Manual de políticas de Seguridad de la Información

Control Interno

Este documento fue preparado por:
Michel Vargas, Jefe Control Interno
Carvajal Tecnología y Servicios
Cali, Colombia

Historial de Cambio

Fecha	Versión Documento	Descripción	Responsable del Cambio	Aprobado por	Cargo Aprobador
29-09-2016	1.0	Creación del documento	Michel Vargas	Michel Vargas	Jefe Área control Interno
24-10-2016	1.1	Ajustes de Ortografía	Michel Vargas	Andrés Fuentes Gensini	Director Global Financiero, Administrativo y de Gestión
03-02-2017	2.0	Se modificaron el 100% de las políticas, realizando una depuración de temas que eran redundantes y estaban presentes en políticas que no correspondían, adicionalmente se modificaron algunos controles que no eran viables de implementar por el nivel de madurez de la Compañía en temas de seguridad.	Michel Vargas	Andrés Fuentes Gensini	Director Global Financiero, Administrativo y de Gestión
03-02-2017	2.1	Se actualiza la tabla de contenido con respecto al punto 3.13 Uso de Internet, Intranet y Almacenamiento en la Nube. Se le quitan los subpuntos 3.13.1 ,3.13.2,3.13.3	Michel Vargas	Andrés Fuentes Gensini	Director Global Financiero, Administrativo y de Gestión
04-08-2017	1.0	Se realiza cambio de alcance y de la política de equipos móviles. Se migra el documento GESEGU MA 001 con Version 2.1 del proceso de seguridad de la información al proceso de Control Interno.	Michel Vargas	Andrés Fuentes Gensini	Director Global Financiero, Administrativo y de Gestión

Tabla de Contenido

1 Objetivo

Establecer los criterios y comportamientos que deben seguir todos los miembros de la comunidad empresarial (colaboradores, contratistas, clientes, practicantes y terceros en general) con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

Las políticas de seguridad de la información contenidas en este documento, son de obligatorio cumplimiento para todos los colaboradores, contratistas y terceros que tengan acceso a información de la Compañía, el no cumplimiento de estas se considera una falta grave y se tratara de acuerdo con el reglamento interno.

2 Alcance

Este manual aplica para todos los colaboradores, contratistas, clientes, practicantes y terceros en general involucrados en el ciclo productivo de los procesos de la Compañía en Colombia, Perú, Ecuador, México y Argentina.

3 Políticas

3.1 Retiro de Activos

- ✓ El retiro de equipos de cómputo, periféricos, dispositivos de almacenamiento, software e información considerada crítica propiedad de la Compañía, fuera de las instalaciones de la Compañía debe seguir los procedimientos establecidos por el procedimiento GESEGU EBS PR 001 - proceso de gestión de activos.

3.2 Control de Acceso

- ✓ La dirección de tecnología es responsable de asegurar que las redes inalámbricas de la Compañía cuenten con métodos de autenticación que eviten accesos no autorizados.
- ✓ El área de gestión de accesos que pertenece a la Dirección de Tecnología es responsable de gestionar los accesos a plataformas, servicios de red y sistemas de información de acuerdo a procesos formales de autorización definidos en el procedimiento de control de acceso.
- ✓ El jefe responsable del proceso y control interno son los encargados de definir la matriz de accesos de su área de acuerdo a las funciones de los cargos.

- ✓ El jefe de área es responsable de verificar semestralmente los derechos de accesos en las plataformas, servicios de red y sistemas de información.
- ✓ Los usuarios que tienen acceso a las plataformas, servicios de red y sistemas de información son responsables de las acciones realizadas en los mismos.

