1. OBJETIVO GENERAL. -

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

2. OBJETIVOS ESPECIFICOS. -

    - Establecer un esquema de sistema de seguridad de la información.
    - Comprometer a todo el personal de la empresa con el proceso de seguridad de la información.

3. SOPORTE NORMATIVO / BASE LEGAL

La elaboración del siguiente procedimiento se sustenta en lo establecido en la Ley Orgánica de Telecomunicaciones (L.O.T.) artículos 78, 80, 85, su Reglamento, Norma Técnica para Coordinar la Gestión de Incidentes y Vulnerabilidades que afecten a la Seguridad de las Redes y Servicios de Telecomunicaciones (Resolución ARCOTEL-2018-0652), el cual establece entre varios puntos lo siguiente: "…Los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos de carácter personal de conformidad…"

Así mismo, se establece: "…Las y los prestadores de servicios implementarán procedimientos internos para atender las solicitudes de acceso a los datos personales de sus abonados, clientes o usuarios por parte de las autoridades legalmente autorizadas…"

Art. 12 de la Norma Técnica "…el encargado de seguridad del prestador de servicios de telecomunicaciones, previo al comienzo de sus actividades en la gestión de incidentes o vulnerabilidades, deberán firmar Acuerdo de confidencialidad o establecerse cláusulas de confidencialidad y no divulgación durante el proceso de contratación de personal, con el representante legal de la empresa prestadora ….en el que se establezcan las obligaciones respecto a la no divulgación y tratamiento de información…"

4. ALCANCE / DESCRIPCION DEL REQUERIMIENTO. -

- Estas Políticas se elaboran de acuerdo al análisis de riesgos y vulnerabilidades que se presenten en la red del permisionario autorizado Victor Cumbicos Ontaneda, así como para asegurar el cumplimiento de regulaciones y leyes aplicables por parte de la Agencia de Regulación y Control (ARCOTEL)

5. DEFINICIONES Y TERMINOLOGIA. –

- **Proceso o Procedimiento. -** Los procedimientos o procesos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico.
- **Política de Seguridad. -** Conjunto de reglas **establecidas** por la autoridad de seguridad de la empresa, que rigen la utilización y prestación de servicios y facilidades de seguridad de la red.

6. AREAS IMPACTADAS E INVOLUCRADAS. –

- Estas Políticas de Seguridad aplican a todo el personal incluyendo: contratistas, consultores y personal temporal.

7. POLITICAS DE SEGURIDAD GENERALES. –

- Brindar una guía para los administradores de la red y encargados de las aplicaciones sobre políticas que deben cumplir para conservar los activos.
- El jefe Técnico es el responsable de que se haga cumplir las políticas y los procedimientos del área técnica.

- Cada jefe de departamento debe asegurarse del cumplimiento de las políticas de la información y procedimientos correspondientes a su área.
- Revisar las políticas de seguridad y procesos considerando un periodo de 6 meses de acuerdo a las nuevas necesidades de la institución, con la finalidad de ser actualizadas de ser necesario.
- Las políticas deben ser socializadas con todos los funcionarios que integran el área Tecnológica e Informática.
- Cada uno de los empleados debe tener al menos un medio de comunicación para mantener el contacto apropiado con las autoridades pertinentes.
- Todos los documentos o correos electrónicos con información sensible deben de estar cifrados mediante llaves de control públicas y privadas.
- Solo el personal autorizado y responsable de la integridad de la información deben tener la llave de control pública y privada para acceder a los documentos cifrados.
- Con la finalidad de poder mejorar y asegurar el cumplimiento de las Políticas de Seguridad de la Información y sus Procesos serán sancionados todos aquellos empleados que infrinjan estos lineamientos aquí descritos. Si es por primera vez será un llamado de atención verbal, si es reincidente habrá un llamado de atención por escrito, sanción económica o despido dependiendo del tipo de infracción.

8. POLITICAS GENERALES PARA ADMINISTRADORES. -

- 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.
- El Encargado de la Seguridad de la Información debe 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.
- Las contraseñas deben ser mayores a 8 caracteres, de alto grado de dificultad, compuestas por letras minúsculas, mayúsculas, números y símbolos.
- 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.
- 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.
- 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.

9. POLITICAS DE GESTION DE ACTIVOS. -

- Debe de generarse un registro de los activos que se involucran en transportar y salvaguardar la integridad de la información.
- Cada uno de los activos debe tener un propietario o responsable, para el manejo o uso del mismo.
- Todos los activos que sirven para el acceso a la red de INTERBYTES deben ser regresados a la empresa al terminar el uso de los mismos, ya sea por término de contrato o por daño.
- La información debe clasificarse según la sensibilidad y el impacto que tenga para la empresa, en este caso se ha considerado 2 tipos de Información: la confidencial y la de carácter general. información sensible cuyo uso no autorizado afectaría a los intereses financieros, técnicos y comerciales de la empresa.

