1. OBJETO

- 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 Grupo VESTA.

- 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.
- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de los ATI en la administración del riesgo.

2. ALCANCE

- La Política General de Seguridad de la Información de GRUPO VESTA se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información.
- La presente política debe ser conocida y cumplida por todo el personal de la Institución.
- Esta Política se aplica en todo el ámbito de GRUPO VESTA, a sus recursos y a la totalidad de los procesos, internos y externos, vinculados a la entidad a través de contratos o acuerdos con terceros.

3. REFERENCIAS, DEFINICIONES Y ABREVIATURAS

3.1. Referencias

- Norma ISO 27002

3.2. Definiciones

ABD: Administrador de Base de Datos.

ATI: Administradores de Tecnología de Información (Help Desk). Responsables de la administración de los equipos de cómputo, sistemas de información y redes de Las Empresas. Vela por todo lo relacionado con la utilización de equipos de cómputo,

sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

Red: Equipos de cómputo, sistemas de información y redes de telemática de Las Empresas.

Usuario: Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por Las Empresas tales como equipos de cómputo, sistemas de información, redes de telemática.

4. RESPONSABILIDADES

a) Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

b) 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.

c) Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

d) 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.

e) El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.

f) 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.

g) 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.

h) 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, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

i) 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.

j) Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

k) 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.

l) 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.

m) 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.

n) Toda solicitud para utilizar un medio de almacenamiento de información compartido, deberá contar con la autorización del jefe inmediato del usuario y del titular del área dueña de la información.

5. POLITICAS DE SEGURIDAD LOGICA

Red

a) 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 las empresas del Grupo.

b) 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.

c) Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

d) No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la empresa.

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

f) 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.

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

h) 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.

6. SERVIDORES

Configuración e instalación

a) Los ATI tienen la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.
b) La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de los ATI.
c) Durante la configuración de los servidores los ATI deben genera 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.
d) Los servidores que proporcionen servicios a través de la red e Internet deberán:
   - Funcionar 24 horas del día los 365 días del año.
   - Recibir mantenimiento preventivo mínimo dos veces al año.
   - Recibir mantenimiento semestral que incluya depuración de logs.
   - Recibir mantenimiento anual que incluya la revisión de su configuración.
   - Ser monitoreados por los ATI.

E) La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:
   - Diariamente, información crítica.
   - Semanalmente, los documentos web.
   - Mensualmente, configuración del servidor.

F) Los servicios hacia Internet sólo podrán proveerse a través de los servidores autorizados por los ATI.

7. CORREO ELECTRÓNICO

a) Los ATI se encargarán de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
b) Para efecto de asignarle su cuenta de correo al usuario, el área de Recursos Humanos ó jefe inmediato, deberá llenar una solicitud en formato establecido para tal fin y entregarlo al área de Tecnología, con su firma y la del Gerente del área.

c) La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.
d) La longitud mínima de las contraseñas será igual o superior a 14 caracteres, que deberá contener como mínimo un signo, una mayúscula y un número.
e) La reasignación de cuenta de correo se hará mediante la solicitud por escrito del jefe inmediato.

8. BASES DE DATOS

a) 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.
b) El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso.
c) 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.
d) En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle una contraseña.
e) La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

9. HELP DESK (ATI)

Los ATI tendrán las siguientes atribuciones y/o responsabilidades:

a) Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.
b) Deberán utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.
c) 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.
d) Deben actualizar la información de los recursos de cómputo de Grupo VESTA, cada vez que adquiera e instale equipos o software.

e) **Deben registrar cada máquina en el inventario de control de equipos de cómputo y red de Grupo VESTA**.
f) Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados por Grupo VESTA, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
g) Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.
h) 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.

10. USUARIOS

Identificación de Usuarios y contraseñas

a) 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.
b) Ningún usuario recibirá un identificador de acceso a la Red, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.
c) El usuario deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto **y será responsable de la confidencialidad de la misma**.
d) 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 La Gerencia.
e) La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
f) Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
g) El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud de los ATI, con el fin de contribuir a la seguridad de la informacion y los servidores en los siguientes casos:
h) Cuando ésta sea una contraseña débil o de fácil acceso.
i) Cuando crea que ha sido violada la contraseña de alguna manera.
j) El usuario deberá notificar a los ATI en los siguientes casos:

k) Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
l) Si tiene problemas en el acceso a los servicios proporcionados por el servidor.
m) Si un usuario viola las políticas de uso de los servidores, los ATI podrán cancelar totalmente su cuenta de acceso a los servidores, notificando a La Gerencia correspondiente.

11. USO APROPIADO DE LOS RECURSOS

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa 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:

a) El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
b) Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de Las Empresas.
c) Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
d) Introducir voluntariamente programas, virus, macros, applets, controles ActiveX 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.
e) Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
f) Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
g) 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.
h) El uso de los grabadores de discos compactos es exclusivo para respaldos de información que por su volumen así lo justifiquen.

12. POLITICAS DE 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 ATI implementarán soluciones lógicas y físicas que garanticen la protección de la información de Grupo VESTA de posibles ataques internos o externos como ser:

a) Rechazar conexiones a servicios comprometidos
b) Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
c) Proporcionar un único punto de interconexión con el exterior.
d) Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
e) Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
f) Auditar el tráfico entre el exterior y el interior.
g) Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

13. FIREWALL

a) La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.
b) Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
c) Los ATI establecerán las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
d) El firewall debe bloquear las “conexiones extrañas” y no dejarlas pasar para que no causen problemas.
e) El firewall debe controlar los ataques de “Denegación de Servicio” y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
f) Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

14. REDES PRIVADAS VIRTUALES (VPN)

a) Los usuarios móviles y remotos de Las Empresas podrán tener acceso al 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 IPSec habilitadas por el Área de Tecnología.
b) Los ATI serán los encargados de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.
c) Es de responsabilidad del usuario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.
d) El uso del sistema VPN debe ser controlado utilizando una contraseña de autenticación fuerte, manteniéndola siempre en secreto.
e) Cuando esté conectado activamente a la red de Grupo VESTA el sistema VPN permitirá el tráfico de acuerdo con el perfil del usuario hacia y desde el equipo computacional a través del túnel VPN, el resto del tráfico pasará por la conexión respectiva.
f) Las puertas de enlace VPN serán configuradas y administradas por los ATI.

15. CONECTIVIDAD A INTERNET

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de Las Empresas tienen las mismas responsabilidades en cuanto al uso de Internet.
- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma. 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.

- Internet es una herramienta de trabajo.
- Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.
- Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

16. RED INALÁMBRICA (WIFI)

Acceso a Funcionarios de Las Empresas:

a) La red inalámbrica es un servicio que permite conectarse a la red Las Empresas e Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de Las Empresas.
b) Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.
c) 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, Ipod, celulares, etc.) con capacidad de conexión Wireless.
d) Los ATI, son los encargados de la administración, habilitación y/o bajas de usuarios en la red inalámbrica de Las Empresas.

Restricciones/prohibiciones de acceso a Internet

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

a) El uso de programas para compartir archivos (Peer to Peer).
b) El acceso a páginas de redes sociales.
c) El uso de sitios de videos en línea o en tiempo real.
d) Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.
e) Uso de JUEGOS "on line" en la red.

<u>Excepciones</u>

a) En caso de eventos, cursos, talleres, conferencias, etc, se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil.
b) En el caso de estos eventos las restricciones para acceder podrán ser “anuladas” temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos un día hábil.