
	POLÍTICAS DE SEGURIDAD PARA SOLUCIONES AVANZADAS DE INFORMÁTICAS Y TELECOMUNICACIONES (SAITEL)	Código: PRO-013-2019
		Versión: 1.0
	REALIZADO POR: ING. FERNANDO OBANDO	Fecha: 12/08/2019
		

Alcance de las Políticas de seguridad

Este Manual de políticas de seguridad es elaborado de acuerdo al análisis de riesgos y vulnerabilidades que se presentan para la red de SAITEL EC, por lo cual las políticas que se establece son solo para la empresa.

Objetivos

Objetivo General

Planear y organizar las actividades para mantener y garantizar la integridad de la información, así como resguardar los activos de la empresa.

Objetivos Específicos

- Establecer un esquema de sistema de seguridad de la información claro bajo la responsabilidad de SAITEL EC.
- Generar mejores prestaciones en la disponibilidad del servicio de Internet que brinda la empresa.
- Comprometer a todo el personal de la empresa con el proceso de seguridad de la información.

Definición de Dominios y Controles de normativa ISO/IEC 27001

Identificación de controles implementados por cada dominio de la normativa.

	No aplica/ sin implementar
	Aplica/ implementado
	Aplica/ en desarrollo
	Aplica/ sin implementar

A.5	Política de seguridad de la información		
A.5.1	Dirección de gestión de seguridad de la información		
A.5.1	Políticas para la seguridad de la información	Aplica	
A.5.1.2	Revisión de las políticas para la seguridad de la información	Aplica	
A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		
A.6.1.1	Roles y responsabilidades de seguridad de la información	Aplica	
A.6.1.2	Separación de funciones	No Aplica	
A.6.1.3	Contacto con las autoridades	Aplica	
A.6.1.4	Contacto con los grupos de interés especial	No Aplica	
A.6.1.5	Gestión de proyectos de seguridad de la información	No Aplica	
A.6.2	Dispositivos móviles y teletrabajo		
A.6.2.1	Política de dispositivo móvil	No Aplica	
A.6.2.2	Teletrabajo	No Aplica	
A.7	Seguridad de los RRHH		
A.7.1	Antes del empleo		
A.7.1.1	Investigación de antecedentes	No Aplica	
A.7.1.2	Términos y condiciones del empleo	No Aplica	
A.7.2	Durante el empleo		
A.7.2.1	Responsabilidades de la dirección	Aplica	
A.7.2.2	Concienciación, educación y formación en seguridad de la información	Aplica	
A.7.2.3	Proceso disciplinario	Aplica	
A.7.3	Finalización y cambio de empleo		
A.7.3.1	Responsabilidades ante la finalización o cambio de empleo	Aplica	
A.8	Gestión de Activos		

A.8.1	Responsabilidad de los activos		
A.8.1.1	Inventario de activos	Aplica	
A.8.1.2	Propiedad de los activos	Aplica	
A.8.1.3	Uso aceptable de los activos	Aplica	
A.8.1.4	Devolución de activos	Aplica	
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información	Aplica	
A.8.2.2	Etiquetado de la información	Aplica	
A.8.3	Manejo de los medios		
A.8.3.1	Gestión de medios extraíbles	No Aplica	
A.8.3.2	Eliminación de los medios	No Aplica	
A.8.3.3	Transferencia de medios físicos	No Aplica	
A.9	Control de Acceso		
A.9.1	Requisitos de negocio para el control de acceso		
A.9.1.1	Política de control de acceso	Si Aplica	
A.9.1.2	Acceso a redes y servicios de red	Si Aplica	
A.9.2	Gestión de acceso de los usuarios		
A.9.2.1	Registro y retiro de usuario	Si Aplica	
A.9.2.2	Provisión de accesos a usuarios	Si Aplica	
A.9.2.3	Gestión de privilegios de derechos de acceso	Si Aplica	
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Si Aplica	
A.9.2.5	Revisión de los derechos de acceso de usuario	No Aplica	
A.9.2.6	Retirada y ajuste de los derechos de acceso	No Aplica	
A.9.3	Responsabilidades del usuario		
A.9.3.1	Uso de la información secreta de autenticación	Si Aplica	
A.9.4	Control de acceso a sistemas y aplicaciones		