3.3 Gestión de Contraseñas

- ✓ El administrador de cada sistema de información es responsable de asegurar que este solicite usuario y contraseña para permitir el acceso.
- ✓ El administrador de cada sistema es responsable de asegurar que este solicite cambio de contraseña cada vez que esta es reestablecida manualmente a un usuario.
- ✓ El colaborador es responsable de asegurar la privacidad de las contraseñas asignadas para acceder a los sistemas de información.
- ✓ El colaborador es responsable de establecer una contraseña segura, que cumpla con las siguientes características:

    - ➢ La longitud de la contraseña debe ser mínimo de 8 caracteres.
    - ➢ Las aplicaciones en las cuales la tecnología utilizada no contemple una longitud mínima de ocho caracteres, la longitud mínima deberá ser la máxima contemplado por el sistema.
    - ➢ La contraseña debe estar compuesta por una combinación de letras Mayúsculas, minúsculas, caracteres numéricos y símbolos especiales como los siguientes: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
    - ➢ No debe usarse una palabra o nombre común que aparezca en un diccionario.
    - ➢ No debe haber una relación obvia con el usuario, sus familiares, el grupo de trabajo u otras asociaciones parecidas.
    - ➢ Debe ser cambiada con una periodicidad de 90 días.
    - ➢ El administrador del sistema debe utilizar contraseñas diferentes como usuario y como administrador.
    - ➢ Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.
    - ➢ No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
    - ➢ Es responsabilidad del administrador de cada sistema establecer los mecanismos para que la contraseña asignada al usuario le sea transmitida de la manera más confidencial posible.

- No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada por terceros.
- No se debe almacenar la contraseña en la computadora. Algunos cuadros de diálogo presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esa opción.
- Las aplicaciones deben almacenar las contraseñas en forma cifrada.
- Las contraseñas predefinidas que traen los equipos y aplicaciones, deben cambiarse inmediatamente al ponerse en operación.
- Las contraseñas deben cambiarse cuando una persona que tiene acceso a cuentas privilegiadas compartidas, se ha retirado o ha sido relevada de sus deberes.

✓ El administrador de cada sistema es responsable de asegurar que las contraseñas que se transmitan a través de redes públicas, estén protegidas contra acceso no autorizado mientras se encuentren en tránsito.

3.4 Activación de Políticas de Seguridad a Nivel de Usuarios

✓ El administrador de cada sistema es responsable de habilitar las contraseñas con los siguientes parámetros:

- Duración: antes de expirar 90 días
- Longitud Mínima: 8 caracteres
- Recordación: Mínimo 3 contraseñas anteriores
- Bloqueo de cuentas: Mínimo después de 5 intentos
- Resetear el conteo de intentos de acceso después de 30 minutos

✓ El administrador de cada sistema es el responsable de verificar semestralmente que los parámetros se encuentren activos.
✓ El usuario es responsable de bloquear su equipo en el momento en que se retire de su puesto de trabajo a una zona donde pierda visibilidad de este.
✓ Para los equipos de comunicaciones como enrutadores y Firewall que requieren contraseñas para examinar o modificar configuraciones se debe también aplica el estándar de contraseñas.

3.5 Registro de Eventos

El registro de eventos se realiza de forma automática por medio de una herramienta (SIEM) donde se capturan los eventos de seguridad de la información y disponibilidad de los recursos tecnológicos, que serán almacenados para consulta en línea por un periodo de seis meses para la validación de consultas. El área de seguridad informática es responsable de monitorear los eventos que se presenten.

3.6 Escritorio y Pantalla Despejados

Todos los colaboradores de la Compañía son responsables de la administración de su escritorio físico y de la pantalla de su equipo de cómputo, para lo cual debe cumplir los siguientes lineamientos:

- ✓ Almacenar de manera segura (con llave u otro control) medios de almacenamiento como (CD/DVD, dispositivos de almacenamiento masivo (memorias USB, discos extraíbles)), papelería y otros elementos que puedan contener información sensible o confidencial; mientras esté ausente de su puesto de trabajo y sin visibilidad de su escritorio.
- ✓ Retirar inmediatamente de la impresora los documentos que contengan información sensible o confidencial.
- ✓ No ingerir alimentos cerca del equipo de cómputo o de la documentación de la Compañía.
- ✓ Al finalizar la jornada laboral o al ausentarse del puesto de trabajo se deben asegurar con llave los cajones, gabinetes o archivadores.
- ✓ Únicamente la información clasificada como pública o interna podrá estar en el escritorio sin custodia.
- ✓ En la pantalla no debe permanecer ningún icono que ejecute un programa que no sea nativo de la plataforma del sistema operativo o archivos o acceso directo a archivo.
- ✓ Para el personal operativo en la pantalla solo deben permanecer los iconos de acceso directo a las diferentes herramientas de gestión de la compañía.

