Política:

POLÍTICAS DE INFORMÁTICA (TI)

Fecha	:	01-12-2020
Versión	:	Versión 4
Código	:	PLT-010-E- SSCC_PLTTI
Elaborado por	:	Carlos Martinez.
Aprobado por	:	Iván Vera.
Vigencia	:	1 año a contar de la publicación.

1. Control de Cambios

Versión	Punto	Cambio	Fecha	Responsable
V4	Actualización	Varios	01-12-2020	Carlos Martínez / Eduardo Quitral / Sebastián Garrido.

2. Objetivo de la Política

El objetivo de las políticas de TI es la asignación y uso aceptable de los Recursos Computacionales, Acceso Lógico, Políticas de Acceso Físico, Políticas de Comunicación Inalámbrica y Clasificación de Datos. Por otra parte, en el presente documento se entregan las políticas corporativas de Empresas FG con respecto al uso, acceso e instalaciones de los servicios informáticos, incluyendo Políticas de asignación de los recursos computacionales, Políticas de Uso, Políticas de Acceso Lógico, Políticas de Acceso Físico, Políticas de Comunicación Inalámbrica, Control de Cambios, Operaciones Informáticas y Clasificación de Datos. Las políticas serán aplicables a todos los colaboradores que utilicen computadoras, sistemas y servicios de redes del grupo de Empresas FG, incluyendo los colaboradores, contratistas, subcontratistas y consultores.

3. Alcance / Tipo de Política

Alcance Específico: Todos los colaboradores de Empresas FG y Usuarios Invitados entre los cuales se pueden distinguir, proveedores, prestadores de servicios, contratistas, subcontratistas, clientes, asesores, entre otros.

Alcance General: Empresas FG en todas sus instalaciones y oficinas que alojen Sistemas de Información, aplicaciones, instalaciones e infraestructura que contribuyan a la actividad empresarial.

4. Gobernabilidad

La política será monitoreada, en su correcta ejecución, por la Gerencia de TI.

5. Índice

6. Definiciones, Uso de Lenguaje

6.1. **Recursos Computacionales:** Relación de tecnologías disponibles para el procesamiento de información, entre ellos, computadoras, impresoras, scanner, servidores, dispositivos móviles, dispositivos de red, dispositivos inalámbricos, etc.

6.2. **Recurso TI:** Disponibilidad de Horas hombre destinadas a la solución de problemas, respuesta a consultas y requerimientos en general a la gerencia de TI, de la unidad Servicios Compartidos.

6.3. **TI.:** Tecnología de la Información.

6.4. **Servicios de Redes:** Envío, recepción y uso de información a través de la red informática, Internet, Intranet, correo electrónico, OneDrive, teletrabajo, gestión documental y cualquier otro servicio informático en línea.

6.5. **Control de proceso:** Control establecido en un proceso para garantizar el cumplimiento de los objetivos de los sistemas e infraestructura.

6.6. **Estructuras de Datos:** El diseño o arquitectura de la base de datos que sustenta a una aplicación.

6.7. **Usuario.** Colaborador, proveedor, cliente, contratista, subcontratista y consultor, a los cuales se les da acceso a los recursos computacionales e información de la empresa.

6.8. **Mecanismo de Autenticación:** Mecanismos que obligan al usuario a demostrar su identidad antes de tener acceso a los recursos de información a través de dispositivo o sistema.

6.9. **Perfil de usuario:** Agrupación o conjunto de privilegios de accesos a sistemas en base a las funciones del trabajo que desarrolla el colaborador.

6.10. **Privilegios:** Permisos por los cuales se otorgará acceso a la información y/o recursos para realizar las actividades correspondientes al cargo o función de un colaborador.

6.11. **Instalación Central de Datos:** Instalación en la cual se ubican servidores principales de procesamiento de información y equipos informáticos relacionados.

6.12. **Plan de TI:** Plan para el desarrollo e implementación de diversas soluciones tecnológicas de apoyo a los procesos de negocio de la empresa, definido durante un período de tiempo.

6.13. **Modo de Producción / Modo de Operación Real:** Modo en el cual las aplicaciones son utilizadas por los usuarios de la empresa para procesos de transacciones comerciales en vivo.

6.14. **Modo de Prueba de Sistema:** Modo en el cual el Departamento de Informática realiza una prueba de la unidad/sistema.

6.15. **Gestión del cambio**: Proceso de control de las modificaciones introducidas al hardware, software, firmware, documentación para garantizar que una protección de la información contra cambios erróneos o no autorizados.

6.16. **Aplicaciones Críticas:** Aplicaciones que tienen un impacto en los informes financieros o de los cuales depende el desarrollo normal de la actividad empresarial.

7. Políticas

7.1. **POLÍTICA DE ASIGNACIÓN DE RECURSOS COMPUTACIONALES.**

El objetivo de esta política es establecer el nivel de perfil adecuado para la adquisición y entrega de los recursos computacionales a los colaboradores de Empresas FG.

7.1.1. **Solicitud de adquisición.**

Toda necesidad de recursos computacionales debe solicitarse a la Gerencia de TI de servicios compartidos, con el objetivo de evaluar los niveles de compatibilidad para el uso empresarial, definir estándares y mantener el control de licenciamientos de software. Esta solicitud debe realizarse al menos una semana antes de la necesidad para los tiempos de evaluación, cotización y compra.

