Ultracom	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		
	Nombre	**Cargo**	**Fecha (d/m/a)**
Revisado por:	Daniela Tabares	Gerente Administrativa (SOINFCO)	30/12/2021
Aprobado por:	Freddy Angarita	Gerente General	30/12/2021

OBJETIVO: Presentar las bases ligadas a los pilares de la seguridad de la información que ULTRACOM IT S.A.S aplica al interior de la empresa y a su vez adapta en los procesos transversales a los proyectos y/o contratos con el propósito innato de garantizar la seguridad, confidencialidad, integridad y continuidad de la información como activo fundamental de la entidad.

ELABORARO POR:

Natalia Gaviria

Gerente Administrativa

ACTUALIZADOR POR:

SOINFCO S.A.S

Proveedor de servicios de tecnologías de información.

PROPOSITO

El presente documento tiene como finalidad brindar una guía de las políticas del SGSI que son necesarias en ULTRACOM para salvaguardar la información.

Este documento se encuentra estructurado en seis políticas de seguridad que son:

- **General**
- **Seguridad de Personal**
- **Seguridad Física**
- **Administración de Operaciones de Computo**

- **Controles de Acceso Lógico**
- **Usuarios privilegiados**

1. POLÍTICA GENERAL

Todo funcionario de ULTRACOM se compromete a cumplir las directrices de confidencialidad y de uso adecuado de los recursos informáticos de ULTRACOM y por ende de sus clientes, así como el estricto apego a las Políticas Generales del SGSI de ULTRACOM y de sus clientes.

2. SEGURIDAD PERSONAL

Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de ULTRACOM, así como el estricto apego al manual de políticas y estándares de seguridad informática para usuarios.

2.1. OBLIGACIONES DE LOS USUARIOS:

Es responsabilidad de los usuarios de bienes y servicios informáticos:

- Cumplir las políticas y estándares de seguridad informática para usuarios del presente manual.
- Portar el carnet de identificación: la compañía asignará un carnet personal e intransferible que lo reconocerá como funcionario de la misma para identificarse dentro de las Instalaciones de ULTRACOM como en instalaciones externas cuando se encuentre en desarrollo de sus funciones. Es su obligación mantenerlo en buen estado y reportar su pérdida al área de Gestión Humana, así como devolverlo al momento de finalización de su relación contractual.

3. SEGURIDAD FÍSICA:

- Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de ULTRACOM, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y al centro de cómputo de la compañía.
- El usuario deberá reportar de forma inmediata al área de Sistemas, cuando detecte que existan riesgos reales o potenciales para equipo de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.
- El usuario tiene la obligación de proteger los medios llámense CD-DVD, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información confidencial o interna.
- Es responsabilidad del usuario evitar en todo momento la fuga de la información que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.
- Áreas de acceso: El personal de ULTRACOM deberá observar y hacer cumplir el nivel de acceso definido a las diferentes áreas de las instalaciones físicas definidas.
- La compañía asignará una tarjeta de acceso físico al edificio, la cual deberá ser personal e intransferible. No deberá ser prestada a terceros ni utilizada por una persona diferente a quien la compañía se la asigna. Es su obligación mantenerlo en buen estado y reportar su pérdida al área de Gestión Humana, así como devolverlo al momento de finalización de su relación contractual.

3.1. PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS DE CÓMPUTO

- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del área de Sistemas, debiéndose solicitar a la misma en caso de requerir este servicio.

- El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones asignadas al usuario de ULTRACOM.
- Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne o el servidor de archivos, ya que el disco duro local está destinado para archivos de programas y sistema operativo.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos. Los adaptadores de portátiles deben permanecer sobre el escritorio.
- Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.
- Mientras se utilice el equipo portátil en el puesto de trabajo debe quedar asegurado con la guaya de seguridad y su clave no debe quedar en posición de apertura. Si va a dejar el equipo portátil en otro puesto de trabajo y va a quedar momentáneamente sin su supervisión, debe trasladar la guaya.
- USBs, CDs, DVDS y en general medios de almacenamiento con información clasificada de la compañía no deben permanecer en sitios sin acceso restringido.

3.2. MANTENIMIENTO DE EQUIPO:

- Únicamente el personal autorizado del área de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.
- Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que

se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación.

3.3. PERDIDA O TRANSFERENCIA DE EQUIPO:

- El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- El resguardo para los portátiles tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.
- El usuario deberá dar aviso de inmediato a las áreas de Gestión Humana y Sistemas de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.
- Daño del equipo: El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, el mismo deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

4. ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO.

Los usuarios deberán utilizar los mecanismos institucionales para proteger información que reside y utiliza la infraestructura de ULTRACOM. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de ULTRACOM o hacia redes externas como internet.

4.1. ALMACENAMIENTO: Los usuarios deberán hacer uso de repositorio de información para alojar información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo. Las actividades que realicen los usuarios de ULTRACOM en la infraestructura de tecnología de la información son registradas y susceptibles de auditoría.

