Anexo A – Política de Seguridad [Referencial]

1.1.1. SEGURIDAD DE TALENTO HUMANO:

Seguridad de la Información en la Gestión del Talento Humano

a. El área de Recursos Humanos cumplirá la función de notificar a todo el personal que ingresa a laborar en la Organización las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.
b. Asimismo, tendrá a su cargo junto con el Oficial de Seguridad de la Información la notificación del Manual de Políticas a todo el personal, de los cambios que en el manual se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad y las tareas de capacitación en materia de seguridad.
c. Se deberán definir y documentar los roles y responsabilidades de la seguridad de los empleados y terceros en concordancia con la política de seguridad de la información, las misma que se enfoca en llevar a cabo controles de verificación del personal al momento de iniciar el proceso de selección y capacitación de seguridad de la información al personal que se incorporará a la Organización.

Compromiso de Confidencialidad

a. Como parte del proceso de contratación, los empleados, cualquiera sea su nivel jerárquico, firmarán un Compromiso de Confidencialidad de la información, en lo que respecta al tratamiento y manejo de la información de la Organización.
b. El Oficial de Seguridad de la Información otorgará al personal que se incorpore a la Organización una capacitación sobre seguridades de la información de manera obligatoria con la respectiva confirmación del área de Recursos Humanos.
c. Se desarrollará un medio para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre: (i) suscripción inicial del Compromiso para todo el personal, (ii) revisión del contenido del Compromiso de manera anual.

Cambio de Puesto de Trabajo

1. Se debe garantizar que los empleados, contratistas y terceras personas abandonan la organización o cambian de empleo de forma controlada.
2. En caso de cambio de puesto de trabajo o cese de funciones, las responsabilidades de seguridad de la información deben estar claramente definidas y asignadas, en la cual se debe incluir la devolución de todos los activos de la organización que estén en su posesión, como la entrega del software, documentos corporativos y equipos de cómputo o dispositivos, tarjetas de accesos, manuales, información guardada en medios electrónicos

Desvinculación de Personal

1. El Jefe o Gerente de la línea de supervisión del empleado desvinculado deberá notificar inmediatamente al área de Recursos Humanos y al Oficial de Seguridad de la Información mediante correo sobre la desvinculación y los motivos.
2. El área de Recursos Humanos enviará la notificación de salida de personal al Oficial de Seguridad con la información del colaborador y cualquier medida o acción especial que sea necesario realizar, solicitando retirar los permisos de accesos a la información de la Organización y en conjunto con Recursos Humanos administrar el documento de entrega – recepción de: accesos físicos (llaves, cajas fuertes, tarjetas electrónicas), tarjetas de identificación, documentos, manuales, accesos lógicos (email, acceso a la red y servidores), acceso a sistemas, datos, material de la empresa (portátil, móvil, etc.)
3. Hacer un seguimiento del uso de aplicaciones y transacciones de acuerdo a las leyes locales.

Pantallas y Escritorios Limpios

1. Se debe adoptar una política de escritorio limpio para información que pueda estar en papeles y dispositivos de almacenamiento removibles.

2. Esto aplica a la protección de cualquier tipo de información, en cualquiera de sus formas y que pueden estar contenidas en escritorios, estaciones de trabajo, computadores portátiles, medios ópticos, medios magnéticos, documentos en papel y en general cualquier tipo de información que es utilizada por empleados y ejecutivos, para apoyar la realización de sus actividades laborales.

1. Cuando un trabajador se ausenta de su lugar de trabajo, en largos períodos de tiempo fuera de su escritorio, los documentos sensibles del trabajo deben ser colocados en cajones cerrados con llave.
2. Al final de la jornada de trabajo el empleado debe poner en orden su escritorio y guardar todos los papeles de oficina en el mueble designado, asegurado con llave.
3. Guarde bajo llave los dispositivos informáticos portátiles, como ordenadores portátiles o dispositivos móviles.
4. Tratar a los dispositivos de almacenamiento masivo como CD-ROM, DVD o unidades USB como sensibles y guardarlos en un cajón cerrado con llave
5. No dejar a la vista documentos sensibles en el escritorio.
6. No escribir claves ni otros datos sensibles en papeles que queden visibles para terceros
7. La información clasificada o sensible, cuando se imprima se debería retirar inmediatamente de las impresoras.

1. Las estaciones de trabajo y equipos portátiles deben tener aplicado el estándar relativo a protector de pantalla, de forma que se active, ante un tiempo sin uso, el protector definido por la Organización.

2. Toda vez que el colaborador se ausente de su lugar de trabajo debe bloquear su estación de trabajo de forma de proteger el acceso a las aplicaciones y servicios de la institución.

3. La pantalla de autenticación a la red de la institución debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información.