3.7 Uso de los Recursos Compartidos en la Red (Carpetas)

Los colaboradores, proveedores, contratistas, clientes y terceros que tengan acceso a los recursos compartidos de la compañía deben cumplir con las siguientes normas:

- ✓ Es responsabilidad de la dirección de tecnología asegurar que el acceso a la red (inalámbricas y físicas) para el uso de recursos compartidos cuente con métodos de validación de acceso implementados
- ✓ No es permitido guardar o intercambiar archivos de audio en cualquier formato (Wav, Mp3, etc.) para fines personales.
- ✓ No es permitido guardar o intercambiar archivos de videos y/o fotografías personales en cualquier formato.
- ✓ No es permitido compartir o almacenar información de la compañía en medios públicos de almacenamiento en la nube no autorizados por la Compañía.
- ✓ Todo colaborador debe validar con el dueño de la información antes de eliminar cualquier información del recurso compartido.
- ✓ Se debe guardar únicamente información relacionada con las funciones de su cargo.

3.8 Protección de datos personales

La compañía da cumplimiento a las normas de protección de datos personales definidos en la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas que lo complementan, así como al Manual de Tratamiento de Datos que se ha adoptado para el efecto.

3.9 Uso del Correo Electrónico Corporativo

Todos los colaboradores y terceros que se les asigne y tengan acceso al servicio de correo electrónico de la Compañía son responsables por su utilización.

- ✓ Se debe ser respetuoso y utilizar un vocabulario adecuado al momento de redactar un correo electrónico.
- ✓ La cuenta de correo electrónico es personal e intransferible, por lo que no debe proporcionarse acceso a otras personas.
- ✓ No está permitido distribuir mensajes con contenidos diferentes a temas laborales o correos SPAM de cualquier índole.
- ✓ Toda solicitud de envío de correos electrónicos masivos (más de 100 destinatarios) debe ser gestionada por medio del área de comunicaciones.
- ✓ Es responsabilidad del colaborador solicitante del envío del correo masivo, revisar el contenido y estructura del mensaje, así como la definición de los destinatarios que lo recibirán.
- ✓ No se permite utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.

- ✓ No se debe modificar o alterar la configuración preestablecida por los ingenieros de la mesa de servicios para el correcto funcionamiento del correo electrónico.
- ✓ La firma del correo electrónico debe ser la definida por la Compañía.
- ✓ Si se recibe un correo de origen desconocido, consúltelo inmediatamente con la mesa de servicios, no se debe abrir o ejecutar archivos adjuntos de correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc.).
- ✓ Proporcione su dirección de correo electrónico para asuntos laborales.
- ✓ Evite difundir las direcciones de correo electrónico de la Compañía para asuntos diferentes a los laborales.
- ✓ Es responsabilidad de los usuarios dar aviso al área de seguridad de la información y mesa de servicios de cualquier fallo de seguridad de su cuenta de correo electrónico, incluyendo su uso no autorizado, pérdida de la contraseña o configuración, etc.
- ✓ Ante el retiro de un colaborador es responsabilidad del jefe inmediato, solicitar la entrega de la información de la compañía.
- ✓ Es responsabilidad del jefe ante la creación de cuentas de correo electrónico genéricas, asignar un responsable para cada cuenta.
- ✓ Al reportar un retiro de cuenta de correo electrónico este quedará en estado inactivo por 30 días, pasado este tiempo, toda la información de la cuenta será borrada definitivamente, sin la posibilidad de recuperarla.
- ✓ Todo colaborador que reciba un correo electrónico e identifique que no es destinatario correcto, debe informar inmediatamente al remitente, y no hacer uso de la información contenida en este.
- ✓ Los mensajes de correo electrónico son considerados prueba legal, ante las autoridades competentes, es por esto que la Compañía podrá hacer uso de estos, como instrumento probatorio de requerirlo.
- ✓ No está permitido el direccionamiento automático, envió o almacenamiento de correos de la empresa en cuentas de correo personales no corporativas
- ✓ Toda la información contenida en el correo electrónico es propiedad de la compañía.