7.1.2. **Perfil de uso de recursos computacionales.**

La Gerencia de TI, deberá definir perfiles de uso, basado en los requerimientos de software, necesarios para el cumplimiento de funciones designadas al cargo.

7.1.3. **Compras y Control de inventario.**

Basado en la evaluación de solicitudes de adquisición, la Gerencia de TI solicitará al menos 3 cotizaciones, según el perfil de uso y definirá con las Gerencias correspondientes, la mejor opción en costos, tiempos de entregas y garantías. Una vez adquirido el recurso computacional, se procederá al registro de inventario para su control de activo y se asignará al soporte correspondiente para su control de entrega, posterior a la instalación de licencias, preparación del entorno y sus respectivas configuraciones.

El Gerente de TI solicitará con la entrega de cualquier recurso computacional un anexo de responsabilidad llamado "Responsabilidad de Asignación de Recursos Computacionales", debiendo estos documentos ser firmados.

La empresa no reembolsara fondos, no aceptará facturas y no entregará soporte a los recursos computacionales, que no hayan sido adquiridos por la Gerencia de Informática o no esté bajo su control de inventario.

7.1.4. **Control de Garantías.**

La Gerencia de TI, deberá exigir garantías a los proveedores de los recursos computacionales adquiridos y ser responsable de la gestión de cumplimiento según condiciones y plazos, en caso de ser necesario.

7.1.5. **Ciclo de vida de los Recursos computaciones.**

Se establece que los recursos computacionales, tendrán un ciclo de vida no superior a tres años desde su adquisición y en disposición de renovación tecnológica. Los recursos computacionales dados de baja podrán ser ofertados al empleado asignado según valor residual igual al 10% del costo de adquisición. En el caso que, el empleado desista de la compra, el recurso computacional será publicado para su subasta en el sitio de intranet de empresas FG.

7.1.6.**Recursos Computacionales de colaboradores desvinculados.**
Sera de responsabilidad directa de la jefatura correspondiente, cuando se ejecute el proceso de desvinculación, la correcta recepción conforme de los recursos computacionales asignados.

La jefatura directa, deberá realizar la solicitud a la Gerencia de TI en forma previa a la desvinculación.

a) Resguardo de los datos del computador y correo electrónico.
b) Listado de los recursos computacionales asignados al colaborador a desvincular.
c) La jefatura directa, deberá definir si el recurso computacional será ofertado con descuento en el cálculo de finiquito.
d) Se deprecia en 36 meses teniendo como valor residual el 10% del valor de la adquisición del recurso computacional. En el caso de que el recurso computacional se venda con anterioridad, el prorrateo se realizara por los meses transcurridos hasta la fecha de la venta.

7.1.7.**Proyectos Tecnológicos.**
Todos los proyectos futuros o actuales deben ser presentados por las gerencias de divisiones a la gerencia de TI y en conjunto con la Gerencia de Servicios Compartidos se hará su revisión y aprobación o rechazo. Todo nuevo proyecto de TI, el gerente de división debe presentarlo al director ejecutivo para su aprobación.

a) Los proyectos TI aprobados, serán de responsabilidad en su desarrollo, pruebas y ejecución de las gerencias de divisiones solicitantes.
b) La Gerencia de TI será responsable de facilitar la infraestructura y/o plataforma necesaria para mantener disponibilidad y seguridad de los proyectos TI aprobados.

POLÍTICA DE USO ACEPTABLE DE LOS RECURSOS COMPUTACIONALES.
El objetivo de esta política es definir el correcto uso de los recursos computacionales asignados a los colaboradores para el fiel cumplimiento de sus obligaciones laborales.

7.1.8.**Los Recursos computacionales son para Fines Empresariales.**
Los recursos computacionales que provee Empresas FG son otorgados a sus usuarios para fines relacionados con los procesos de cada área de trabajo.

a) Las comunicaciones electrónicas realizadas a través de los recursos computacionales de Empresas FG., considerando toda la comunicación electrónica enviada, recibida, o almacenada como mensajes empresariales, inclusive mensajes personales son propiedad intelectual de Empresas FG.
b) Los usuarios no deben utilizar estos recursos para su beneficio personal, lo que incluye compartir accesos de claves de identidad de usuarios.
c) No se debe utilizar el acceso a Internet para realizar trabajos lucrativos no autorizados.
d) Se restringe el uso personal de cada recurso, evitando interferir con el rendimiento laboral.

7.1.9.**Monitoreo y Privacidad.**
La Gerencia TI es el responsable por el Monitoreo, gestión, mantenimiento y soporte de los recursos de Empresas FG. Así mismo es el responsable de proveer seguridad y disponibilidad.

a) Ningún usuario debe esperar privacidad con respecto a cualquier mensaje electrónico. Si bien no es una práctica habitual, Empresas FG se reserva el derecho de monitorear, acceder, revisar, copiar, almacenar o borrar cualquier comunicación electrónica, inclusive mensajes personales, del sistema para cualquier fin, según lo estime pertinente.

