1. Introducción

Las políticas de seguridad informática tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes Voz y Datos) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de la empresa.

La compañía ha desarrollado las siguientes Políticas de Seguridad Informática que, a su vez, son un conjunto de normas enmarcadas en el ámbito administrativo de la empresa.

Esas políticas aplican para todo el personal de la institución, y para el proveedor de IT contratado para tal fin.

2. Objetivo

1. Dotar de la información necesaria a los usuarios, empleados y gerentes, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la Red, así como la información que es procesada y almacenada en estos.

2. Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la empresa.

3. Los objetivos que se desean alcanzar luego de implantar las Políticas de Seguridad son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de TI en la administración del riesgo.
- Compromiso de todo el personal de la empresa con el proceso de seguridad, agilizando la aplicación de los controles.
- Que la prestación del servicio de seguridad gane en calidad.
- Todos los empleados se convierten en interventores del sistema de seguridad.

3. Vigencia

Todas estas amenazas están en continuo proceso de expansión, lo que, unido al progresivo aumento de los sistemas de información y dependencia del negocio, hace que todos los sistemas y aplicaciones estén expuestos a riesgos cada vez mayores, que, sin una adecuada gestión de los mismos, pueden ocasionar que su vulnerabilidad se incremente y consiguientemente los activos se vean afectados. Todo empleado es responsable del cumplimiento de los estándares, directrices y procedimientos de control de acceso, así como también notificar a su nivel jerárquico superior, cuando por algún motivo no pueda cumplir con las Políticas de Seguridad indicando el motivo por el cual no le es posible apegarse a la normativa de seguridad. Cabe destacar que este nivel de responsabilidad va a ser conocido por las diferentes áreas de la empresa quienes serán las garantes de que esta información sea conocida por cada integrante de área. La documentación presentada como Políticas de Seguridad entrará en vigencia desde el momento en que sean aprobadas por la Gerencia. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de la empresa o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

4. Notificaciones de violaciones de seguridad

Es de carácter obligatorio para todo el personal (Fijo, Contratado), la notificación inmediata de algún problema o violación de la seguridad, del cual fuere testigo; esta notificación debe realizarse por escrito vía correo electrónico a La Gerencia y/o a los TI y/o a la Gerencia de Calidad, quienes están en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente.

Es responsabilidad de todo empleado que maneje datos o información a través de accesos debidamente autorizados, el cumplimiento de las políticas de control de acceso, puesto que estas descansan en el establecimiento de responsabilidades donde se incurra en alguna violación en materia de seguridad acarreando sanciones a quien las haya causado, puesto que esto ocasionaría perjuicios económicos a la empresa de diversa consideración. Es por ello que las personas relacionadas de cualquier forma con los procesos tecnológicos deben ser conscientes y asumir que la seguridad es asunto de todos y, por tanto, se debe conocer y respetar las Políticas de Seguridad. Está fundamentado como una exigencia que el personal de la organización conozca sus responsabilidades, sanciones y medidas a tomar al momento de incurrir en alguna violación o falta, escrita en las Políticas de Seguridad firmado por el empleado o proveedor o cualquier empresa del grupo. Por esta razón se entenderá que sólo una adecuada política de seguridad tecnológica apoyará la concientización para obtener la colaboración de los empleados, haciéndoles conscientes de los riesgos que podemos correr y de la importancia del cumplimiento de las normas. Políticas de Seguridad Informática

5. Licenciamiento

Todos los productos de Software que se utilicen deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

El área de Tecnología promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

6. Bases de datos

Para la operación del software de red en caso de manejar los datos empresariales mediante sistemas de información, se deberá tener en consideración lo siguiente:

- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información de la empresa. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.
- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.
- Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente, asimismo, los HDD de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación.
- Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

7. POLÍTICAS DE SEGURIDAD FÍSICA

7.1. Acceso Físico:

La empresa destinará un área que servirá como centro de telecomunicaciones donde ubicará los sistemas de telecomunicaciones y servidores. Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de tecnología o con permiso de los TI. Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo o el superior responsable o los TI, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a las personas delegadas del Área Administrativa de La empresa y al personal de seguridad del edificio.