3.10 Uso de la Mensajería Instantánea

Está restringido el uso de programas de Mensajería Instantánea, como (Messenger MSN, Yahoo Messenger, Google Talk, páginas web de conexión para mensajería instantánea, como Ebuddy, Iloveim, Sinmessenger o páginas web de chat). Solo se permitirá el uso de la herramienta que la Compañía ha dispuesto para tal fin.

3.11 Propiedad Intelectual

Los colaboradores son responsables de respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual para toda la información que se instala, copia o descarga de internet.

3.12 Segregación de funciones

Toda tarea en la cual los colaboradores tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir la concentración de funciones y evitar el uso no autorizado o modificación sobre los activos de información de la Compañía. Por tal razón todos los sistemas de disponibilidad crítica o media deben implementar las reglas de acceso que aseguren la segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

3.13 Uso de Internet, Intranet y Almacenamiento en la Nube

Internet:

La Compañía provee el servicio de internet para empleados, proveedores, contratistas, clientes y terceras partes que se encuentren dentro de nuestras instalaciones y requieran de la prestación de este servicio de manera contralada, se deben seguir los siguientes lineamientos:

- ✓ El servicio de Internet esta designado para el uso laboral, con los permisos otorgados de acuerdo al nivel de acceso autorizado.
- ✓ Con el propósito de garantizar la seguridad de la información y de la infraestructura tecnológica, la compañía se reserva el derecho de filtrar el contenido al que el usuario puede acceder a través de internet desde los recursos y servicios propiedad de la compañía, así como a monitorizar y registrar los accesos realizados desde los mismos.
- ✓ Por motivos de seguridad y para evitar el contagio de virus, se prohíbe la descarga de software desde Internet; en caso de requerir algún programa se debe comunicar con la línea de soporte (25000).

- ✓ Está prohibido la descarga de material gráfico que contenga actividad sexual, nudismo, violencia o cualquier otra actividad que vaya en contra de los valores corporativos de la Compañía. El incumplimiento de esta directriz será considerado una falta grave, sancionada de acuerdo al procedimiento de sanciones disciplinarias.
- ✓ Se prohíbe la utilización de este recurso para cualquier actividad que atente contra la ética y buen nombre de Compañía.
- ✓ Se recomienda no dejar abiertas páginas que se actualizan periódicamente ni varias conexiones simultáneas, ya que consumen recursos y congestionan la de red innecesariamente.
- ✓ La información usada, consultada, publicada o transmitida a través de internet debe ser de uso únicamente corporativo por lo tanto no está permitido el almacenamiento, acceso, transmisión y retransmisión de:

    - ➢ Mensajes difamatorios, calumniosos, amenazantes o lesivos a los intereses de la compañía, de los colaboradores o de otras personas o instituciones, cualquiera sea su naturaleza.
    - ➢ Mensajes de naturaleza racial, política, bélica, religiosa o cualquier otro que pueda generar discriminación.
    - ➢ Cartas de cadena, cualquiera que sea su naturaleza.
    - ➢ Publicidad, ventas, mercadeo, promociones, apuestas, etc., a título personal del colaborador.
    - ➢ Material que viole la propiedad intelectual: derechos de autor, marcas registradas, patentes, secretos industriales o comerciales, música, video, fotos e imágenes.