A.9.4.1	Restricción del acceso a la información	Si Aplica	
A.9.4.2	Procedimientos seguros de inicio de sesión	Si Aplica	
A.9.4.3	Sistema de gestión de contraseñas	Si Aplica	
A.9.4.4	Uso de programas utilitarios privilegiados	No Aplica	
A.9.4.5	Control de acceso al código fuente del programa	No Aplica	
A.10	Criptografía		
A.10.1	Controles criptográficos		
A.10.1.1	Política de uso de los controles criptográficos	Si Aplica	
A.10.1.2	Gestión de llaves	Si Aplica	
A.11	Seguridad física y del entorno		
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad física	No Aplica	
A.11.1.2	Controles físicos de entrada	No Aplica	
A.11.1.3	Seguridad de oficinas, despachos e instalaciones	No Aplica	
A.11.1.4	Protección contra las amenazas externas y ambientales	No Aplica	
A.11.1.5	Trabajo en áreas seguras	No Aplica	
A.11.1.6	Áreas de carga y entrega	No Aplica	
A.11.2	Equipos		
A.11.2.1	Ubicación y protección de equipos	Si Aplica	
A.11.2.2	Instalaciones de suministro	Si Aplica	
A.11.2.3	Seguridad del cableado	Si Aplica	
A.11.2.4	Mantenimiento de los equipos	Si Aplica	
A.11.2.5	Eliminación de activos	Si Aplica	
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Si Aplica	
A.11.2.7	Reutilización o eliminación segura de equipos	Si Aplica	
A.11.2.8	Equipo de usuario desatendido	No Aplica	
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Si Aplica	

A.12	Seguridad de las operaciones		
A.12.1	Procedimientos y responsabilidades operacionales		
A.12.1.1	Documentación de procedimientos de operación	Si Aplica	
A.12.1.2	Gestión de cambios	Si Aplica	
A.12.1.3	Gestión de capacidades	Si Aplica	
A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción	No Aplica	
A.12.2	Protección contra un malware		
A.12.2.1	Controles contra un malware	No Aplica	
A.12.3	Copia de seguridad		
A.12.3.1	Copias de seguridad de la información	Si aplica	
A.12.4	Registro y monitoreo		
A.12.4.1	Registro de eventos	Si aplica	
A.12.4.2	Protección de la información de registro	Si aplica	
A.12.4.3	Registros de administración y operación	Si aplica	
A.12.4.4	Sincronización del reloj	Si aplica	
A.12.5	Control de software operacional		
A.12.5.1	Instalación del software en los sistemas operativos	Si aplica	
A.12.6	Gestión de la vulnerabilidad técnica		
A.12.6.1	Gestión de vulnerabilidades técnicas	Si aplica	
A.12.6.2	Restricciones en la instalación del software	Si aplica	
A.12.7	Consideraciones de auditoría de sistemas de información		
A.12.7.1	Controles de auditoría en los sistemas de información	Si aplica	
A.13	Seguridad de las Comunicaciones		
A.13.1	Gestión de seguridad de la red		
A.13.1	Controles de red	Si aplica	

A.13.1.2	Seguridad de los servicios de red	Si aplica	
A.13.1.3	Separación en las redes	Si aplica	
A.13.2	Transferencia de información		
A.13.2.1	Políticas y procedimientos de transferencia de información	Si aplica	
A.13.2.2	Acuerdos de transferencia de información	Si aplica	
A.13.2.3	Mensajería electrónica	Si aplica	
A.13.2.4	Acuerdos de confidencialidad o no revelación	Si aplica	
A.14	Adquisición, desarrollo y mantenimiento del sistema		
A.14.1	Requisitos de seguridad de los sistemas de información		
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Si aplica	
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Si Aplica	
A.14.2	Seguridad en el desarrollo y en los procesos de soporte		
A.14.2.1	Política de desarrollo seguro	Si Aplica	
A.14.2.2	Procedimientos de control de cambios en sistemas	Si Aplica	
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Si Aplica	
A.14.2.4	Restricciones a los cambios en los paquetes de software	No Aplica	
A.14.2.5	Principios de ingeniería de sistemas seguros	Si aplica	
A.14.2.6	Ambiente de desarrollo seguro	Si aplica	
A.14.2.7	Desarrollo externalizado	No Aplica	
A.14.2.8	Pruebas de seguridad del sistema	Si aplica	
A.14.2.9	Pruebas de aceptación de sistemas	Si aplica	
A.14.3	Datos de prueba		
A.14.3.1	Protección de los datos de prueba	No Aplica	
A.15	Relaciones con proveedores		
A.15.1	Seguridad de la información en relación con los proveedores		