4.2. INSTALACIÓN DE SOFTWARE: Los usuarios que requieran la instalación de software que no sea propiedad de ULTRACOM deberán solicitar su autorización a Sistemas justificando su uso, a través de la herramienta de gestión de HelpDesk, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación. Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de ULTRACOM, que no esté autorizado por Sistemas. Se procederá a desinstalar software no aprobado o sin licencia que no esté aprobado por el área encargada.

4.3. ADMINISTRACIÓN DE LA CONFIGURACIÓN: Los usuarios de las áreas de ULTRACOM no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información.

4.4. SEGURIDAD DE LA RED

- Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por Sistemas en la cual los usuarios realicen la exploración de los recursos informáticos en la red de ULTRACOM, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.
- Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentra fuera o ausente), el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a ULTRACOM, a menos que cuente con la autorización del titular del área.

- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de ULTRACOM
- Acceso a VPN`s y demás dispositivos con los cuales se puedan acceder o tener acceso remoto deberán estar debidamente autorizados por la Sistemas y sólo podrán conectarse desde equipos de la compañía.

4.5. CONTROLADORES DE CÓDIGO MALICIOSO

- Para prevenir infecciones por virus informáticos, los usuarios de ULTRACOM, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y autorizado por la Sistemas.
- Está prohibido el uso de Memorias USB y dispositivos de almacenamiento, para prevenir infección de tipo informático, así como filtración de información y código fuente.
- Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el área de Sistemas en programas tales como: Antivirus; correo electrónico; Office; Navegadores; u otros programas. Así como desactivar o cambiar la configuración del firewall o antivirus, temporal o permanentemente.

Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:

- Serán sujetos de monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas como pornografía y juegos.
- Saben que existe la prohibición de transmisión de archivos de tipo confidencial no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización del área de Sistemas.

- La utilización de internet es para el desempeño de su función y puesto y no para propósitos personales.

4.6. CONTROLADORES DE ACCESO LÓGICO:

- Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso a los recursos.
- Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica.
- Cada usuario que accede a la infraestructura tecnológica de ULTRACOM debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.
- Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan.
- Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.
- Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de ULTRACOM deberán ser notificados a través de la herramienta de gestión de Help Desk.
- Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.
- La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, deben ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

- Cuando un usuario olvide, bloquee o extravíe su contraseña, al no tener ingreso al mismo o presentar dificultad deberá notificarlo al área de sistemas.
- Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas: No deben contener números consecutivos; Deben estar compuestos de al menos siete (7) caracteres. Estos caracteres deben ser alfanuméricos, es decir números y letras.
- Si el usuario tiene asignado un portátil, y la compañía lo autoriza permanente u ocasionalmente para retirarlo y trabajar en cliente o desde un sitio diferente a la compañía y dicho funcionario necesita copiar información del servidor de archivos de la red de manera local, a su regreso deberá sincronizar la información local y actualizar el servidor de archivos de la red; posteriormente debe eliminar las copias locales.
- Eliminar copias no controladas por los sistemas de gestión de ULTRACOM con el fin de evitar fugas o perdida de información si se llegase a perder el dispositivo de manera temporal o permanente.

5. USUARIOS PRIVILEGIADOS

Los usuarios privilegiados son aquellos que disponen de permisos lógicos y físicos especiales, que por la naturaleza su función es necesario dentro de ULTRACOM, entre ellos se encuentran los usuarios administradores de centro cómputo, personal de seguridad física, administradores de estaciones, administradores de bases de datos, administradores de aplicaciones, entre otros.

Los usuarios de ULTRACOM que disponen de usuarios privilegiados deben cumplir los siguientes ítems.

- Uso: El uso del privilegio es personal e intransferible, de igual forma es sólo para la función o actividad a desarrollar

- Auditoria: Sin importar el momento u actividad que se encuentre desarrollando, el usuario privilegiado podrá ser auditado a través de logs de registro y de grabación que se realice de la sesión de trabajo.
- Asignación: La asignación de un permiso o privilegio no podrá ser brindada a un usuario genérico, es necesario que la misma se conceda sólo a título personal.
- Cuentas de servicio: Las cuentas lógicas privilegiadas que sean utilizadas por servicios u aplicaciones, sólo podrán ser utilizadas para tales fines y no podrán ser utilizadas por un usuario para el trabajo cotidiano u actividades de gestión.

SEGUIMIENTO Y GESTIÓN.

Trimestralmente se debe realizar un seguimiento y gestión acorde a la política de seguridad de la información buscando corroborar y madurar la adopción de la misma, igualmente, velar por el cumplimiento de esta con procesos auditivos internos en cada uno de los procesos, dejando como evidencia bitácora que refleje los resultados tangibles del proceso en cuanto a cada pilar de la política del SGSI para ULTRACOM IT S.A.S.