CONTROL DE ACCESOS

TIPO DE DOCUMENTO: Procedimiento

CÓDIGO: PRO GSI 016

I. AUTORIZACIONES

Elaboró:	*Revisó:*	*Autorizó:*
Ing. Salvador Santiago Araujo *Gerente Administrativo*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*

Última revisión: octubre 2025

No. de versión: 11

Fecha de emisión: Agosto 2015

Revisó: DGE

Aprobó: DGE

INDICE

CONTENIDO **PÁGINA**

II. OBJETIVO

Establecer los lineamientos y controles necesarios para garantizar que todos los **usuarios internos, externos y terceros autorizados** obtengan únicamente los **permisos adecuados y necesarios** para acceder a los sistemas, aplicaciones, infraestructuras tecnológicas y servicios de información de la organización, asegurando el cumplimiento del **principio de privilegio mínimo** y la protección de la **confidencialidad, integridad y disponibilidad de la información**.

Este procedimiento tiene como finalidad evitar que la seguridad de la información se vea comprometida por accesos indebidos, credenciales mal gestionadas o configuraciones inadecuadas. Para ello, se definen los **mecanismos de autenticación, control de accesos lógicos y físicos, procesos de altas, bajas y modificaciones de cuentas, recertificación periódica de privilegios, y gestión de accesos privilegiados**.

III. ALCANCE

Este procedimiento aplica a **todas las áreas, procesos, colaboradores internos, externos, proveedores, contratistas y terceros autorizados** que requieran acceso a los **sistemas de información, aplicaciones corporativas, infraestructura tecnológica, redes, activos físicos y servicios administrados por la organización**, en el marco del **Sistema de Gestión de Seguridad de la Información (SGSI)**.

IV. HISTORIAL DE CAMBIOS

Versión	Descripción de cambios	Autor(es)	Fecha de cambio
1	Versión inicial.	MBS	Agosto 2015
2	Adecuación en diversos puntos respecto al manejo de usuarios y contraseñas.	MBS	Noviembre 2015
3	Cambio de Formato	LBR	Octubre 2016
4	Adecuaciones generales a los puntos 1.1, 2.1,	LBR	Mayo 2017

5	Actualización de formatos	RML	Enero 2018
6	Actualización de referencias, modificación a metodología de acceso a la red y a los servicios de red, registros de usuarios, incapacidades y vacaciones	RML	Mayo 2019
7	Adecuaciones generales a los puntos 2.5, 3.1, 4.1 y 5.1.	RFML	Octubre 2020
8	Actualización del punto 3 Baja de usuarios y/o cambio de puestos (3.4 y 3.5); se agregó el punto 7 Usuarios Privilegiados.	RFML	Julio 2021
9	Se agregó la nota en el punto 2.5, donde la empresa debe notificar al cliente BBVA sobre cualquier ABC de usuarios, así como la declaración de la FOR GSI 036.	RFML	Abril 2022
10	Se adecua la sección 7. Usuarios privilegiados y se cambia el nombre del Coordinador de Sistemas TI por Coordinador de Sistemas TI.	CST	Septiembre 2023
11	Actualización del procedimiento de control de accesos para reforzar procesos de altas, bajas, modificaciones y recertificación de privilegios, alineados al principio de privilegio mínimo y a los requisitos de la norma ISO/IEC 27001:2022.	SSA	Septiembre 2025

V. REFERENCIAS

- MAN GSI 001 Manual de gestión de seguridad de la información
- POL GSI 001 Políticas generales de seguridad de la información
- FOR GSI 025 Matriz de roles por activos de información críticos
- FOR GSI 031 Carta responsiva
- FOR GSI 032 Autorización de accesos
- FOR SIS 009 Excepciones por puesto
- LIS GSI 004 Catálogo de software y aplicaciones permitidos en CIA
- LIS GSI 008 Lista de usuarios
- LIS GSI 023 Inventario y clasificación de activos

VI. ABREVIACIONES Y DEFINICIONES

Abreviaciones:

DGE	Director General / Director General Adjunto
CSG	Coordinador de Sistemas de Gestión
CST	Coordinador de Sistemas TI
ESI	Encargado de Sistemas
N/A	No Aplica
SGC	Sistema de Gestión de Calidad
SGSI	Sistema de Gestión de Seguridad de la Información

Definiciones:

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

VII. DESARROLLO DE ACTIVIDADES

No.	Descripción	Responsable(s)
1	**Acceso a la red y a los servicios de red**	
1.1	**Control general** El acceso a la red corporativa constituye un punto crítico de seguridad, ya que a través de ella los usuarios se comunican con los servidores de la organización, bases de datos y aplicativos estratégicos. Por ello, la organización aplica **controles físicos, lógicos y administrativos estrictos**, de manera que únicamente equipos inventariados y usuarios autorizados puedan conectarse y obtener acceso a los recursos internos. Estos controles se basan en la autenticación centralizada en Active Directory, la segmentación de tráfico por VLAN y la obligatoriedad de establecer túneles cifrados en Printunl, lo que asegura que todos los accesos estén plenamente identificados, registrados y bajo trazabilidad. • En **LAN y WLAN**, el ingreso está protegido por el **portal cautivo de Fortinet**, que solicita credenciales personales y, tras su validación, asigna automáticamente la **VLAN específica del rol del usuario** (ejemplo: Dirección General, Recursos Humanos, Contabilidad, Sistemas, etc.). Esto impide que un equipo conectado físicamente a la red o vía inalámbrica tenga acceso sin autenticación previa. • Para acceder a **servidores, aplicaciones o bases de datos**, no basta con superar el portal cautivo: es **obligatorio establecer la VPN Printunl**, que cifra todo el tráfico y valida tanto las credenciales AD como el **certificado SSL corporativo instalado en el endpoint**, asegurando que solo equipos autorizados y con postura de seguridad mínima puedan interactuar con la infraestructura. • En el caso de **acceso remoto (teletrabajo)**, el portal cautivo no interviene. El control recae completamente en la **VPN Printunl**, que exige autenticación en Active Directory, certificado SSL vigente y verificación de seguridad en el equipo (BitLocker activo y SentinelOne en operación).	Gerente Administrativo Coordinador TI Auxiliar TI Colaboradores en GRAL
1.2	**Acceso alámbrico (LAN)**	Gerente Administrativo Coordinador TI Auxiliar TI Colaboradores en GRAL

	El acceso mediante red alámbrica constituye uno de los puntos más sensibles de la infraestructura, ya que los nodos físicos podrían ser utilizados como vectores de intrusión si no existieran controles adicionales. Para prevenir este riesgo, cada puerto de red se encuentra mapeado, enrutado y registrado en GLPI, con detalle de su ubicación física, equipo asociado y usuario responsable. Esto asegura trazabilidad total y permite que cualquier cambio o movimiento quede documentado en la plataforma de inventario y en tickets de CIA - Desk. • Aunque un dispositivo se conecte físicamente a un puerto activo, no obtiene acceso inmediato a la red interna. El usuario debe primero autenticarse en el portal cautivo de Fortinet, el cual valida sus credenciales de Active Directory y asigna la VLAN correspondiente a su rol. Esto evita accesos anónimos y garantiza que cada conexión esté segmentada conforme al perfil del usuario. • Una vez validado en Fortinet, el acceso a servidores, aplicaciones y bases de datos requiere obligatoriamente establecer un túnel seguro en la VPN Printunl. Este cliente valida no solo las credenciales de AD, sino también el certificado SSL corporativo instalado en el endpoint. Adicionalmente, la postura mínima de seguridad exige que el dispositivo tenga habilitado BitLocker y SentinelOne en operación para que se permita el tráfico hacia la red interna. • Solo tras completar estas validaciones se habilita la comunicación con servidores críticos, aplicativos corporativos y bases de datos. Este modelo garantiza que incluso en conexiones físicas dentro de las oficinas, el acceso se otorgue únicamente a dispositivos registrados y bajo estándares de seguridad definidos por el SGSI. De esta manera, el acceso LAN queda protegido bajo un esquema de doble autenticación (Fortinet + Printunl), con segmentación en VLAN y validación de dispositivos, evitando que la conexión física represente una vulnerabilidad en la red corporativa.	
1.3	**Acceso inalámbrico (Wi-Fi corporativa)** El acceso inalámbrico representa un punto sensible de la infraestructura, ya que puede ser utilizado como vía de intrusión si no se controla adecuadamente. Por esta razón, la organización implementa un esquema de seguridad que exige **autenticación múltiple, segmentación en VLAN y cifrado de tráfico** para cada conexión Wi-Fi. Los **Access Points Huawei** están configurados con **SSID diferenciados por área**, lo que permite que cada rol tenga una red exclusiva con políticas específicas, garantizando el cumplimiento del **principio de privilegio mínimo** también en las redes inalámbricas. • **Flujo de conexión inalámbrica:** 1. El dispositivo se conecta al **SSID correspondiente** mediante una contraseña compleja y periódicamente renovada. 2. El usuario es redirigido al **portal cautivo de Fortinet**, donde debe autenticarse con sus credenciales de Active Directory; una vez validadas, Fortinet asigna la **VLAN asociada** a ese SSID.	Gerente Administrativo Coordinador TI Auxiliar TI Colaboradores en GRAL