A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	No Aplica	
A.15.1.2	Requisitos de seguridad en contratos con terceros	No Aplica	
A.15.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones	No Aplica	
A.15.2	Gestión de la provisión de servicios del proveedor		
A.15.2.1	Monitoreo y revisión de los servicios de proveedores	No Aplica	
A.15.2.2	Gestión de cambios en los servicios de proveedores	No Aplica	
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes de seguridad de la información y mejoras		
A.16.1.1	Responsabilidades y procedimientos	Si aplica	
A.16.1.2	Informe de los eventos de seguridad de la información	Si aplica	
A.16.1.3	Informe de debilidades de seguridad de la información	Si aplica	
A.16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	Si aplica	
A.16.1.5	Respuesta a incidentes de seguridad de la información	Si aplica	
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Si aplica	
A.16.1.7	Recopilación de evidencias	Si aplica	
A.17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio		
A.17.1	Continuidad de seguridad de la información		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Si aplica	
A.17.1.2	Implementación de la continuidad de seguridad de la información	Si aplica	
A.17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información	Si aplica	
A.17.2	Redundancias		
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Si aplica	

A.18	Cumplimiento		
A.18.1	Cumplimiento de los requisitos legales y contractuales		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Si aplica	
A.18.1.2	Derechos de propiedad intelectual	Si aplica	
A.18.1.3	Protección de los registros	Si aplica	
A.18.1.4	Protección y privacidad de la información de carácter personal	Si aplica	
A.18.1.5	Reglamentos de controles criptográficos	Si aplica	
A.18.2	Revisiones de seguridad de la información		
A.18.2.1	Revisión independiente de seguridad de la información	Si aplica	
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Si aplica	
A.18.2.3	Comprobación del cumplimiento técnico	Si aplica	

Asignación de Responsabilidades

- Responsabilidades Generales

Departamento: Todos a quienes sean afectados por el SGSI
Responsable: Gerente General

- Gestión de cumplimiento de normativa

Departamento: Todos a quienes sean afectados por el SGSI
Responsable: Gerente General, jefes de área

- Gestión de riesgos

Departamento: Todos a quienes sean afectados por el SGSI
Responsable: Jefes de área

- Revisión y medición del SGSI

Departamento: Todos a quienes sean afectados por el SGSI
Responsable: Responsable de seguridad

- Gestión de Activos

Departamento: Todos a quienes sean afectados por el SGSI

Responsable: Departamento de Sistemas, departamento técnico

- Gestión de incidencias

Departamento: Todos a quienes sean afectados por el SGSI

Responsable: Departamento técnico

- Gestión de comunicación

Departamento: Todos a quienes sean afectados por el SGSI
Responsable: Gerente general

Políticas de Seguridad Generales

Art 1.- Este documento, "Políticas de seguridad" en base a la norma ISO 27001, establece cómo se debe manejar la seguridad de la información en la gestión de infraestructura y aplicaciones.

Art 2.- Brindar una guía para los administradores de la red y encargados de las aplicaciones sobre políticas que deben cumplir para conservar los activos.

Art 3.- El Jefe Técnico es el responsable de que se haga cumplir las políticas y los procedimientos del área técnica.

Art 4.- Cada jefe de departamento debe asegurarse del cumplimiento de las políticas de la información y procedimientos correspondientes a su área.

Art 5.- Revisar las políticas de seguridad siempre que se produzcan cambios significativos en la institución, con la finalidad de ser actualizadas de ser necesario.

Art 6.- Las políticas deben ser socializadas con todos los funcionarios que integran el área Tecnológica e Informática.

Art. 7.- Cada uno de los empleados debe tener al menos un medio de comunicación para mantener el contacto apropiado con las autoridades pertinentes.

Art. 8.- Todos los documentos o correos electrónicos con información sensible deben de estar cifrados mediante llaves de control públicas y privadas.

Art. 9.- Solo el personal autorizado y responsable de la integridad de la información deben tener las llaves de control pública y privadas para acceder a los documentos cifrados.

Políticas Generales Para Administradores

Art. 10.- Cada vez que se necesite realizar un cambio de equipos en los nodos de distribución de servicio se debe hacer un respaldo de la información y de las configuraciones.

Art 11.- Todos los administradores deben cambiar las contraseñas de los equipos que se encuentran en la Infraestructura de red cada que se realice cambios bruscos en el personal que tiene injerencia sobre la red.

Art 12.- Las contraseñas deben ser mayores a 8 caracteres, de alto grado de dificultad, compuestas por letras minúsculas, mayúsculas, números y símbolos.