7.2. Protección Física Data Center:

- Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por la gerencia de Tecnología.
- Aire acondicionado. Mantener la temperatura a 21 grados centígrados.
- Respaldo de energía con respaldo de planta eléctrica.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores. Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Prevención y/o detección de incendios.
- Contar por lo menos con dos extintores de incendio adecuado y cercano al Data Center.

7.3. Infraestructura

Las dependencias deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes. El resguardo de los equipos de cómputo deberá quedar bajo el área de Tecnología contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.

7.4. Instalaciones de equipos de cómputo

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- El Área de Tecnología, así como las áreas operativas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
- Los IT deben llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.
- Los encargados del área de tecnología son los responsables de organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

- El Área de Recursos Humanos deberá reportar a los IT cuando un usuario deje de laborar o de tener una relación con la empresa, para que se le realice levantamiento de equipos y gestionar la baja de accesos y permisos en aplicativos y en red, entregando paz y salvo al área de TH.

7.5. Respaldos

- Las Bases de Datos de La empresa serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.
- Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro (Cloud) que permitirá tener contingencia y continuidad de negocio.

7.6. Recursos de los usuarios

7.6.1. Uso

- Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de la empresa, de acuerdo con las políticas que en este documento se mencionan.
- Los usuarios deberán solicitar apoyo al área de Tecnología ante cualquier duda en el manejo de los recursos de cómputo de la empresa.
- El correo electrónico de cada usuario, no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la empresa, tales como cadenas, publicidad y propaganda comercial, política, social, etc). Se debe utilizar los recursos dedicados a tales tareas bajo la responsabilidad de la persona a cargo.
- El material informático o de comunicación, como celulares, asignado a cada empleado no puede ser utilizado para otros fines, diferentes a los indicados por la empresa.

7.6.2. Derechos de Autor

- Queda estrictamente prohibido inspeccionar, copiar y almacenar ítems de cualquier índole, que violen la ley de derechos de autor, como está estipulado en cláusula de confidencialidad de los contratos laborales.
- Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la empresa, para lo cual se tiene perfil estándar con recursos limitados.
- No está autorizada la descarga de Internet de programas informáticos no autorizados por La Gerencia o la Gerencia de Tecnología de TI.
- Si se descubre que un empleado ha copiado programas informáticos o archivos no permitidos en forma ilegal, este puede ser sancionado, suspendido o despedido.
- Si se descubre que un empleado ha copiado programas informáticos en forma ilegal para dárselos a un tercero, también puede ser sancionado, suspendido o despedido y se pondrá en conocimiento del área jurídica de la empresa, para que den el debido manejo.
- Si un usuario desea utilizar programas informáticos autorizados por la empresa en su hogar, debe consultar con los IT para asegurarse de que ese uso esté licenciado.
- El personal encargado de soporte de Tecnología realizará auditorias anuales, que permitan identificar cualquier situación inusual.
- Si se encuentran copias sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.

- La empresa autoriza el uso de programas informáticos de diversas empresas externas. La empresa no es dueña de estos programas informáticos o la documentación vinculada con ellos y, a menos que cuente con la autorización del creador de los programas informáticos, no tiene derecho a reproducirlos excepto con fines de respaldo.

- Los usuarios que se enteren de cualquier uso inadecuado que se haga en La empresa de los programas informáticos o la documentación vinculada a estos, deberán informar de manera inmediata al área de tecnología para que se tomen las medidas pertinentes, dependiendo de la gravedad del asunto.

8. Políticas de seguridad lógica

8.1. Red

Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de la Empresa entre usuarios, departamentos, oficinas y hacia afuera a través de conexiones con otras redes o con la empresa del Grupo.

El Área de Tecnología no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo de tecnología IT. No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la empresa.

Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la empresa y se usarán exclusivamente para actividades relacionadas con la labor asignada.

Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

El uso de analizadores de red es permitido única y exclusivamente por IT para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad bajo las Políticas de Seguridad.

No se permitirá el uso de analizadores para monitorear o censar redes ajenas a La empresa y no se deberán realizar análisis de la Red desde equipos externos a la entidad.

Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

8.2. Servidores

IT tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la red.

La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de los IT.

Durante la configuración de los servidores los IT deben generar las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

Los servidores que proporcionen servicios a través de la red e Internet deberán: o Funcionar 24 horas del día los 365 días del año. O Recibir mantenimiento preventivo mínimo una vez al año o recibir mantenimiento semestral que incluya depuración de logs. O recibir mantenimiento anual que incluya la revisión de su configuración. O Ser monitoreados por lo IT.