7.1.10. **Respaldo de correos electrónicos.**
Se requerirá que los usuarios conserven los mensajes de correos electrónicos relacionados con aspectos fundamentales a los procesos de negocio. Los mensajes de correo electrónico que no cumplan esto, se deberán borrar cuando ya no se los necesite. Se mantendrá una retención de 15 días de los mensajes borrados por usuarios en los servidores para restauración en el caso que sea necesario.

7.1.11. **Actividad Prohibida y uso del buen Juicio.**

a) Queda prohibido el uso de comunicaciones electrónicas para establecer cualquier comunicación o acción que sea amenazante, discriminatoria (por motivo de raza, credo, edad, sexo, discapacidad física, orientación sexual, u otros), difamatoria, calumniosa, obscena, violenta, intimidante, degradante, pornográfica u hostigante.
b) No se divulgará información personal en las comunicaciones electrónicas, sin previa autorización por escrito de la jefatura de cada área de Trabajo.
c) Las comunicaciones electrónicas de Empresas FG no se utilizarán para fines lucrativos o político partidistas.
d) Queda prohibido la destrucción o alteración de comunicaciones electrónicas, con el fin de perjudicar o dañar a un empleado o a Empresas FG.
e) Los Recursos computacionales no se utilizarán para fines ilegales o ilícitos cualesquiera sean, ni para violar los derechos de propiedad intelectual de terceros.
f) Los usuarios no deben intentar burlar o alterar las medidas de seguridad tanto en la infraestructura de red como en cualquier sistema conectado o accesible mediante Internet. Si un usuario identifica o percibe un problema de seguridad real o posible, deberá contactar inmediatamente a la casilla de correo electrónico soporte@empresasfg.com con copia al Gerente de TI.
g) Los usuarios utilizarán el mismo buen juicio para preparar comunicaciones electrónicas que para preparar una copia impresa de un memorándum.
h) Los usuarios deben asegurarse de que los mensajes de correo electrónico sólo se envíen a usuarios con necesidades concretas de información.
i) El contenido de las comunicaciones electrónicas puede tener consecuencias financieras y comerciales considerables para el personal y pueden ser comprendidos inadecuadamente fuera de contexto. Dada

la facilidad para enviar estos mensajes, se deben tomar resguardos extras para asegurarse de que no se los envía precipitadamente.

j) Se debe tener en cuenta que los mensajes enviados desde computadoras de o desde la infraestructura de la red pueden ser leídos por otras personas además del destinatario. Por consiguiente, asegurarse de que los mensajes sean corteses, profesionales y de tipo comercial.
k) Los usuarios no deben revelar sus contraseñas a terceros, ni permitir que otra persona, empleado o no, use sus cuentas. Igualmente, los usuarios no utilizarán cuentas de otros individuos.
l) Los usuarios no podrán realizar cambios en la configuración de los recursos asignados, entre ellos, sistemas financieros y operacionales, aplicaciones de escritorio, sistemas operativos y otros.
m) Queda prohibido el acceso a sitios Internet, con potencial consumo elevado de ancho de banda, entre ellos, Descargas de Software Gratuito, Radio y TV por internet, Transmisión de medios y descargas, Compartición de archivos peer to peer.
n) Queda prohibido el uso de internet para actividades ilegales o no éticas, tales como, Organizaciones controversiales, hacking, tráfico de drogas, pedofilia, violencia explícita, pornografía y otros materiales para adultos.

7.1.12. **Propiedad Intelectual y Licencias.**

La facilidad de copiado mediante diversos sistemas de comunicación electrónicos representa un gran riesgo de violación de la propiedad intelectual. Cada usuario debe ser consiente de los derechos de terceros y debe respetarlos.

a) Los programas que puedan estar rotulados como "gratuitos", "de dominio público" y "para uso público" pueden ser gratuitos para uso personal, pero no para uso corporativo. Al descargar un programa de Internet, el uso de dicho programa puede violar los requerimientos de derechos de autor o de licencia. Siempre se debe obtener la aprobación de la Gerencia de TI., antes de utilizar cualquier paquete de programas disponibles al público.
b) No haga copias de los programas de los que tiene licencia Empresas FG.
c) Ningún usuario puede instalar programas que provengan originariamente de la computadora de su casa o de otra Empresa, salvo que pueda demostrar mediante licencia por escrito que tal uso está permitido.

7.1.13. **Protección Antivirus.**

Los usuarios pueden crear, ejecutar, reenviar, o introducir, sin saberlo, códigos informáticos diseñados para auto duplicar, dañar, o impedir de otra manera el funcionamiento de la memoria, los dispositivos de almacenamiento, sistemas operativos y programas de la computadora.

a) No se pueden cargar programas ni otros archivos en las computadoras de Empresas FG, a menos que se los analice con un programa antivirus autorizado. La inutilización de cualquier dispositivo antivirus instalado en cualquier sistema o red constituye una violación a la presente política.

7.1.14. **Medidas Disciplinarias.**

La Gerencia de TI se reserva el derecho de revocar, en cualquier momento, todo privilegio de acceso a usuarios, en caso de violación de la presente Política o de la legislación vigente, y en caso de comportamientos que alteren el funcionamiento normal de los sistemas informáticos de **Empresas FG**. No se permite ningún comportamiento que afecte negativamente la capacidad de terceros en el uso de los sistemas y redes o que pueda dañar u ofender a terceros. Las violaciones a la presente política pueden suponer una sanción disciplinaria que puede llegar hasta la desvinculación laboral.