Intercambio de Información

1. Concientizar al personal sobre la toma de debidas precauciones, por ejemplo, no revelar información sensible como para evitar ser escuchado o interceptado, al hacer una llamada telefónica, por personas cercanas, en especial al utilizar teléfonos móviles; terceros que tengan acceso a la comunicación mediante la intervención de la línea telefónica, terceros en el lado receptor.
2. Recordar al personal que no sostengan conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas.
3. No dejar mensajes en contestadores automáticos.

Desconexión de Terminales por Tiempo Muerto

El Oficial de Seguridad de la Información, junto con los Propietarios de la Información definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad de la Organización, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, el mismo que será definido por los administradores del aplicativo, para evitar el acceso de personas no autorizadas.

1. Para los equipos de usuarios se implementará la desconexión por inactividad, que limpie la pantalla y evite el acceso no autorizado. Asimismo, si un usuario debe abandonar su puesto de trabajo momentáneamente, deberá bloquear su sesión, recalcando la estricta responsabilidad y administración de su equipo y claves personales; a los efectos de evitar que terceros puedan acceder y mal utilizar su información

a. CONTROLES DE ACCESO FÍSICO

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Oficial de Seguridad de la Información a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico considerarán al menos lo siguiente:

1. Acompañar e inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área.

2. Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán controles de autenticación para autorizar y validar todos los accesos. Se mantendrá un registro protegido para permitir auditar todos los accesos.
3. Implementar el uso de una identificación visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

b. RETIRO/SALIDA DE LOS BIENES

Los equipos, la información y el software no serán retirados o sacados de las oficinas de la Organización sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro o salida no autorizada de activos de la Organización,

GESTIÓN DE ACTIVOS:

a. REQUERIMIENTOS DE SEGURIDAD DE TECNOLOGIA DE LA INFORMACION

1. Requerimientos de seguridad en el ámbito físico.

- Control de acceso a las instalaciones y centro de computo
- Prever la incorporación de bloqueos o medidas de protección física.
- Uso de formularios para brindar acceso a las instalaciones.
- Cerraduras electromagnéticas con control de aproximación.
- Cámaras para identificación de visitantes.
- Proceso para Control de acceso a instalaciones de tecnología de información.

a. Identificación de Riesgos del Acceso de Terceras Personas

1. El tipo de Acceso requerido (físico/lógico y a qué recurso).
2. Los motivos por los cuales se solicita el acceso.
3. El valor de la información.
4. Los controles empleados por la tercera parte.
5. La incidencia de este acceso en la seguridad de la información de la Organización.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Organización, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo de confidencialidad que defina las condiciones para la conexión o el acceso

1.1.2. GESTIÓN DE COMUNICACIONES Y OPERACIONES:

a. SEGURIDAD DEL CORREO ELECTRÓNICO

1. Protección contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.
2. Protección de archivos adjuntos de correo electrónico.
3. En caso de ser necesario, uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos
4. Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

b. COMPUTACIÓN MÓVIL Y TRABAJO REMOTO (COMPUTACIÓN MÓVIL)

Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.; que sean pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

1. La protección física necesaria
2. El acceso seguro a los dispositivos
3. La utilización de los dispositivos en lugares públicos bajo la responsabilidad del usuario.
4. El acceso a los sistemas de información y servicios de la Organización a través de dichos dispositivos.
5. Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
6. La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia, deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

1. Permanecer siempre cerca del dispositivo.
2. No dejar desatendidos los equipos.
3. No llamar la atención acerca de portar un equipo valioso.
4. No poner identificaciones de la Organización en el dispositivo, salvo los estrictamente necesarios.
5. No poner datos de contacto técnico en el dispositivo.
6. Mantener cifrada la información clasificada.

7. De acuerdo al perfil laboral, evitar el uso fuera de la oficina de los dispositivos y en los casos que amerite siempre y cuando sean necesarios.

El Jefe de Infraestructura deberá elaborar y proporcionar al propietario del dispositivo un procedimiento que le permita reportar de manera inmediata, cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de la Organización, los que incluirán:

1. Revocación de las credenciales afectadas
2. Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

c. RESGUARDO DE LA INFORMACIÓN

Se determinarán los requerimientos para resguardar cada software o información en función de su criticidad.

El Director de Informática dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración.

d. ANÁLISIS DE UBICACIÓN IDÓNEA PARA REPOSITORIO REMOTO

1. El lugar elegido debe ofrecer las condiciones adecuadas, permitir el acceso únicamente a la persona autorizada, ser accesible geográficamente a través de más de una vía terrestre.

2. La localidad elegida no debe estar en un piso bajo, pues correría el riesgo de inundación.

3. La localidad elegida no debe estar en bajo un techo desmontable, pues correría el riesgo de colapse del mismo.

4. Tomando en cuenta las consideraciones anteriores se ha determinado que la Agencia Tumbaco es la más apropiada para alojar los respaldos de información.

a. ADMINISTRACIÓN DE PRIVILEGIOS

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal por parte de la Dirección a la cual correspondan. Se deben tener en cuenta los siguientes pasos:

1. Identificar los privilegios asociados a cada producto del sistema.
2. Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento.
3. Mantener un proceso de autorización y un registro de todos los privilegios asignados.