La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo: o Diariamente, información crítica. O Semanalmente, los documentos web. O Mensualmente, configuración del servidor y logs.

Los servicios hacia Internet sólo podrán proveerse a través de los servidores autorizados por IT.

8.3. Bases de Datos

El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso.

Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.

En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para volver a asignarle su contraseña.

La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

8.4. Recursos de Cómputo

IT son los encargados de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la cantidad de usuarios y a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

IT debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo Los IT son los únicos autorizados para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

8.5. Responsabilidades y/o atribuciones de los ingenieros de soporte

- Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.
- Deberán utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos. Deberán realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.
- Deben actualizar la información de los recursos de cómputo de la empresa, cada vez que adquiera e instale equipos o software.
- Deben registrar cada máquina en el inventario de control de equipos de cómputo y red de la empresa.

- Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.
- Reportar a la Gerencia los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.
- Deben realizar un reporte periódico de todas las actividades de mantenimiento preventivo o correctivo realizadas durante cada semestre.

8.6. Renovación de equipos

- Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.
- Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al área de Tecnología a fin de que se seleccione el equipo adecuado. Sin el visto bueno de Tecnología no podrá liberarse una orden de compra.
- La Gerencia puede utilizar la infraestructura de la Red para proveer servicios a los usuarios externos y/o visitas previa autorización los IT..
- Los IT son los responsables de la administración de contraseñas y deberán guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.
- No se darán equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales en La empresa, excepto por orden expresa de La Gerencia.
- Los IT realizarán las siguientes actividades en los servidores de La empresa.
- Los IT son los únicos autorizados para asignar las cuentas a los usuarios.

8.7. Usuarios

- Todos los usuarios con acceso a un sistema de información o a la Red, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- Ningún usuario recibirá un identificador de acceso a la Red, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.
- El usuario deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recurso que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el director de cada área.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud de los IT, con el fin de contribuir a la seguridad de los servidores en los siguientes casos: o Cuando ésta sea una contraseña débil o de fácil acceso. o Cuando crea que ha sido violada la contraseña de alguna manera.

- El usuario deberá notificar a los IT en los siguientes casos: o Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor o Si tiene problemas en el acceso a los servicios proporcionados por el servidor.
- Si un usuario viola las políticas de uso de los servidores, los IT podrán cancelar totalmente su cuenta de acceso a los servidores, notificando a La Gerencia correspondiente.

8.8. Responsabilidades Personales

- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.
- El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.
- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.
- En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.
- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.
- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte. Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.
- Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.
- Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco del equipo de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

8.9. Uso Apropiado de los Recursos

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para complementar las obligaciones y propósito de la operación para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

Queda Prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de La empresa.
- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales, discriminatorios u ofensivos.
- Introducir voluntariamente software dañino o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
- Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus. Antivirus de la Red
- Todos los equipos de cómputo de la empresa deberán tener instalada una Solución Antivirus.
- Periódicamente se hará el rastreo en los equipos de cómputo de La empresa, y se realizará la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la red.

8.10. Responsabilidad de los IT.

Las responsabilidades del equipo IT son:

- Implementar la Solución Antivirus en las computadoras de la empresa.
- Solucionar contingencias presentadas ante el surgimiento de virus que la solución no haya detectado automáticamente.
- Configurar el analizador de red para la detección de virus.
- Los IT aislaron el equipo o red, notificando a la Gerencia correspondiente, en las condiciones siguientes:
    - Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otros equipos y redes.
    - Si el usuario viola las políticas antivirus.
    - Cada vez que los usuarios requieran hacer uso de discos USB 's, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o en un equipo designado para tal efecto en las áreas de cómputo de las dependencias.
- En caso de contingencia con virus los IT deberán seguir el procedimiento establecido. La solución corporativa de seguridad de antivirus es Microsoft Defender, esta solución integra herramientas Antivirus, antispyware, firewall y prevención contra intrusiones, para multiplataforma (Windows), para todos los clientes.

9. SEGURIDAD PERIMETRAL

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto

permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

Los IT implementarán soluciones lógicas y físicas que garanticen la protección de la información de la compañía ante posibles ataques internos o externos.