- ✓ Es responsabilidad de los colaboradores, proveedores, contratistas, clientes y terceras partes a quienes se les otorgue acceso al servicio de internet hacer buen uso de los recursos informáticos que la compañía le suministra para el desarrollo de sus actividades.
- ✓ Es responsabilidad de los colaboradores, proveedores, contratistas, clientes y terceras partes a quienes se les otorgue acceso al servicio de internet no gestionar inscripciones a boletines y/o notificaciones vía correo electrónico que no se encuentren asociadas estrictamente a temas laborales.
- ✓ Todo acceso a internet de proveedores, contratistas, clientes, visitantes y terceras partes debe ser aprobado y gestionado por el responsable del tercero.
- ✓ Los administradores del servicio de internet (Infraestructura Tecnológica Ingenieros IT) podrán tomar acciones correctivas con aquellos accesos que generen consumo excesivo del recurso y que impacten negativamente la calidad del servicio, así mismo podrán restringir de manera unilateral el acceso a sitios y páginas que por alguna circunstancia vayan en contra de

las políticas corporativas o que representen un riesgo para los sistemas y la infraestructura tecnológica de la compañía.

Intranet:

La Intranet es una herramienta utilizada para dar a conocer a todo el personal, información de interés general, por lo cual la información disponible en la intranet, es para uso interno y no puede ser reproducida o retransmitida a terceros.

Almacenamiento en la Nube:

- ✓ Solo se almacena información en la nube en las herramientas (OneDrive y Share Point) administradas por la Compañía.
- ✓ No está permitido el almacenamiento de información de propiedad de la Compañía en servicios no licenciados o no autorizados.
- ✓ Es responsabilidad del usuario propietario de la cuenta:
  - ➢ Garantizar que la información que se almacene en la herramienta seleccionada cumpla con la Política de Clasificación y Etiquetado de la información.
  - ➢ No almacenar información personal en el sitio corporativo.
  - ➢ Gestionar los permisos que asignen a otras personas para acceder a la información almacenada.
  - ➢ Si la cuenta debe ser eliminada, facilitar la custodia de la información entregando acceso a su jefe inmediato.

3.14 Protección contra software malicioso

Es responsabilidad de la Dirección de tecnología asegurar que todos los recursos informáticos estén protegidos mediante herramientas y software de seguridad como antivirus, anti-spam, antispyware, agentes o procesos que permitan las actualizaciones de sistema operativo de manera periódica, para que estos protejan contra código malicioso. Se deben llevar a cabo acciones necesarias para proteger la red de la Compañía manteniendo la consola de antivirus actualizada, monitoreando los eventos de esta y recuperándose de la introducción de software malicioso, capacitar a los usuarios en cuanto a las herramientas utilizadas y a la prevención de estas amenazas. También será encargado de autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

- ✓ Así mismo, no está permitido:

  - ➢ La desinstalación y/o desactivación de software y herramientas de seguridad.
  - ➢ Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, y/o que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica.

- ✓ La dirección de tecnología es responsable de tener acceso a fuentes de conocimiento que le permita identificar tendencias en virus y debilidades en las plataformas, manteniendo contacto con los proveedores de antivirus en el mercado, para determinar y seguir las recomendaciones de terceros en caso de ataques o vulnerabilidades.

3.15 Gestión de vulnerabilidades técnicas

- ✓ La dirección de tecnología es responsable de:

  - ➢ Identificar, valorar, revisar y gestionar las vulnerabilidades técnicas del conjunto de plataformas tecnológicas que soporten los sistemas de información críticos, con el objetivo de realizar la corrección sobre los hallazgos arrojados.
  - ➢ Verificar por lo menos una vez cada trimestre la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la Compañía.
  - ➢ Generar por lo menos una vez al año el plan de pruebas de vulnerabilidades para las plataformas críticas del negocio cuya viabilidad técnica y de administración lo permita.
  - ➢ Implementar los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas.