Se podrá ejercer autoridad sin previo aviso, y la gerencia renuncia a cualquier responsabilidad relacionada con la pérdida o daño causados a la información o programas.

7.2. **POLÍTICA DE ACCESO LÓGICO.**

El objetivo de esta política es proporcionar acceso lógico seguro y adecuado, para evitar el acceso no autorizado a los Sistemas y recursos computacionales de Empresas FG. Este tipo de acceso generalmente involucra la autorización, autenticación, no-denegación, clasificación de datos y monitoreo de seguridad.

7.2.1. **Gestión de la Seguridad de la Información.**

c) La Gerencia de TI debe ser operado bajo la supervisión de la Gerencia de servicios Compartidos y debe regularse con el plan de TI y sus actividades operativas.
d) Se debe distribuir la Política TI a todo el personal de Empresas FG.

7.2.2. **Mecanismo de Autenticación.**

a) A los Usuarios Autorizados se les debe asignar cuentas individuales y contraseñas únicas para ingresar a la red, a las aplicaciones y sistemas de información de Empresas FG.
b) Para el entorno del sistema operativo o escritorio, se establece el uso de contraseñas y cierre de cuentas, según se indica a continuación:

- Las Contraseñas y Nombres de Usuarios serán únicas para cada usuario autorizado.
- Las Contraseñas estarán conformadas por un mínimo de 6 caracteres alfanuméricos (que no sean nombres comunes o frases). Para identificar la fragilidad de una contraseña, debe haber listas controladas informativamente de las reglas definidas para contraseñas y verificación periódica (Ej. secuencias de letras y números, repetición de caracteres, iniciales, palabras y nombres comunes).
- Las contraseñas serán privadas (es decir, no serán compartidas o codificadas a los programas, o escritas en papel).
- Transcurridos 90 días, el sistema obligará a un cambio de contraseña.
- Las cuentas de usuarios quedarán inhabilitadas tras cinco intentos fallidos de ingresar al sistema.
- Todos los intentos fallidos de ingresar al sistema quedarán guardados para revisión, inspección y para tomar las medidas necesarias.
- Las sesiones quedarán suspendidas tras 20 minutos de inactividad y se deberá volver a entrar con la contraseña del usuario.
- Los nombres de usuarios y las contraseñas deben quedar inhabilitados transcurrido un período determinado sin uso.
- Al desvincular o renuncia de un colaborador, sus cuentas de accesos serán cerradas.

7.2.3. **Datos directos y gestión de acceso a la Red.**

a) La Gerencia de TI, debe garantizar la implementación de políticas de TI, para acceso directo a la información, a fin de evitar el acceso no autorizado a todas las bases de datos.

b) El personal de TI designado debe guardar las configuraciones de seguridad, mediante respaldo.
c) El personal de TI designado debe realizar una revisión semestralmente para garantizar la coherencia con la política de seguridad.
d) El personal de TI designado de Empresas FG. debe revisar la actividad de registro de servidores, identificar posibles violaciones y luego aumentar o actuar sobre dichas cuestiones de manera oportuna.
e) El personal TI designado establece las restricciones específicas a cuentas y privilegios, tales como normas de contraseña única, no-utilización de nombres de usuarios genéricos, distribución limitada de contraseñas, uso de nombres de acceso para auditoría en las actividades.
f) Para redes inalámbricas, la información debe encriptarse utilizando certificado de seguridad y filtros MAC habilitados.

7.2.4.**Manejo de Virus y Licencias de Software.**

a) Se debe restringir el uso de software no autorizado.
b) Se deben implementar procedimientos adecuados para identificar el uso de software no autorizado.
c) Se deben realizar auditorías anuales para identificar y evaluar los Contratos de Licencias de Software para el software en uso.
d) El software de antivirus debe estar instalado en todas las computadoras.
e) El software de antivirus debe estar configurado para actualizar automáticamente las definiciones de virus

7.2.5.**Acceso de Usuarios y Gestión de Remuneraciones y Bienestar.**

a) Se deben crear procedimientos de administración de cuentas para agregar, cambiar o borrar cuentas de usuarios. Este procedimiento debe incluir la instalación de mecanismos de autorización.
b) Se deben implementar procedimientos formales de administración para gestionar los perfiles del grupo, los derechos y funciones de acceso, incluyendo procesos de autorización.
c) El reclutamiento de personal de TI debe estar en concordancia con la política PLT-006-Selección y contratación de Personal.
d) Las funciones de los usuarios se deben definir en función del nivel de acceso que necesita el empleado para ejecutar sus obligaciones efectivamente. Como pauta para determinar este acceso, se deben utilizar los principios de Separación de Tareas y de Menor Privilegio (sobre la base de la necesidad, únicamente).
e) Se deben evaluar las responsabilidades laborales de los colaboradores, según la descripción de cargo.
f) El acceso de los colaboradores a todos los sistemas e instalaciones debe ser rescindido inmediatamente tras la renuncia / rescisión, y se seguirá el procedimiento definido por las gerencias a cargo.
g) Cuando el empleado renuncie o cuando se rescinda su contrato, el gerente a cargo deberá notificar inmediatamente al Departamento de TI.