Art 13.- Los administradores no deben utilizar la misma contraseña en todos los equipos que tienen a su cargo, ni tampoco compartir estas contraseñas con personas que no están autorizadas o que son ajenas a la institución.

Art 14.- No abrir documentos adjuntos de dudosa procedencia, y tampoco hacer clic en enlaces de mensajes solicitados cuando no se conozca el origen de los mismos.

Art 15.- No brindar información de datos personales o del personal a desconocidos por teléfono o e-mail, sin antes validar el origen de la petición y la autorización de la autoridad pertinente.

Políticas de Gestión de Activos

Art 16.- Debe de generarse un registro de los activos que se involucran en el proceso de transportar y salvaguardar la integridad de la información.

Art 17.- Cada uno de los activos debe tener un propietario o responsable, para el manejo o uso del mismo.

Art 18.- Todos los activos que sirven para el acceso a la red de SAITEL deben ser regresados a la empresa al terminar el uso de los mismo, ya sea por término de contrato o por daño, bajo el proceso establecido en el manual de procedimiento de desinstalación.

Art 19.- La información sensible debe clasificarse según el impacto que tenga para la empresa, la misma que será etiquetada etiquetadas según la guía de uso del protocolo TLP provista por el organismo de control ARCOTEL.

Políticas de Seguridad de las Operaciones

Art. 20.- Todos los procedimientos de la gestión de activos deben estar documentados, etiquetados (LTP), revisados y aprobados por las autoridades respectivas.

Art. 21. Todos los procedimientos de la gestión de vulnerabilidades y suspensión de servicio deben estar documentados, etiquetados (LTP), revisados y aprobados por las autoridades respectivas.

Art. 22.- Cada procedimiento para el tratamiento de la gestión de riesgos debe de estar documentados, etiquetados (LTP), revisados y aprobados por las autoridades respectivas.

Art. 23.- Los procedimientos de revelación de información privada o limitada, deben de estar documentados, etiquetados (LTP), revisados y aprobados por las autoridades respectivas.

Art. 24.- Los procedimientos de retiro y desinstalación de equipos por termino de contrato deben de estar documentados, etiquetados (LTP), revisados y aprobados por las autoridades respectivas.

Art. 25.- El procedimiento del respaldo de información sensible de la empresa debe estar documentado, etiquetado (LTP), revisado y aprobado por las autoridades correspondientes.

Art. 26.- La suspensión del servicio de internet debe ser divulgado en una plataforma de acceso público, mediante comunicados de los eventos o mantenimientos programados.

Art. 27.- Todos los eventos de suspensión o posible afectación al servicio de internet se debe registrar mediante la generación de tickets, los cuales se clasifican de acuerdo al grado de criticidad en la red.

1. Eventos de mantenimiento o controlados - BLANCO
2. Eventos de baja afectación a la red - VERDE
3. Eventos de mediana afectación a la red - AMARILLO
4. Eventos de alta criticidad a la red - ROJO

Políticas de Control de Acceso

Art. 28.- Se asignará únicamente usuarios personales y se evitará utilizar usuarios genéricos, para el acceso al sistema de integrado de SAITEL EC.

Art. 29.- Todos los usuarios con acceso al sistema integrado dispondrán de una autorización de acceso de usuario y contraseña.

Art. 30.- Todos los empleados deberán tener una credencial de identificación con nombre y cargo que desempeña.

Art. 31.- El usuario y contraseñas asignado se comunicará al empleado al ingreso a la empresa junto con un contrato de confidencialidad e integridad de la información.

Art. 32. La instalación de nuevo software debe ser solo con el usuario de administrador de cada dispositivo en la red de SAITEL.

Art. 33.- Los dispositivos de los trabajadores que se encuentran conectados a la red de SAITEL, se deben de usar para las funciones que desempeñan en cada área, es prohibido acceder a páginas que contengan contenido pornográfico.

Art. 34.- En este apartado se centra al acceso físico a las instalaciones con la finalidad de prevenir accesos no autorizados o accidental de terceros o sobre el sistema de la organización. Los entornos a proteger son los nodos de distribución de servicio de internet