	3. Para habilitar comunicación con servidores y aplicaciones internas, el usuario debe además iniciar sesión en el **cliente VPN Printunl**, que valida el **certificado SSL del endpoint** y las credenciales de AD. 4. Solo tras superar ambos filtros, la conexión inalámbrica permite el acceso a aplicaciones críticas y bases de datos. • **SSID por sede:** ○ **Nezahualcóyotl:** DIRCOR (Dirección General), REHCOR (Recursos Humanos), CONCOR (Contabilidad), SISCOR (Sistemas), GESCOR (Gestión Domiciliaria), INVCOR (Investigación de Crédito), INVITADOS (proveedores/clientes/autoridades con acceso aislado a internet). ○ **Insurgentes:** DIRCOR (Dirección General), COSVAL (Cobranza Social), CREVAL (Jurídico), SISCOR (Sistemas), REHCOR (Recursos Humanos), INVITADOS (acceso aislado a internet para externos autorizados). ○ **Toluca:** DIRCOR (Dirección General), RECCALS (Supervisores de Call Center), RECCALC (Gerencia de Recuperación de Cartera), SISCOR (Sistemas), REHCOR (Recursos Humanos), INVITADOS (acceso aislado a internet para externos autorizados). • **Reglas de seguridad de Wi-Fi corporativa:** ○ Cada **SSID está vinculado a una VLAN exclusiva**, con políticas de firewall definidas que impiden tráfico lateral entre áreas. ○ La red de **invitados (CIASC-INVITADOS)** está **totalmente segregada**: únicamente ofrece salida a internet y no tiene rutas hacia servidores, VLAN internas ni aplicaciones corporativas. ○ Las contraseñas de acceso a cada SSID son generadas con **complejidad alta**, se distribuyen de forma controlada y se actualizan periódicamente por el área de Sistemas. ○ Incluso después de autenticarse en Fortinet, **todo tráfico hacia recursos críticos debe pasar obligatoriamente por la VPN Printunl**, lo que asegura que solo dispositivos corporativos inventariados en **GLPI** y con controles activos (BitLocker, SentinelOne, certificado SSL) puedan interactuar con la infraestructura. Con este esquema, la organización garantiza que el acceso inalámbrico esté sujeto a las mismas medidas de control que el acceso LAN, eliminando riesgos de intrusión y manteniendo visibilidad total sobre cada conexión registrada.	
1.4	**Acceso remoto (teletrabajo)** El teletrabajo representa un punto de riesgo elevado para la organización, ya que implica el acceso a la infraestructura desde ubicaciones externas y redes que no están bajo control corporativo. Para mitigar este riesgo, la organización establece que únicamente el	Dirección General Gerente Administrativo Gerente de Investigación de Crédito Coordinador TI Auxiliar TI

	personal previamente autorizado podrá conectarse de manera remota, y siempre bajo un esquema de **VPN corporativa con controles reforzados de autenticación y postura de seguridad en el endpoint**.
	