h) La Gerencia de TI es responsable de garantizar que todos los colaboradores de Empresas FG y usuarios invitados devuelvan los equipos al finalizar el contrato o al rescindirse los servicios, y se retirarán en ambos casos sus derechos de acceso a los sistemas y servicios informáticos.
i) El área de Remuneraciones y Bienestar debe notificar a la Gerencia de TI en forma oportuna las altas y bajas de colaboradores de Empresas FG.
j) Como parte de su obligación contractual, todos los empleados y usuarios invitados deben aceptar y firmar las cláusulas y condiciones de empleo (o) compromiso con la Empresa y este documento proporcionado por Remuneraciones y Bienestar debe indicar su responsabilidad de cumplimiento de los procedimientos de la presente Política de Informática.

7.2.6. **Segregación de Tareas y revisión de perfil.**

a) La Gerencia de TI emitirá una auditoria periódica de perfiles de usuarios cada 6 meses, para realizar análisis de separación de las tareas.
b) La Gerencia de TI emitirá una auditoria de las listas de distribución de cuentas de usuarios cada 6 meses y los derechos de acceso a la gerencia, o acceso a propietarios de proceso para confirmación, para realizar análisis y actualización de miembros de usuarios.
c) Asimismo, se deben definir periódicamente los perfiles y funciones del grupo, para garantizar que la distribución de tareas continúa siendo adecuada para los cargos disponibles dentro de la organización.
d) Los dueños de procesos deben crear procedimientos por medio de los cuales la gerencia a cargo validará la asignación de funciones y perfiles de los usuarios.
e) Cada seis meses, la Gerencia de TI, realizará una evaluación de los usuarios con respecto a sus funciones o perfiles, para identificar funciones incompatibles – relacionadas con la función en sí misma, o por haber sido designado a una función o perfil de grupo.

7.3. POLÍTICA DE ACCESO FÍSICO

El objetivo de esta política es proporcionar instalaciones adecuadas y seguras para albergar y proteger los Equipos de comunicación, servidores, sistemas de respaldo y otros Activos informáticos de la empresa y a la vez proporcionar un ambiente de trabajo productivo, en el que se minimicen los riesgos de alteración de la actividad empresarial producidos por el hombre o desastres naturales.

7.3.1. Las instalaciones para el procesamiento de la información de la empresa deben estar albergadas en áreas seguras, protegidas por un perímetro de seguridad definido mediante barreras de seguridad adecuadas, y controles de ingreso. Deben estar protegidas físicamente del ingreso no autorizado, daños e interferencia.

7.3.2. Todos los servidores, componentes de la red como enrutadores (*routers*), hubs, etc. u otros dispositivos para usuarios múltiples (que no sean impresoras, máquinas de fax, etc.) deben estar almacenados en salas informáticas seguras, o en gabinetes cableados con las condiciones climáticas requeridas.

7.3.3. El acceso a la sala de servidores debe estar justificado, autorizado, registrado y monitoreado. Esto se aplica a todas las personas que ingresen a las instalaciones, incluyendo empleados de Empresas FG, proveedores, clientes, vendedores, visitantes o cualquier otra parte.

7.3.4. Si el personal designado de TI o cualquier empleado con acceso autorizado irrestricto a la sala del servidor renuncia, o si se rescinde su contrato de trabajo, se debe eliminar inmediatamente el acceso a la sala de servidores.

7.3.5. Se deben cambiar las contraseñas en el momento de la renuncia (o rescisión del contrato de trabajo) del Gerente de TI, o empleado con acceso irrestricto. Los procedimientos de cambio de contraseña están definidos en la Política de Seguridad de Acceso Lógico.

7.3.6. El acceso a la sala del servidor está restringido sólo al personal autorizado.

7.3.7. El Gerente de TI, o personal designado de Empresas FG. deben definir las instalaciones de almacenamiento locales y externas.

7.3.8. En la lista de equipos y dispositivos especializados se deben incluir aire acondicionado, extintores de fuego adecuados, detectores de humo, alarmas para incendios, suelo elevado antiestático.

7.3.9. Todos los equipos de TI deben estar protegidos contra desperfectos eléctricos, mediante el uso de medidas de protección adecuadas, tales como el Estabilizador de Energía (UPS, por su sigla en inglés), respaldo de batería, o generadores eléctricos. Dichos equipos deben estar ubicados en una habitación adecuada, separada de la sala del servidor / de informática, con acceso físico adecuado y controles de temperatura.

7.3.10. El cableado de energía y comunicaciones que transporte datos o que sustente los servicios informáticos debe estar protegido de intercepción o daños.

7.3.11. Toda la gestión de la instalación, incluyendo equipos de energía y comunicaciones, debe cumplir con la legislación y normativa vigente, los requerimientos técnicos y empresariales, las recomendaciones del fabricante y las pautas de salud y seguridad.

7.3.12. Se deben mantener todos los equipos de TI y utilidades de apoyo de acuerdo con la frecuencia y especificaciones de servicio recomendadas por el proveedor correspondiente.