10. POLITICA DE SEGURIDAD DE LAS OPERACIONES. -

- Todos los procedimientos de la gestión de activos deben estar documentados, revisados y aprobados por las autoridades respectivas. Todos los procedimientos de la gestión de vulnerabilidades y suspensión de servicio deben estar documentados, revisados y aprobados por el encargado de la seguridad de la información y el representante legal.
- Cada procedimiento para el tratamiento de la gestión de riesgos debe de estar documentados, revisados y aprobados por el encargado de la seguridad de la información y el representante legal.
- Los procedimientos de revelación de información privada o limitada, deben de estar documentados, revisados y aprobados por el encargado de la seguridad de la información y el representante legal.
- El procedimiento del respaldo de información sensible de la empresa debe estar documentado, revisado y aprobado por el encargado de la seguridad de la información y el representante legal.
- La suspensión del servicio de internet debe ser divulgado en una plataforma de acceso público, mediante comunicados de los eventos o mantenimientos programados en el portal web de INTERBYTES
- Todos los eventos de suspensión o posible afectación al servicio de internet se deben 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
  2. Eventos de baja afectación a la red
  3. Eventos de mediana afectación a la red
  4. Eventos de alta criticidad a la red

11. POLITICAS DE CONTROL DE ACCESO. -

- Se asignará únicamente usuarios personales y se evitará utilizar usuarios genéricos, para el acceso al sistema de INTERBYTES
- Todos los usuarios con acceso al sistema dispondrán de una autorización de acceso de usuario y contraseña.
- Todos los empleados deberán tener una credencial de identificación con nombre y cargo que desempeña.
- 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.
- La instalación de nuevo software debe ser solo con el usuario de administrador de cada dispositivo en la red de INTERBYTES
- Los dispositivos de los trabajadores que se encuentran conectados a la red de INTERBYTES, se deben de usar para las funciones que desempeñan en cada área, es prohibido acceder a páginas que contengan contenido pornográfico.
- En este apartado se centra al acceso físico a las instalaciones con la finalidad de prevenir accesos no autorizados o accidentales de terceros o sobre el sistema de la organización. Los entornos a proteger son los nodos de distribución de servicio de internet
- Sólo el personal autorizado tendrá el acceso a los nodos de distribución del servicio de Internet.
- Las configuraciones de la red de transporte, distribución y acceso deberán ser ejecutada solo por el personal capacitado y autorizado.
- Las claves de acceso a los nodos tanto de candados como de alarmas deben ser solo de conocimiento de personal autorizado.
- 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 INTERBYTES
- El acceso a los nodos, oficinas o áreas de trabajo que contengan información sensible debe estar físicamente restringido.
- Cuando un trabajador termina su relación laboral con INTERBYTES 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.
- El jefe técnico o a quien él delegue, debe generar una lista de personal autorizado a ingresar a los diferentes nodos.
- El acceso del personal interno o externo, autorizados a ingresar a los nodos, debe quedar registrado detallado el motivo y la fecha de ingreso.
- Todos los dispositivos de los clientes/abonados que tienen acceso a la red y servicios de INTERBYTES deben estar registrados por la dirección IP y cliente a quien corresponde el dispositivo.

12. POLITICAS DE SEGURIDAD PARA LA INFRAESTRUCTURA. -

- Toda la infraestructura computacional y de redes no puede ser usada para fines o actividades no relacionadas con el servicio que brinda INTERBYTES
- Cada uno de los equipos que tienen como propósito el transporte de información deben tener un respaldo de iguales características o similares en la bodega de la sucursal más cercana en caso de requerir ser reemplazado.
- 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).
- Debe existir personal interno que tenga el conocimiento de cada uno de los nodos y elementos pasivos de interconexión de la red de INTERBYTES, se debe asignar grupos por zonas y tipo de red (transporte, distribución, acceso).
- 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.
- 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.
- El Encargado de la Seguridad de la Información 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.
- Todas las redes inalámbricas deben tener un sistema de autenticación para los usuarios.
- Sólo los equipos de computación de INTERBYTES deben estar configurados para que puedan conectarse a la red cableada.
- Los servidores que se encuentran en producción en los nodos deberán tener un sistema antivirus de acuerdo al sistema operativo de cada uno.
- Todas las conexiones remotas del personal de INTERBYTES deben tomar las medidas de seguridad correspondientes, para esto se determina la utilización de VPNs y las respectivas directrices para la creación de contraseñas.
- La comunicación entre los equipos de telecomunicaciones debe tener en cuenta la utilización de llaves públicas o métodos de encriptación de datos.
- Cada uno de los nodos debe contar con redundancia de energía eléctrica para prevenir las caídas de servicio por fallas o eventualidades en el suministro eléctrico.
- 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.
- Con la finalidad de preservar la seguridad y disponibilidad de la infraestructura de red se debe generar eventos de mantenimiento programados periódicamente.

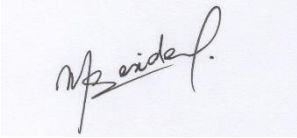
13. POLITICAS DE SEGURIDAD PARA LOS RECURSOS HUMANOS. -

- En el contrato de todo trabajador debe constar una mención sobre el compromiso de mantener la confidencialidad de la información, además del Acuerdo de Confidencialidad y Seguridad de la Información estipulado por ARCOTEL en Resolución ARCOTEL-2018-0652.
- Todo trabajador debe conocer y cumplir la normativa interna relacionada con la seguridad e integridad de la información.
- Se debe informar que la obligación sobre la confidencialidad de la información de INTERBYTES siguen vigentes después de un cambio o terminación de empleo.

14. CONTROL DE CAMBIOS. -

Historial de Control de Cambios		
Edición #	Fecha de aplicación	Descripción del cambio
1	30/01/2023	Documento Inicial

15. FIRMAS



ELABORADO POR:	REVISADO POR:	APROBADO POR:
Ing. Mariuxi Desiderio	Ing. Victor Cumbicos O.	Ing. Victor Cumbicos O.
CONSULTOR EXTERNO	JEFE TECNICO	REPRESENTANTE LEGAL