3.16 Instalación de Software

Las únicas áreas autorizadas para realizar instalación de software son:

- ✓ Alta disponibilidad de E-Bussines (Servidores)
- ✓ Seguridad informática de ITO (Servidores)
- ✓ Soporte técnico especializado

Durante el proceso de instalación, se debe asegurar:

- ✓ El software propietario debe contar con su respectiva licencia y en el caso del software libre debe estar permitido el uso comercial.
- ✓ El instalador únicamente será descargado de la página oficial del fabricante.
- ✓ En caso que algún colaborador requiera realizar instalación de software, tiene que contar con la autorización de la jefatura de área, que notificará al oficial de seguridad y control interno. Se debe generar evidencia de dicha autorización y de la duración de la misma.

3.17 Gestión de seguridad en redes

- ✓ La dirección de tecnología es responsable de definir e implementar los controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Compañía, considerando la ejecución de las siguientes acciones:

    - ➢ Establecer controles para proteger la confidencialidad, disponibilidad e integridad de los datos y de los sistemas de información.
    - ➢ Garantizar mediante actividades de supervisión, que los controles se aplican en la infraestructura que soporta el procesamiento e intercambio de información.
    - ➢ Mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica.
    - ➢ Identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios, cuando estos se contraten externamente.
    - ➢ Establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica.
    - ➢ Velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos.

3.18 Teletrabajo o Conexión Remota

- ✓ El desarrollo de teletrabajo es gobernado por la norma **VGHDH002-Teletrabajo**, es responsabilidad de los jefes y de los colaboradores que solicitan realizar teletrabajo asegurar que cumplen con cada uno de los requisitos exigidos por la norma.
- ✓ La dirección de tecnología es responsable de asegurar que los medios de conexión remota a los sistemas de la Compañía tengan implementados controles de autenticación y encripción.

3.19 Medios Removibles

- ✓ Sólo los empleados autorizados por la dirección de cada unidad de negocio pueden hacer uso de los medios de almacenamiento removibles.
- ✓ El empleado es responsable de asegurar el dispositivo a fin de no poner en riesgo la información de la Compañía.
- ✓ El almacenamiento, etiquetado y eliminación de cualquiera de estos medios de almacenamiento, debe estar de acuerdo con el esquema de clasificación y seguir los procedimientos relacionados con la GESEGU EBS PR 001 - Gestión de activos de información.
- ✓ En caso de un medio removible se vaya a retirar de la operación porque no se requiere se le debe aplicar el procedimiento de borrado seguro

3.20 Relación con proveedores

- ✓ El colaborador responsable del proveedor o contratista debe asegurar que:
  - ➢ Antes de iniciar la ejecución del contrato, suscriba un acuerdo de confidencialidad de la información, donde se comprometa a no divulgar, usar o explotar la información a la que tenga acceso.
  - ➢ Gestionar los accesos a los sistemas de información, servicios de tecnología y equipos de cómputo que requiera el proveedor o contratista para la ejecución del contrato.
  - ➢ Autorizar por escrito el envío, copia o tratamiento de información de propiedad de la Compañía por parte de los proveedores.
  - ➢ Revisar los requisitos de seguridad de la información que deben cumplir de acuerdo al servicio que presta. Estos requisitos deben estar incluidos en el contrato o en los acuerdos de niveles de servicio, incluyendo el derecho a realizar seguimiento y revisión de los servicios prestados que la Compañía considere necesarios.

3.21 Desarrollo seguro

- ✓ La dirección de tecnología es responsable de asegurar que los desarrollos internos y externos de los sistemas de información cumplan con los requisitos de seguridad definidos en la fase inicial del ciclo de desarrollo, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido.

- ✓ Los desarrolladores de los sistemas de información deben considerar las siguientes practicas:

  - **Principio del Menor Privilegio:** Las cuentas de usuario deben tener la menor cantidad de privilegios para llevar a cabo sus actividades. Estos pueden reflejarse en una matriz de gestión de accesos por rol. Esto abarca derechos de usuario, permisos de recursos tales como: CPU, memoria, red y sistemas de archivos.