7.3.13. Las reparaciones y servicios sólo las puede realizar personal de mantenimiento autorizado y todas las actividades de mantenimiento deben quedar registradas.

7.4. **POLÍTICA DE COMUNICACIÓN INALÁMBRICA.**

El objetivo de esta policita es prohibir el acceso a las redes inalámbricas de Empresas FG a través de mecanismos de comunicación no seguro. Sólo los sistemas de autentificación y accesos definidos que cumplan los criterios de esta política están aprobados para la conectividad.

7.4.1. Esta política considera todos los dispositivos de comunicación inalámbricos (sean estas computadoras portátiles, teléfonos celulares, PDAs, etc.), conectados a cualquiera de las redes inalámbricas de Empresas FG. Esto incluye cualquier forma de comunicación inalámbrica de dispositivos capaces de transmitir paquetes de datos. Dispositivos inalámbricos y o redes sin ningún tipo de conectividad a redes de Empresas FG no entran en el ámbito de esta política.

7.4.2. Registro e Inventario. Todos los puntos de accesos inalámbricos, tarjetas de redes inalámbricas de computadores y dispositivos de bolsillos deben registrarse en un formato definido para su aprobación y control.

7.4.3. Las señales inalámbricas conocidas como SSID no deben configurarse con la información de la compañía, nombre de usuarios o áreas de trabajo.

7.4.4. El tráfico generado entre los puntos de accesos y las tarjetas inalámbricas de las computadoras autorizadas y conectadas deben estar encriptada.

7.4.5. Los puntos de accesos inalámbricos deben configurarse para filtrar números de registros MAC.

7.4.6. Los puntos de accesos inalámbricos deben de someterse semestralmente a pruebas de accesos y control.

7.5. **POLÍTICA DE SEGURIDAD**

El objetivo de esta política es mantener la disponibilidad y seguridad de todos los entornos operativos e infraestructura asociada con controles de revisión periódica para minimizar riesgos de operación y alteraciones que puedan impactar el buen funcionamiento de sistemas y servicios críticos de Empresas FG. Se establecen los siguientes controles TI:

7.5.1. **Revisión de Logs.** Las aplicaciones críticas y servicios de redes deberán mantener registros de eventos de errores y/o alertas que requieran atención. Semanalmente, personal designado de la Gerencia TI deberá revisar estos eventos y mitigar preventivamente cualquier incidencia que pueda afectar la disponibilidad.

7.5.2. **Copias de Seguridad y recuperación**. El Gerente TI debe mantener respaldos de bases de datos de las aplicaciones críticas, a través tareas automatizadas en horarios no laborales. Frecuentemente se deben realizar actividades de revisión de integridad de los respaldos.

7.5.3. **Respaldo de las Configuraciones.** Todas las configuraciones de recursos computacionales destinados a mantener conectividad y seguridad de las redes deben mantenerse respaldados ante posibles cambios de hardware por degradación o fallas.

7.5.4. **Monitor de Salud.** Las aplicaciones criticas deben mantener un monitor de telemetría para brindar una capacidad de observación completa para analizar, solucionar problemas y optimizar las aplicaciones en sus entornos de software y hardware.

7.5.5. **Control de Datos en puntos de Integración de Sistemas.** Las conectividad e integración de las aplicaciones criticas con servicios empresariales y auxiliares deben mantenerse con herramientas que permitan trazabilidad y control de errores en el flujo de datos.

7.5.6. **POLÍTICA DE CLASIFICACIÓN DE DATOS.**

El objetivo de esta policita es definir una correcta clasificación de los datos, basado en la sensibilidad y criticidad de la información que es generada por cada proceso de negocio de Empresas FG. De esta manera se puede asegurar un apropiado nivel de protección en el acceso y distribución de la información.

7.5.7. Todos los datos de Empresas FG y los datos que se han confiado a los colaboradores, se categorizan en los tres siguientes grupos:

7.5.7.1. **Confidencial**: El acceso a esta información se limita única y exclusivamente a la necesidad de conocerla. La divulgación de datos requiere la aprobación del propietario y, en el caso de terceros, la firma de un acuerdo de confidencialidad en conjunto con el contrato de prestación de servicios. El tipo de información incluye los datos financieros, información de recursos humanos y exploración de datos.

7.5.7.2. **Para Uso Interno:** Esta información sólo será divulgada a terceros en caso de que se haya firmado un acuerdo de confidencialidad. La

divulgación no espera causar daños graves a Empresas FG, y se ofrece acceso libre a todos los miembros de la empresa. Los datos incluyen listados de teléfono de colaboradores, listas de direcciones, marco normativo vigente, diagramas de red, etc.

7.5.7.3. **Público:** Esta información es adecuada para la difusión pública. Los ejemplos incluyen, naturalmente anuncios, comunicados de prensa, folletos de marketing, etc.

Si los datos no han sido clasificados, la clasificación por defecto es "Para Uso interno."

7.5.8. Empresas FG mantendrá resguardo de las bases de datos definidas para los sistemas de información y sitios. Todos los datos deben ser mantenidos y protegidos de conformidad con la norma de clasificación de datos.