	• El acceso remoto se realiza **exclusivamente mediante el cliente VPN Printunl**, el cual está configurado con perfiles de conexión definidos por el área de Sistemas y vinculados a roles específicos en la organización.
	• Antes de establecer la conexión, el cliente valida:
	  ○ Las **credenciales de Active Directory** del usuario.
	  ○ El **certificado SSL corporativo** instalado en el equipo.
	  ○ La **postura mínima de seguridad** del endpoint: cifrado de disco activo con **BitLocker**, protección antimalware **SentinelOne** en ejecución y actualización, y registro del dispositivo en **GLPI** como equipo corporativo autorizado.
	• A diferencia del acceso LAN o WLAN, en el teletrabajo no interviene el portal cautivo de Fortinet. El control de acceso y la **segmentación de VLAN** se aplican de manera automática por Printunl, según el perfil asignado en el servidor.
	• Cada conexión queda registrada en los logs de Printunl. Estos registros son revisados cada 15 días por el coordinador TI y los resultados se registran en el formato **LIS GSI 002 – Revisión de LOGS** y cualquier anomalía se documenta en **CIA - Desk** como incidente de seguridad.
	
	Con este esquema, CIASC asegura que el acceso remoto tenga los mismos niveles de control y visibilidad que el acceso local, garantizando que solo dispositivos corporativos autorizados y bajo controles de seguridad activos puedan interactuar con los recursos internos.	

1.5	**Acceso a bases de datos y aplicaciones críticas** El acceso a bases de datos y aplicaciones críticas constituye un punto de riesgo elevado, ya que en ellas se concentra la información sensible de la organización y de sus clientes. Por este motivo, la organización establece que todo acceso debe realizarse únicamente desde **PCs y laptops inventariadas en GLPI** y asignadas formalmente a un usuario mediante la **Carta Responsiva FOR GSI 031**. El uso de software para interactuar con estas bases está limitado estrictamente a lo establecido en el **LIS GSI 004 – Catálogo de software autorizado**, prohibiéndose el uso de gestores o aplicaciones no aprobadas. • **Bases de datos críticas identificadas:** ERP CIASC, Aspel, SICOB, FileMaker, GLPI, CIA - Desk e Intranet de Sistemas de Gestión. Estas plataformas constituyen el núcleo de los procesos administrativos, operativos y de soporte de la organización. • **Acceso directo a bases:** está restringido exclusivamente al **personal de Desarrollo y de Sistemas**, quienes tienen la responsabilidad de administrar, configurar y crear accesos. Estos accesos son registrados en GLPI y toda acción queda documentada en tickets de CIA - Desk para garantizar trazabilidad.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL

	• **Usuarios finales:** únicamente pueden interactuar con los **entornos de trabajo y actividades** habilitados en cada aplicación (formularios, consultas, reportes o asignación de tareas), sin privilegios para acceder o manipular directamente la base de datos. Esto asegura que la información solo sea gestionada a nivel de aplicación y nunca a nivel de motor de datos. • **ERP CIASC:** en particular, los **equipos celulares corporativos de asesores de campo** y los **equipos de cómputo del personal operativo** en oficinas corporativas tienen un acceso limitado que les permite exclusivamente la **captura de formularios y la ejecución de tareas operativas**. Dicho acceso restringido **no otorga en ningún caso privilegios sobre la base de datos central**, la cual permanece bajo control de Desarrollo, Gerencia Administrativa y Dirección General. • **Restricciones y excepciones:** queda prohibido copiar, exportar o respaldar información contenida en las bases de datos a medios locales, dispositivos externos o carpetas personales. Cualquier excepción debe contar con autorización formal de la **Dirección General o la Gerencia Administrativa** y debe estar documentada en **CIA - Desk**, dejando evidencia de la aprobación y del responsable que autorizó la operación. Con este control, CIASC asegura que el acceso a bases de datos críticas se limite únicamente a los roles autorizados, bajo condiciones seguras, y que todo acceso, modificación o excepción quede documentado en los sistemas de gestión, manteniendo la **confidencialidad, integridad y disponibilidad de la información** conforme a los principios del SGSI.	
1.6	**Restricción por ventana operativa** En los accesos LAN y WLAN, la conexión a la red está protegida no solo por autenticación de usuario, sino también por políticas de control de horario configuradas en Fortinet. Mediante estas reglas se bloquea el tráfico en todas las VLAN corporativas fuera de las horas de operación definidas para cada sede: • En la oficina **Toluca**, de lunes a domingo, el tráfico de todas las VLAN se encuentra bloqueado antes de las 06:30 horas y después de las 20:30 horas, quedando operativa únicamente durante la jornada establecida. • En las oficinas de **Nezahualcóyotl e Insurgentes**, de lunes a sábado, el tráfico se bloquea antes de las 08:30 horas y después de las 20:30 horas, asegurando que la red solo se utilice en horario laboral. • La VLAN de **invitados** (CIASC-INVITADOS) se encuentra aún más restringida, habilitada únicamente de 09:30 a 18:30 horas de lunes a viernes, quedando completamente inactiva fuera de ese rango. Estas configuraciones impiden que existan conexiones válidas en horarios no autorizados, reducen la superficie de ataque en periodos de inactividad y fortalecen la protección contra accesos indebidos, alineándose al principio de defensa en profundidad del SGSI.	

2	**Registro de usuarios**	
2.1	**Administración de usuarios y contraseñas** La creación, modificación y baja de usuarios en los sistemas, aplicaciones y servicios de la organización se gestiona exclusivamente por el área de Sistemas. Los accesos se otorgan de acuerdo con la función del puesto y aplicando el **principio de privilegio mínimo**, es decir, asignando únicamente los permisos necesarios para el desempeño de sus responsabilidades.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL
2.2	**Notificaciones de Recursos Humanos** De acuerdo con el mapa de proceso de **Recursos Humanos MAP REH 001**, es responsable de notificar al área de Sistemas, a través de **CIA - Desk y/o correo institucional**, los eventos que requieran la creación o modificación de cuentas de usuario. Entre estos eventos se incluyen: • Ingreso o reingreso de personal (con datos: número de empleado, nombre completo, puesto y sucursal). • Cambio de puesto o funciones del colaborador, lo que implica la revisión y ajuste de accesos otorgados.	Gerente Administrativo Coordinador TI Desarrollador Gerente de RH Reclutador de RH Auxiliar TI Colaboradores en GRAL
2.3	**Solicitudes de accesos** **Colaboradores** Las solicitudes de accesos para colaboradores internos deben ser gestionadas por el área de Recursos Humanos en coordinación con el responsable directo del área solicitante o superior jerárquico. La formalización se realiza mediante ticket en CIA - Desk, donde se deben especificar de manera detallada los recursos requeridos, tales como: • Equipo de cómputo. • Dispositivo móvil corporativo. • Cuenta de correo electrónico institucional. • Carpetas y directorios en servidores. • Sistemas corporativos como ERP CIASC, SICOB, FileMaker, Intranet de Sistemas de Gestión, entre otros. Cuando la solicitud implica el envío físico de equipos a sucursales, el área de Sistemas debe documentar la salida y recepción de los equipos en el formato FOR SIS 005 – Entradas y salidas de equipos, de acuerdo con lo establecido en el PRO SIS 001 – Procedimiento de Sistemas.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Gerente de RH Inplant RLB Responsables de Área