  - **Seguridad por Defecto:** Todos los accesos que se hagan a los sistemas deben ser validados, el sistema debe exigir la complejidad y cambio periódico de las contraseñas. Adicionalmente se deben cambiar las credenciales por defecto y eliminar código de ejemplo.

  - **Defensa en Profundidad:** Se debe proveer a la aplicación de más de un mecanismo de defensa, con el fin de proteger los servidores de bases de datos los cuales contienen información sensible.

  - **Manejo Adecuado de Errores:** Se debe utilizar mecanismos de manejo de errores tipo try catch con el fin de publicar la información mínima requerida por el usuario y evitar dar información adicional a los atacantes.

  - **Validación de Datos de Entrada:** Todos los datos de entrada de la aplicación deben ser verificados y sanitizados para garantizar que lo que está ingresando a los sistemas es lo esperado y además evitar inyecciones de código.

  - **Criptografía:** Para intercambiar información sensible utilizar protocolos para cifrar las comunicaciones, y en el caso de almacenamiento la información confidencial debería estar cifrada utilizando algoritmos fuertes y claves robustas.

- **Control de Cambios:** Cualquier cambio que se haga debería quedar documentado, esto facilitará modificaciones futuras.

- **Manejo de Logs:** Las aplicaciones deben dejar rastro para el seguimiento de las principales actividades realizadas por los usuarios, por ejemplo: actividades de autenticación y de inserción y modificación de registros en bases de datos. De igual forma, se debe manejar registros de auditoria enfocado en el manejo de errores de la aplicación.

- **Gestión de Vulnerabilidad Técnica:** Hacer un seguimiento de las tecnologías utilizadas para el desarrollo. Estas van evolucionando y cualquier mejora que se haga puede dejar obsoleta o inseguras versiones anteriores.

- **Manejo de Sesiones:** Se deben implementar medidas de manejo de sesión que mitiguen los principales ataques: predicción de sesión, fijación o secuestro de sesión. Adicionalmente se debe incluir como mínimo los siguientes elementos: establecer un time out de sesión, establecer un tiempo máximo de validez de sesión, utilizar cookies no persistentes, invalidar los identificadores de sesión, no reutilizar los identificadores de sesión y usar identificadores de sesión aleatorios.

- **Pruebas de Seguridad y de Aceptación:** Todo desarrollo realizado deberá contemplar las pruebas de seguridad y de aceptación dependiendo del tipo de proyecto (Corte o robustecimiento de producto lo acepta el Gerente de producto o si es proyecto con cliente, el cliente es quien aprueba el cumplimiento de estos requisitos), de acuerdo a lo establecido en el proceso de Calidad de Productos y Servicios.

3.22 Revisión de seguridad de la información

- ✓ La alta dirección es responsable de contratar la revisión anual del SGSI con fin de validar la eficacia de los controles y cumplimiento de la norma ISO 27000.
- ✓ La dirección de tecnología es responsable de que se realice una revisión semestralmente de manera aleatoria los sistemas de información con respecto al cumplimiento de las parametrizaciones, políticas y procedimientos de seguridad de la información.
- ✓ Los líderes de proceso deben revisar semestralmente el cumplimiento de las políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad.

3.23 Clasificación de la Información

Todos los colaboradores de la Compañía son responsables de clasificar, etiquetar y dar el tratamiento a la información de acuerdo con el procedimiento de Clasificación y Etiquetado de la Información a excepción de la información de tipo "Público" que no requiere etiquetado.

3.24 Controles Criptográficos

La Dirección de Tecnología es responsable de:

- ✓ Asegurar que los sistemas de información o aplicativos que requieran transmitir información confidencial o privada, cuenten con protocolos de cifrado de datos actuales.
- ✓ Verificar el cumplimiento del procedimiento de gestión de llaves criptográficas asegurando la apropiada gestión de las llaves en todas sus etapas: generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción.

3.25 Transferencia de información

- ✓ Toda transmisión de información debe contar con los mecanismos de protección definidos por la Compañía de acuerdo al tipo de información definida en el procedimiento de "Clasificación de Información".