7.5.9. Los propietarios de datos son los altos directivos de Empresas FG (o sus representantes) que tienen la planificación y la política a nivel de responsabilidad para los datos dentro de sus áreas funcionales y las responsabilidades de gestión para determinados segmentos de datos institucionales. Las responsabilidades incluyen la asignación de acceso de datos, promocionar políticas gestionar los recursos de datos.

7.5.10. Cada departamento o área podrá adoptar políticas que definan nuevas clasificaciones con más restricciones que las señaladas en la presente política.

7.5.11. Los propietarios de los datos son responsables de garantizar que la información se encuentra bajo su control y se adhiere a esta política y la norma de clasificación de datos..

7.5.12. La Gerencia de TI es responsable de mantener la política y garantizar la existencia de infraestructuras de apoyo a esta política.

7.5.13. Todos los colaboradores de Empresas FG que tienen acceso a datos o información confidencial son responsables de velar por que no sea divulgada a personas no autorizadas y que se elimine correctamente cuando ya no sea necesario.

7.5.14. La Empresa se reserva el derecho de modificar o poner fin a modificar esta política en cualquier momento.

7.6. **Política de Gestión de Cambios en TI.**

El objetivo de la presente política es definir el proceso de gestión y control de todos los cambios, incluyendo el mantenimiento de emergencia y los parches para software, relacionados con los Sistemas Informáticos dentro del ambiente de producción de Empresas FG.

7.6.1. La Política de Gestión de Cambio en TI se aplica, entre otras, a las siguientes áreas de Informática.

a) Hardware y software del Sistema.
b) Equipos y software de comunicación.
c) Sistema de Información ERP.
d) Cambios empresariales (reorganización, traslado, reducción de personal, etc.).
e) Documentación y procedimientos de los sistemas de información.
f) Software de aplicación en uso, incluyendo software instalado en máquinas operativas.
g) Reparación de problemas (reparaciones aplicadas como respuesta a solicitudes de cambio / problemas) que producen cambios en los sistemas de aplicación o en la infraestructura

7.6.2. La Política de Gestión de Cambios y los Procedimientos debe ser comunicada a los colaboradores y usuarios invitados de Empresas FG.

7.6.3. Todas las solicitudes de cambio deben ser registradas formalmente en formularios de solicitud de cambio.

7.6.4. Todas las solicitudes de cambio deben ser presentada por el Gerente de División al Director Ejecutivo, para su aprobación.

7.6.5. La Gerencia de TI debe garantizar que los requerimientos de control de los sistemas y de la empresa se vean respetados antes de autorizar todas las solicitudes de cambio.

7.6.6. Para cada solicitud de cambio, el Gerente de División debe evaluar el impacto que se hará en la productividad de los usuarios y los costos económicos de manera estructurada y se lo debe documentar en formato adecuado.

7.6.7. Sobre la base del impacto en la actividad empresarial normal y la urgencia por introducir los cambios, todas las solicitudes serán categorizadas y se les asignará un orden de prioridad.

7.6.8. Los cambios a las Estructuras de Datos deben realizarse de acuerdo con las especificaciones y se los debe implementar de manera oportuna.

7.6.9. Se debe conservar un Registro electrónico de Gestión de Cambios para todas las solicitudes de cambio, y se incluirán los siguientes ítems:

a) Formulario de solicitud de cambio en que se indique la fecha de cambio.
b) Historial de revisión del cambio.
c) Nombre del Director Ejecutivo que aprueba el cambio.
d) Nombre de Gerente de División que solicita el cambio.
e) Descripción del cambio.
f) Resultado del cambio – sea exitoso o no.
g) Lista de sistemas, recursos, usuarios, etc. actualizados.
h) Descripción de flujos y controles de proceso actualizados.

i) Detalles de documentos actualizados.
j) Flujo de aprobación o rechazo.

7.6.10. Actualización de documentación de los sistemas de información, entregada a proveedores, debe ser preservada para el seguimiento del cambio y para futuras consecuencias de los cambios.
7.6.11. La Gerencia de TI es facilitador de Ambientes de Pruebas para todas las aplicaciones fundamentales.
7.6.12. Se debe presentar un proceso de estabilización, posterior a la implementación y cambios de los sistemas para garantizar una puesta en operación satisfactoria.
7.6.13. La documentación y procedimientos del sistema se deben actualizar en consecuencia.
7.6.14. El modo de prueba del Sistema y el modo para producción en vivo deben estar separados unos de otros.
7.6.15. Un implementador de sistemas o programas no debe tener acceso a la información de producción en vivo.
7.6.16. Cuando sea posible, se debe implementar una segregación o separación de obligaciones entre el personal de desarrollo y el personal responsable de mover un programa al modo de producción.
7.6.16.1.1.1. Se debe asignar responsabilidades tanto para la infraestructura técnica como para la aplicación relacionada con los cambios.
7.6.16.1.1.2. Sólo el perfil del administrador deben tener acceso completo a las carpetas donde se graban las aplicaciones.
7.6.16.1.1.3. Las actividades del administrador deben ser registradas y monitoreadas.
7.6.16.1.1.4. Los cambios introducidos en los archivos/directorios de producción deben ser registrados por el módulo de rastreo de auditoría para las aplicaciones financieras.
7.6.16.1.1.5. Todos los cambios de configuración de cualquier aplicación fundamental deben ser registrado por las características de registro de auditoría de la aplicación.
7.6.16.1.1.6. En lo posible, se deben utilizar herramientas de monitoreo de cambios para detectar cambios en el modo de producción en vivo.
7.6.17. **Actualizaciones, Parches y Reparaciones.**
7.6.17.1.1.1. Todas las actualizaciones introducidas a sistemas operativos (Entornos Windows, MacOS, Server) deben responder a procedimientos de actualización aprobados y deben ser suministrados por los fabricantes correspondientes. Si no se encuentran disponibles estos procedimientos, la Gerencia de TI debe documentar e inspeccionar el proceso de actualización.
7.6.17.1.1.2. El Gerente de TI debe aprobar el proceso de actualización antes de la implementación de la actualización.
7.6.17.1.1.3. En el caso de todas las aplicaciones fundamentales, el personal calificado (usuarios del proceso que depende de las gerencias de división y personal designado de TI debe ser facilitador) debe verificar adecuadamente las actualizaciones