4. Establecer un período de vigencia para el mantenimiento de los privilegios.
5. Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

b. ADMINISTRACIÓN DE CONTRASEÑAS (CLAVES) DE USUARIO

La asignación de contraseñas (claves) se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

1. Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Este documento será solicitado y custodiado por medio de la Mesa de Servicios como respaldo de la entrega de la clave y el perfil asignado al usuario.
2. Generar a los usuarios contraseñas provisorias seguras que serán asignadas automáticamente y entregadas mediante correo electrónico o personalmente en sobre de seguridad.
3. Garantizar que los usuarios cambien las contraseñas iniciales o provisorias
4. Almacenar las contraseñas sólo en sistemas informáticos protegidos.
5. Utilizar otras tecnologías de autenticación y autorización de usuarios registrados. Todos los sistemas deben tener la siguiente configuración:
   - Las contraseñas deberán tener un mínimo de 8 caracteres, deben contener números, letras mayúsculas y minúsculas y al menos un carácter especial.
   - Se suspenderá o bloqueará la cuenta del usuario después de tres intentos fallidos de ingreso con una contraseña incorrecta.
   - Las contraseñas se caducarán automáticamente cada 15 días (recomendable) o 30 días (máximo) para los sistemas.
   - Impedir que las ultimas 5 contraseñas puedan ser reutilizadas.
   - Los literales mencionados anteriormente deben ser soportados y solventados por medio de la Mesa de Servicios, la misma que debe elaborar y socializar un procedimiento que le permita administrar y respaldar la gestión de claves a usuarios.
   - En caso de presentarse incidentes de riesgo deberán ser reportados al Oficial de Seguridad de la Información.

c. ADMINISTRACIÓN DE CONTRASEÑAS CRÍTICAS (ADMINISTRADOR, SERVIDORES Y DEMÁS)

1. Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
2. Las contraseñas seleccionadas (de administrador de los servidores) serán seguras, y su definición será efectuada como mínimo por dos personas (1 del personal de Informática y 1 de Seguridad de la Información), de manera que ninguna de ellas conozca la contraseña completa.
3. Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.

4. La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
5. Cada contraseña crítica se renovará una vez utilizada y será modificada luego de 6 meses en caso de que no se la haya utilizado.
6. Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Oficial de Seguridad de la Información.
7. Las contraseñas deberán tener un mínimo de 12 caracteres, deben contener números, letras mayúsculas y minúsculas y al menos un carácter especial.
8. La contraseña de Administrador de las estaciones de trabajo del personal de Informática será diferente a la de Administrador de los usuarios, esta contraseña será administrada por el Oficial de Seguridad de la Información y la segunda por el personal de Informática.

d. CONTROL DE ACCESOS A LOS SISTEMAS DE INFORMACIÓN

a. AISLAMIENTO DE LOS SISTEMAS SENSIBLES

Son aplicables las siguientes consideraciones:

1. Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación (Ver 5. Clasificación y Control de Activos).
2. Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.
3. Coordinar con el Responsable del Área informática, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.
4. Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
5. Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

b. MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deberán incluir:

1. Identificación del usuario.
2. Fecha y hora de inicio y terminación.
3. Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma (Ver Identificación Automática de Terminales).
4. Registros de intentos exitosos y fallidos de acceso al sistema.
5. Registros de intentos exitosos y fallidos de acceso a datos y otros recursos, por ejemplo transacciones u opciones del sistema que contenga información restringida.

c. ACCESO A INTERNET

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Oficial de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el jefe inmediato del usuario solicitante. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

El Oficial de Seguridad de la Información se encargará de revisar las configuraciones de los grupos y permisos de navegación para evitar conflictos y posibles fugas de información por accesos no autorizados a internet.

d. CONTROL DE CONEXIÓN A LA RED

Se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los dispositivos de red que separen los diferentes dominios de la red

e. PROTECCIÓN CONTRA SOFTWARE MALICIOSO (MALWARE)

El Oficial de Seguridad de la Información definirá los controles y prevención para la protección contra software malicioso (malware). El Director de Informática y Comunicaciones o el personal designado por éste, implementará dichos controles.

Estos controles deberán considerar los siguientes aspectos:

1. Se prohíbe el uso de software no autorizado por la Organización, las reglas de Active Directory no deben permite instalaciones, se programa una inspección anual.
2. Para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas los controles y monitoreo se hace a través de Firewall de la Institución.
3. Instalar y actualizar periódicamente software de detección y protección contra virus.
4. Mantener los sistemas al día con las últimas actualizaciones de seguridad
5. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Organización.

6. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto y de dispositivos de almacenamiento masivo.

Concientizar al personal acerca del problema de un mensaje de correo electrónico con contenido falso o engañoso y atrayente y de cómo proceder frente a los mismos.