Dentro de las funciones de la seguridad perimetral se incluyen:

- Todos los accesos tengan factor de autenticación, el cual dependiendo de la información requerirá usuario y contraseña, y en caso de accesos superiores validación mediante VPN.
- Las contraseñas el factor de autenticación, para las redes wifi será trimestral y para la VPN será mensual.
- Proporcionar mínimo dos canales de conexión de distinto proveedor con el exterior.
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
- Proteger sistemas o servicios vulnerables mediante factor de autenticación.

9.1. Redes Privadas Virtuales (VPN).

Los usuarios móviles y remotos de la empresa podrán tener acceso a red interna privada cuando se encuentren fuera de la empresa alrededor del mundo en cualquier ubicación con acceso al Internet público, utilizando las redes privadas VPN.

Los IT serán los encargados de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.

9.2. Conectividad a Internet

La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de la empresa, tienen las mismas responsabilidades en cuanto al uso de Internet.

No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

9.3. Red Inalámbrica (WIFI)

9.3.1. Acceso a Funcionarios de la empresa:

La red inalámbrica es un servicio que permite conectarse a la red, la Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de la empresa.

Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.

Las condiciones de uso presentadas definen los aspectos más importantes, que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (Computadoras portátiles, celulares, etc.) con capacidad de conexión wifi.

Los IT, son los encargados de la administración, habilitación y/o bajas de usuarios en la red inalámbrica de la empresa.

9.3.2. Identificación y activación

Para hacer uso de la red inalámbrica, el solicitante deberá ser miembro de algún área de la empresa o tener autorización especial.

Como primer paso para hacer uso de este servicio, se debe contar con autorización verbal o escrita.

Los IT determinarán las medidas pertinentes de seguridad, para usar las redes inalámbricas.

Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar a los IT para su respectiva baja del equipo de la red inalámbrica.

9.3.3. Tecnología

La red inalámbrica de la empresa usa el estándar 802.11b/g/n con cifrado WPA2. Por lo tanto, las tarjetas de red inalámbrica deben poseer la certificación Wi-Fi™ de este estándar y soportar los requerimientos descritos.

A pesar de que se usan amplificadores de señal, la cobertura queda sujeta a diversos factores, por lo que NO SE GARANTIZA, de ninguna forma el acceso desde cualquier punto fuera de cobertura de la empresa.

- Sólo será soportado el protocolo TCP/IPV4 en la red inalámbrica.
- No se permiten la operación ni instalación de puntos de acceso, conectados a la red cableada de la empresa sin la debida autorización por parte los TI.
- No se permite configurar las tarjetas inalámbricas como puntos de acceso, o la configuración de equipos como servidores adicionales.

9.3.4. Restricciones y/o prohibiciones de acceso a Internet

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

- El uso de programas para compartir archivos (Peer to Peer).
- El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- El uso de sitios de videos en línea o en tiempo real.
- Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.
- Uso de JUEGOS "on line" en la red.

9.3.5. Excepciones

Todas las prohibiciones con autorizaciones especiales.

9.3.6. Acceso a Invitados:

La red inalámbrica de reuniones, será la asignada a invitados el cual es un servicio que permite conectarse única y exclusivamente a personal externo de la empresa (clientes, proveedores) a internet sin la necesidad de algún tipo de cableado.

Los usuarios invitados no tendrán acceso a la Red de La empresa ni a ningún recurso de uso privado de La empresa.

10. Plan de contingencias informáticas

Los IT crearán para los departamentos un plan de contingencia informática, que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos informáticos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

11. Historial de cambios

Fecha	Versión	Descripción del Cambio	Realiza el cambio
15/11/2018	01	● Creación del documento	Olivier Gallet / Gerente SAC,IT y Calidad
06/10/2021	02	● Definición de índice ● Inclusión del numeral 10 del documento “Contingencias informáticas” ● Inclusión del numeral 7.6.2 “Derechos de autor”, Primer párrafo.	Oscar Ibagón / Director de Calidad
29/11/2023	03	Actualización del documento ● Se implementan los requerimientos de seguridad informática	Willian Perez Zapata / Director IT
25/01/2024	04	• Creación del documento	Willian Pérez / Carolina Casas