y parches para software en el modo prueba antes de ser aplicados al modo en producción.

7.6.17.1.1.4. Los cambios se harán a más tardar el día jueves de cada semana.

7.6.17.1.1.5. Las grandes actualizaciones que requieran que el sistema operativo esté inactivo durante un lapso considerable deben ser programadas con antelación y deben ser aprobadas por el Gerente de TI y el Gerente de Servicios Compartidos.

7.6.17.1.1.6. Se deberá notificar sobre actualizaciones programadas a los usuarios afectados por la inactividad del sistema.

7.6.18. **Cambios de Emergencia.**

La implementación de cambios debe ser una actividad bajo moderamiento y controlada. No obstante, en casos de emergencia, en donde se interrumpe el normal funcionamiento de la actividad empresarial, puede ser necesaria la implementación inmediata de cambios en el sistema. Estos casos reciben el nombre de Cambios de Emergencia. Los Cambios de Emergencia deben ser manejados por personal capacitado a cargo de los sistemas, y entre los requerimientos para manejar estos cambios se incluyen:

a) Criterios para definir la(s) situación(es) en las cuales implementar un cambio de emergencia.
b) Documentación sobre los detalles del cambio de emergencia.
c) Los cambios de fácil aplicación y que no superen las 48 horas de ejecución y sin inversión, requieren de la aprobación del Gerente de la División y del Gerente de TI correspondientes, para ocuparse de cambios de emergencia.
d) Los cambios de emergencias que requieran una reestructuración en alto porcentaje en la funcionalidad del sistema actual, una gran inversión adicional y un periodo de tiempo prolongado requieren de la aprobación del Director Ejecutivo.

7.6.19. Siempre que sea posible, se deben realizar pruebas mínimas.

7.6.20. Se debe realizar un monitoreo posterior al cambio para garantizar que el problema fue totalmente resuelto y que no se registran otras casuísticas.

8. POLÍTICA DE PROPIEDAD Y RESPONSABILIDAD.

8.1. **Funciones y Responsabilidades de TI.**

8.2. Las funciones y responsabilidades de los colaboradores se han segregado por divisiones de acuerdo con el área de conocimiento correspondiente:

8.2.1. **Gerencia de TI.** Es responsable de la Gestión y dueño de los procesos y servicios relacionados con la tecnología de información. Manteniendo en control la disponibilidad y seguridad de todos los recursos Computacionales e Informáticos de Empresas FG.

8.2.2. **Administrador de Sistemas.** El administrador de sistemas es el responsable de la gestión y el apoyo a los sistemas de Información de Empresas FG, incluyendo las bases de datos y multi instancia en las diferentes configuraciones de cada módulo y sistemas asociados.

8.2.3. **Administrador de Red.** es el responsable de supervisión y mantenimiento de la infraestructura de red Local (LAN). Además, esta posición es responsable de procesos relacionados con planes de contingencia, respaldos de configuraciones, incluyendo, pero no limitados a supervisión y monitoreo de sistemas antivirus, actualización de parches críticos y de seguridad.

8.2.4. **Soporte Computacional.** El técnico de soporte computacional es responsable de entregar solución a problemas de hardware y software reportados por usuarios de Empresa FG, asistirlos en forma remota o en terreno, considerando los tiempos de respuestas adecuados en relación con el tipo de problema.

8.3. Anualmente, se realizan evaluaciones del personal para garantizar la Gerencia de TI tenga el número suficiente de colaboradores competentes, necesarios para alcanzar los objetivos, de acuerdo con las políticas.

9. POLITICA DE CUMPLIMIENTO Y VERIFICACIÓN.

9.1. La Gerencia de TI deberá realizar revisiones anuales, actualizaciones y difusión de los cambios de las políticas.

9.2. Todo incumplimiento de estas políticas debe ser reportado al Gerencia de TI de Empresas FG.

9.3. La violación de estas políticas puede resultar en la suspensión de cuentas de accesos y los privilegios asignados en los recursos de la red y/o recibirá una sanción.

9.4. Empresas FG Solicitará la asistencia de organismos encargados de hacer cumplir la ley cuando un delito se ha cometido.

9.5. La Gerencia de TI asegurará planes de contingencia ante cualquier falla o incidente que se produzca en relación con estas Políticas.