POLÍTICA DE TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN

COLABORADORES

Elaborado por:	Revisado por:	Aprobado por:
Victor Pesantes ***TÉCNICO EN DISEÑO***	***Fernando Hernandez*** ***INGENIERO DE SOPORTE***	***Ing. Pamela Loaiza*** ***GERENTE GENERAL***
Fecha: 06/01/2024	Fecha: 06/01/2024	Fecha: 06/01/2024

CONTROL DE CAMBIOS

VERSIÓN	DETALLE / CAMBIOS	FECHA DE APROBACIÓN
01	Emisión inicial	Fecha: 06/01/2024

ÍNDICE

1. INTRODUCCIÓN

La política seguridad de la información es un documento que describe las reglas a seguir por parte de los miembros del Departamento de soporte técnico SPEED FIBER SPEEDFIBER.CIA.LTDA con el fin de asegurar confidencialidad, disponibilidad e integridad de los recursos tecnológicos.

2. OBJETIVO

Garantizar la seguridad de la información en la empresa SPEED FIBER SPEEDFIBER. CIA.LTDA

3. ALCANCE

Este documento es aplicable para todo el personal de SPEED FIBER SPEEDFIBER.CIA. LTDA. que tenga bajo su responsabilidad y resguardo sistemas de cómputo, programas (software), servicios informáticos (internet, correo electrónico, etc…).

4. POLÍTICA DE TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN

4.1. DEFINICIÓNES

Cuarto de Equipos: Instalación de gran tamaño donde se albergan y mantienen numerosos equipos electrónicos como servidores, ventiladores, conexiones y otros recursos necesarios que se utilizan para mantener operativa una red o un sistema de computadoras.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Backup: Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Contraseña: Clave de acceso a un recurso informático

Firewall: conjunto de recursos de hardware y software que protegen a recursos informáticos de accesos indebidos.

Monitoreo: Verificación de las actividades de un usuario con respecto a los recursos informáticos de la empresa.

Política: Toda intención y directriz expresada formalmente por la institución.

Sistema Operativo: Software que controla los recursos físicos de un computador.

Usuario: Toda persona que puede tener acceso a un recurso informático.

4.2. RESPONSABILIDADES, NOTIFICACIONES Y REPORTES DE INCIDENCIA

Es responsabilidad de los usuarios notificar las novedades en cuanto a estas políticas se refiere, o desperfecto de algún equipo tecnológico. El medio para notificarlo en primera instancia será al correo fhernandez@speedfiber.com.ec el cual está destinado para solventar inconvenientes de las “Tecnologías de la información y las comunicaciones (TIC)” de la empresa. Este correo lo recibirá el personal de soporte técnico. En caso de que el usuario no pueda enviar un correo electrónico se podrá notificar mediante las siguientes vías de comunicación:

Telefonía Interna: extensión: 2011 Fernando Hernandez; 2015 Victor Pesantes.

En casos de emergencia tecnológica y solo en estos casos, se utilizará los números particulares del personal de soporte técnico al número: +593 99 959 1306

4.3. FUNCIONES Y RESPONSABILIDADES

Gerente General

- Revisar, evaluar y aprobar el conjunto de metodologías y normas presentadas en este documento e insertarlo como política de seguridad en la empresa SPEED FIBER SPEEDFIBER.CIA.LTDA.
- Asistir a las reuniones convocadas por el Líder de Infraestructura sobre temas de trabajo y levantamiento de información.