3.26 Seguridad física

- ✓ El ingreso de personal a las instalaciones de la Compañía se gobierna por la norma corporativa **VGHBN050- Ingreso de personal a las instalaciones de la Compañía Carvajal**
- ✓ Las áreas que procesan o almacenan información sensible o confidencial, deben contar con medidas de control de acceso físico.
- ✓ Los privilegios de acceso a las áreas seguras y restringidas de la Compañía deben ser revisados, actualizados y monitoreados por lo menos dos veces al año.
- ✓ En las instalaciones calificadas como áreas seguras:
  - ➢ No se permite el ingreso de visitante sin el acompañamiento de uno de los operadores responsables del área.
  - ➢ No se permite el ingreso de alimentos, ni bebidas.

- Debe registrarse en una bitácora el ingreso de visitantes

3.27 Protección, ubicación, suministro eléctrico de los equipos de cómputo y seguridad de cableado

- ✓ Para la protección, ubicación, suministro eléctrico de los equipos de cómputo y seguridad del cableado, se seguirán los lineamientos definidos por la norma corporativa "**VECTI007- Seguridad de los equipos informáticos**"
- ✓ Los equipos que hacen parte de la infraestructura, tales como, servidores, equipos de comunicaciones y seguridad informática, centros de cableado, plantas eléctricas, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, estaciones de trabajo y dispositivos de almacenamiento y comunicación que contengan o brinden servicios de soporte a la información confidencial o privada, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado. De igual manera, se deben mantener alejados de sitios que puedan tener riesgo de afectación por fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo.
- ✓ Los usuarios no deben mover o reubicar los equipos de cómputo o comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin autorización de las jefaturas de las áreas de tecnología respectivas.

3.28 Uso aceptable de equipos

- ✓ Los recursos tecnológicos de la Compañía deben ser utilizados para la operación de los negocios, no deben ser usados para fines personales que pongan en riesgo la seguridad de la información, que vayan en beneficio de terceros o actividades en contra de los principios y valores de la Compañía.

- ✓ El responsable del equipo debe asegurar que:

  - Todo el software esté licenciado, incluyendo música, libros, imágenes y video.
  - Todo el software instalado ha sido previamente aprobado para su uso en la Compañía.
  - Las novedades (fallas, incidentes de seguridad, pérdidas, traslados, actividades sospechosas, etc.) son reportadas al responsable del manejo de los recursos tecnológicos de la empresa.
  - Utiliza mecanismos físicos para evitar el hurto o la pérdida de su equipo, tales como:

- Cable de protección o guaya de seguridad para portátiles
- Dejar el equipo bajo llave al terminar su labor diaria
- Marcado físico del equipo si este pertenece a la Compañía.
- Autorización escrita del Jefe inmediato para retirarlo de la Empresa

✓ Los colaboradores deben reducir el riesgo de daño causado en equipos de cómputo por acciones inadecuadas (consumo de alimentos o bebidas, obstrucción de ventilación, ubicación inadecuada, entre otros)

3.29 Dispositivos Móviles por Empleados

✓ No está permitido el almacenamiento de información de la Compañía en dispositivos que no sean asignados por esta.
✓ Los colaboradores tienen permitido consultar el correo electrónico en sus dispositivos móviles
✓ Los teléfonos celulares deben tener activo el mecanismo validación de acceso.
✓ Debe tener el parámetro de bloqueo automático de pantalla activo con un tiempo máximo de 1 minuto
✓ Es responsabilidad del colaborador en caso de pérdida del celular o equipo portátil, realizar el cambio de las credenciales de acceso a la plataforma Office 365 en el menor tiempo posible y reportar a la línea 25000 la pérdida del computador para que procedan a cambiar la contraseña de dominio.
✓ Los equipos portátiles deben tener cifrado completo del disco.

3.30 Periodo de revisión

Este documento de políticas de seguridad de la información serán objeto de revisión al menos cada 6 meses.