- 1.- Sólo el personal autorizado tendrá el acceso a los nodos de distribución del servicio de Internet.
- 2.- Las configuraciones de la red de transporte, distribución y acceso deberán ser ejecutada solo por el personal capacitado y autorizado.
- 3.- Las claves de acceso a los nodos tanto de candados como de alarmas deben ser solo de conocimiento de personal autorizado.
- 4.- El ingreso a cada nodo de distribución de internet se deberá realiza con los elementos de protección personal especificados en el manual de seguridad industrial de SAITEL.
- 5.- El acceso a los nodos, oficinas o áreas de trabajo que contengan información sensible debe estar físicamente restringido.
- 6.- Cuando un trabajador termina su relación laboral con SAITEL sus permisos de acceso a dependencias deben ser revocados, la lista de personas y permisos debe ser actualizada periódicamente, de acuerdo a la política de R.R.H.H.
- 7.- El jefe técnico o a quien él delegue, debe generar una lista de personal autorizado a ingresar a los diferentes nodos/data centers.
- 8.- El acceso del personal interno o externo, autorizados a ingresar a los nodos/data center, debe quedar registrado detallado el motivo y la fecha de ingreso.

Art. 35.- Todos los dispositivos de los clientes/abonados que tienen acceso a la red y servicios de SAITEL deben estar registrados por la dirección IP y cliente a quien corresponde el dispositivo.

Políticas de Seguridad para la Infraestructura

Art. 36.- Toda la infraestructura computacional y de redes no puede ser usada para fines o actividades no relacionadas con el servicio que brinda SAITEL.

Art. 37.- Cada uno de los equipos que tienen como propósito el transporte de información deben tener un respaldo de iguales características o similar en la bodega de la sucursal más cercana en caso de requerir ser reemplazado.

Art. 38.- Cada uno de los Nodos debe tener redundancia de conexión a la red, la cual debe ser automatizada (solo en casos puntuales se permite que se gestione manualmente por el personal capacitado)

Art. 39. Debe existir personal interno que tenga el conocimiento de cada uno de los nodos/data centers y elementos pasivos de interconexión de la red de SAITEL, se debe asignar grupos por zonas y tipo de red (transporte, distribución, acceso).

Art. 40.- El monitoreo de la red debe ser constante por medio de software especializado para la administración de la red, así como de personal capacitado y autorizado para realizar cambios y los correctivos que corresponda.

Art. 41.- El cronograma de mantenimiento de la red y prevención de incidentes debe ser de conocimiento de todo el personal en el área encargada de ejecutar el trabajo.

Art. 42.- El jefe técnico debe elaborar un cronograma anual con los grupos que actuarán sobre la identificación de eventualidades en la red o pérdida de servicio, mitigación y solución de los eventos que se presenten.

Art. 43.- Todas las redes inalámbricas deben tener un sistema de autenticación para los usuarios.

Art 44.- Sólo los equipos de computación de SAITEL. deben estar configurados para que puedan conectarse a la red cableada.

Art 45.- Los servidores que se encuentran en producción en el data center deberán tener un sistema antivirus de acuerdo al sistema operativo de cada uno.

Art 46.- Todas las conexiones remotas del personal de SAITEL deben tomar las medidas de seguridad correspondientes, para esto se determina la utilización de VPNs y las directrices dadas en el Art. 12 para la creación de contraseñas.

Art 47.- La comunicación entre los equipos de telecomunicaciones del data center debe tener en cuenta la utilización de llaves públicas o métodos de encriptación de datos.

Art. 48.- Cada uno de los nodos/data centers debe contar con redundancia de energía eléctrica para prevenir las caídas de servicio por fallas o eventualidades en el suministro eléctrico.

Art. 49.- Los equipos encargados del transporte y acceso a la red deben estar ubicados en un espacio controlado y seguro, a excepción de casos puntuales donde no se pueden restringir el ingreso, en estos sitios se debe asegurar con gabinetes y otros medios físicos posibles de acuerdo al lugar.

Art. 50.- Con la finalidad de preservar la seguridad y disponibilidad de la infraestructura de red se debe generar eventos de mantenimiento programados periódicamente.

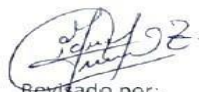
Políticas de seguridad para los Recursos Humanos (R.R.H.H.)


Art. 51.- En el contrato de todo trabajador debe constar una mención sobre el compromiso de mantener la confidencialidad de la información.

Art. 52.- Todo trabajador debe conocer y cumplir la normativa interna relacionada con la seguridad e integridad de la información.

Art. 53.- Se debe informar que la obligación sobre la confidencialidad de la información de la empresa SAITEL EC siguen vigentes después de un cambio o terminación de empleo.


Realizado por:
Ing. Fernando Obando
Técnico SAITEL


Revisado por:
Ing. Miguel Cuasapaz
Jefe Técnico SAITEL


Aprobado por:
Ing. Freddy Marlon Rosero Cuaspa
Gerente General SAITEL