Líder de Infraestructura(Ingeniero de soporte)

- Monitorear el desempeño de los controles asociados en seguridad de la información.
- Supervisar y ejecutar la investigación de incidentes de seguridad de la información desde su notificación hasta su resolución.
- Mantener actualizada la infraestructura tecnológica de la empresa SPEED FIBER SPEEDFIBER.CIA.LTDA.
- Brindar soporte técnico al usuario final a través de la generación de tickets de soporte

Técnico de Soporte

- Colaborar en la ejecución para el mejoramiento de la infraestructura tecnológica de SPEED FIBER SPEEDFIBER.CIA.LTDA.
- Brindar soporte técnico al usuario final a través de la generación de tickets de soporte
- Apoyar en la resolución en incidentes de seguridad de la información desde su notificación hasta su resolución

4.4. SEGURIDAD FÍSICA Y LÓGICA

TIPO	RIESGOS	POLÍTICAS
4.4.1 ACCESO	Acceso no autorizado	El Líder de Infraestructura tiene asignada una oficina y un área utilizada como centro de datos, donde se encuentran ubicados los sistemas de comunicaciones y servidores en donde su acceso es restringido sólo a personal autorizado.
		Uso de cámaras de video vigilancia con grabación, sistema de alarmas y sensores de movimiento.
	Acceso a terceros	Las visitas internas o externas del cuarto de equipos deben ser justificadas, identificadas y vigiladas durante el acceso al centro de datos por el Líder de infraestructura u otro personal designado por esta persona.
	Horario de acceso	Las visitas a las instalaciones físicas del centro de datos se deben hacer de lunes a viernes desde las 08:00 hasta las 17:00 horas, a menos que haya una previa coordinación y aceptación en un horario diferente al establecido.
4.4.2 CENTRO DE DATOS	Temperatura inadecuada	Mantener el ambiente con aire acondicionado a temperatura de 17° C a 21° C.
	Respaldo de energía	Contar con un respaldo de energía redundante (UPS)
	Energía estática en los equipos	El edificio debe tener una puesta a tierra en sus instalaciones.
	Área inadecuada de instalación	Los equipos para uso interno se instalan en lugares adecuados, en lo posible lejos del polvo y tránsito de personas.
	Equipos obsoletos	El Lidere de Infraestructura evalúa la vida útil de los equipos informáticos.

4.4.3 EQUIPO	Daño de Equipo Intencional	A todo personal que se le asigne un equipo de cómputo deberá firmar el acta de asignación

DE CÓMPUTO		de recursos informáticos.
	Fallo de equipo de cómputo	El Líder de Infraestructura es responsable de realizar mantenimientos preventivos y correctivos de los equipos de cómputo.
	Falla de Servidor	El Líder de Infraestructura es responsable de realizar mantenimientos preventivos y correctivos de los servidores.
	Activos no inventariados ni identificados	El resguardo de los equipos TI (Tecnología de Información) queda a cargo del Líder de Infraestructura, este se actualiza cada vez que ingrese un equipo nuevo o haya sido de baja.
	Cambio de equipo	Para realizar un cambio de equipamiento informático sin recargo económico, el colaborador deberá demostrar el deterioro por el uso normal del mismo, caso contrario se descontará el daño encontrado y se repondrá el equipo tecnológico. En caso de pérdida del equipamiento tecnológico, el colaborador deberá asumir el costo del mismo y se repondrá dicho equipamiento.
	Teléfonos Celulares	El equipo celular será entregado al colaborador el cual deberá usarlo únicamente para actividades de la empresa, queda prohibido su uso para fines personales. Además, está prohibido cambiar la información de perfil y subir historias personales de whatsapp que no tengan referencia al objetivo de la empresa.
	Salida de Personal	Al momento de retirarse una persona de la empresa es obligación del empleado entregar el equipamiento tecnológico, dicha entrega debe realizarse mediante el acta: recepción de recursos informáticos**.**
4.4.4 CONTROL DE ACCESOS	Conexiones fuera de oficina	Toda conexión del colaborador fuera de oficina y sedes de la organización es realizada mediante una conexión privada (VPN) con credenciales usuario y contraseña.
	Autenticación de usuarios	Las contraseñas para usuarios deberán ser mínimo 8 caracteres que incluyen mayúsculas, minúsculas, números y símbolos. Para administradores deberán tener una complejidad mínima de 12 caracteres en sus contraseñas. Las contraseñas deberán ser cambiadas cada 6 meses.
4.4.5 ACCESO WEB	Infección de virus o malware	Uso de antivirus en servidores y equipos de usuario final.
	Descarga e instalación de programas no autorizados	El personal no debe descargar programas de Internet sin la autorización del Lider el cual se encarga de proveer de todas las herramientas necesarias para el trabajo de los colaboradores.

