia y control a las regulaciones.
- Llevar a cabo las revisiones de cumplimiento de seguridad de la información; se recomienda que de manera anual se realice el plan de auditoría por personal externo.
- De manera periódica realizar el plan de verificación de los sistemas de información, por medio de una evaluación donde se verifique que los mismos se encuentran configurados de acuerdo a las reglas y políticas definidas.

8. Versionado

Confeccionado por	Diego Álvarez
Código de documento	PSI.V7
Versión	V7
Fecha de última actualización	25/08/2022
Revisado por	CSI
Aprobado por	CSI