4.4.6 ACCESO INALÁMBRICO	Seguridad en red inalámbrica	Con el fin de proteger la seguridad de la información y el acceso a la red por medio de la conexión WI-FI, el Departamento de tecnologías implementó el protocolo 802.11 b/g/n con claves de acceso robustas basadas en WPA2 + WPA3 Personal; esto la hace menos vulnerable a ataques de delincuentes cibernéticos y accesos de usuarios no autorizados.

5. SEGURIDAD EXTERNA

5.5.1 EXTERNOS	Terremotos Inundaciones Guerras	Siendo los desastres naturales los más difíciles de predecir y controlar, se reduce la pérdida de información significativamente con un adecuado entrenamiento del personal. El departamento de Tecnologías es capaz de ubicar los archivos y medios externos de almacenamiento con información vital de respaldo para protegerlas.
	Pandemia Paro Anarquía	Ante una pandemia, paro y anarquía el Departamento de Tecnologías provee los servicios de conexión remota segura y confiable mediante el uso de VPN con el fin de resguardar la salud del colaborador y la información de la empresa.

6. INFORMACIÓN

6.6.1 INFORMACIÓN	Respaldo de información	Se realiza respaldos de información automáticos diarios y semanales además de contar con un repositorio en la nube.
	Acceso Indebido a la Información	Los usuarios que administren las credenciales administradoras de la empresa deberán utilizar un gestor de contraseñas con cifrado AES-256.

7. USUARIO

7.7.1 USUARIO	Uso inadecuado de los recursos de la organización	Los recursos informáticos como computadores, celulares, datos, software, redes y sistemas de comunicación están disponibles exclusivamente para cumplir con las obligaciones y

		los propósitos de operatividad para los que fueron diseñados e implementados.
	Uso indebido de información	Todos los usuarios con acceso a un sistema de información o la intranet disponen de una autorización, perfil y privilegio el cual acceden mediante un usuario y una contraseña; por lo tanto, es responsable de la confidencialidad e integridad del recurso al que accede.
	Robo de información	Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona, ni mantenerla por escrito a la vista o al alcance de terceros.
	Compartición de credenciales de autenticación	Ante la salida de personal que maneja información sensible, se procede a dar de baja a los accesos y los servicios. También se realiza un cambio a las credenciales que corresponden a las labores del personal saliente.
	Incidentes de Seguridad	Cualquier incidente de seguridad debe reportarse por escrito al correo electrónico fhernandez@speedfiber.com.ec
	Bloqueo estación de trabajo	Todas las estaciones de trabajo que utilizan los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 3 minutos. Por otra parte, el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para las labores a desempeñar.
	Correo Electrónico	El correo electrónico será asignado al momento de ingresar a la empresa, este correo será configurado únicamente en los equipos asignados al empleado y no se dará acceso a la contraseña del mismo. Abstenerse de utilizar el correo institucional para cualquier propósito ajeno a las funciones relacionadas con el cargo que se desempeña en la empresa. Todo correo electrónico sospechoso deberá ser notificado al Departamento de Tecnología.

8. PERSONAS

8.8.1 RESPONSABILIDADES Y AUTORIDADES	No disponer del personal humano capacitado para la rápida toma de decisiones en el	Se designa al personal humano a cargo del programa de seguridad de la información para la gestión de incidentes y respuesta inmediata.

	caso de una eventualidad	
	No exista funciones derogadas específicas a los colaboradores.	Disponer de descripciones de trabajo escritas para los colaboradores de la empresa.

9. . INCUMPLIMIENTO

El incumplimiento a esta política puede sujetarse a suspensión de los servicios tecnológicos, hasta sanciones definidas por talento humano y gerencia administrativa y como sanción máxima podrá ser desvinculado de la compañía.