	Proveedores o invitados El acceso para proveedores, contratistas o invitados que deban desempeñar funciones en las instalaciones debe ser solicitado por el responsable del área donde se llevará a cabo la actividad. La solicitud se registra en CIA - Desk e incluye los privilegios temporales requeridos. • En accesos que impliquen conexión a sistemas críticos o servicios internos, el área de Sistemas debe escalar la solicitud para su autorización formal con la Gerencia Administrativa o la Dirección General, dependiendo de la criticidad del acceso. • Para el caso en que el proveedor o invitado solo requiera conectividad a internet, se autoriza el acceso a la red inalámbrica **CIASC-INVITADOS**. **Accesos a la red CIASC-INVITADOS** Cuando el requerimiento se limite al uso de la red inalámbrica de invitados: • El responsable del área debe levantar la solicitud en CIA - Desk. • El área de Sistemas configura en el portal cautivo de Fortinet un usuario temporal con una contraseña única para el invitado. • El tiempo de conexión permitido se limita a lapsos de 1, 2, 3, 4 o 5 horas, sin que ningún acceso temporal pueda superar las 8 horas continuas. • Si se requiere extender el acceso más allá de este límite, se debe gestionar una nueva autorización y generar un nuevo usuario en Fortinet.	
2.4	**Verificación previa a la creación de accesos** Antes de generar un usuario en cualquier sistema, el área de sistemas debe verificar: • Que el empleado esté registrado en la base de datos de empleados en FileMaker. • Que el rol asignado corresponda al puesto definido en la **Matriz de roles por activos de información críticos (FOR GSI 025)**, con el fin de asegurar que los privilegios otorgados correspondan a las funciones del cargo.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL
2.5	**Creación y documentación de accesos** Una vez validada la solicitud y verificado el rol del usuario en la **Matriz de roles por activos de información críticos (FOR GSI 025)**, el área de Sistemas procede con lo siguiente:	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL

	• Creación de usuario y asignación de contraseña inicial temporal en el sistema correspondiente, de acuerdo con las políticas de complejidad establecidas. • Registro del usuario en el Inventario y clasificación de usuarios de GLPI. • Elaboración de la Carta Responsiva FOR GSI 031 (usuario y activos asignados) y de la Autorización de Accesos FOR GSI 032, las cuales deben actualizarse en cada modificación de permisos. Nota – Requisito BBVA: En los casos en que la organización presta servicios a BBVA, se debe notificar a dicha institución sobre cualquier alta en la plantilla que afecte el servicio brindado. Con base en esta notificación, BBVA gestionará las credenciales de acceso a su plataforma extranet. Adicionalmente, el colaborador asignado debe firmar la Carta Compromiso de Accesos BBVA (FOR GSI 036) como condición para la entrega de sus credenciales, garantizando el cumplimiento de las políticas y lineamientos de seguridad definidos por el cliente.	
2.6	**Recertificación de accesos** La recertificación de accesos es un control fundamental del SGSI que permite validar periódicamente que los privilegios otorgados a los usuarios correspondan a su rol vigente y que las cuentas de empleados inactivos o de áreas distintas no permanezcan habilitadas indebidamente. Este proceso garantiza la aplicación continua del principio de privilegio mínimo y reduce la posibilidad de accesos no autorizados. • Periodicidad y coordinación: la Coordinación de Sistemas TI debe realizar la **recertificación de accesos de manera trimestral**. • Formato de control: la revisión se documenta en el **FOR SIS 010 – Recertificación de accesos**, donde se listan todos los usuarios activos y se valida su acceso frente a los derechos y permisos asignados. • Estados de recertificación: de acuerdo con los resultados, cada usuario debe clasificarse en uno de los siguientes estados: o Activo: el acceso se considera vigente y no requiere acciones adicionales. o Marcada: el acceso no se considera válido; se documenta como “no certificado” y se notifica al responsable para su corrección. o Suspendida: la cuenta queda bloqueada temporalmente y se notifica al área correspondiente. o Suprimida: el acceso es eliminado de manera definitiva y se emiten notificaciones de cierre.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL

	• Acciones y sanciones: cualquier hallazgo de accesos indebidos (cuentas activas de excolaboradores, privilegios no autorizados, uso de accesos de otras áreas) se gestiona como incidente de seguridad en CIA-Desk. Además, conforme al Código de Convivencia, pueden aplicarse sanciones administrativas a los colaboradores que incurran en mal uso de los accesos. Con este procedimiento, CIASC asegura que los accesos no solo se gestionen al momento de la creación o baja, sino que se revisen periódicamente para mantenerlos actualizados, controlados y en cumplimiento con los requisitos de la ISO/IEC 27001:2022.	
3	**Incapacidad, vacaciones, bajas de usuarios y cambios de puesto**	
3.1	**Notificación de incapacidades y vacaciones** El área de **Recursos Humanos** debe informar al área de sistemas, a través de **CIA - Desk y/o correo institucional**, cuando un colaborador se encuentre en incapacidad médica o vacaciones con duración mayor a una semana. Para reducir el riesgo de uso indebido de las cuentas durante este periodo: • El área de sistemas procede a **deshabilitar la cuenta o restablecer la contraseña temporalmente** en todos los sistemas críticos. • En caso de que durante la ausencia sea indispensable utilizar la cuenta, el responsable del área deberá solicitar la reactivación temporal vía correo electrónico, contando con autorización expresa de la **Dirección General**.	Dirección General Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Gerente de RH Inplant RLB Responsables de Área
3.2	**Bajas de usuarios y abandono de trabajo** En los casos de **baja definitiva, abandono de trabajo, cambio de departamento o cambio de puesto**, el área de Recursos Humanos debe notificar de inmediato al área de Sistemas mediante CIA - Desk y/o correo institucional. Dentro de las primeras **24 horas** posteriores a la notificación, el área de sistemas debe: • **Revocar o deshabilitar** todos los accesos del colaborador en **Active Directory (AD), Fortinet (portal cautivo), VPN Printunl, correo institucional y aplicativos** (ERP CIASC, Aspel, SICOB, FileMaker, GLPI, CIA - Desk, Intranet de Sistemas de Gestión). • En **Bonsaif, Presence y SICOB** las cuentas **no se eliminan**, únicamente se **desactivan**, preservando la trazabilidad de gestiones históricas realizadas por el colaborador. • Retirar al colaborador del **checador biométrico** para impedir registros posteriores.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Gerente de RH Inplant RLB Responsables de Área

	• Actualizar el estado del colaborador y activos asignados en **GLPI** (usuarios, equipos, periféricos). • Coordinar la **entrega de activos** con recabación de firma en la **Carta Responsiva FOR GSI 031** y registrar la recepción en GLPI. **Nota – Requisito BBVA:** En el caso de servicios asociados a **BBVA**, la organización debe notificar a dicha institución sobre la baja del colaborador, para que BBVA proceda al **reset de credenciales en la extranet** y asegure la continuidad operativa sin riesgos de acceso indebido.	
3.3	**Proveedores o invitados** El responsable del área **avisa a Sistemas** (CIA - Desk) para **deshabilitar de inmediato** el usuario temporal en **Fortinet (portal cautivo)** y cualquier otra cuenta provisional.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Responsables de Área
3.4	**Cambios de puesto o funciones** Cuando un colaborador cambia de puesto o de área: • El área de sistemas realiza **recertificación de accesos** con base en la **Matriz de roles por activos de información críticos (FOR GSI 025)**, **retirando** privilegios del rol anterior y **asignando** únicamente los que corresponden al nuevo rol (principio de privilegio mínimo). • Se **formaliza** la modificación con **FOR GSI 032 – Autorización de accesos** (firma del responsable del área) y se **actualizan** GLPI.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Gerente de RH Inplant RLB Responsables de Área
3.5	En caso de que algún colaborador haya causado baja o haya abandonado su trabajo, sus accesos de usuario serán eliminados y/o deshabilitados, esta actividad se deberá realizar en comunicación conjunta entre el departamento de sistemas y recursos humanos.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Gerente de RH Inplant RLB Responsables de Área
4	**Responsabilidad y uso de las claves de acceso**	
4.1	**Uso personal e intransferible** El manejo de credenciales constituye un control crítico en la seguridad de la información, ya que el uso indebido de un usuario y contraseña puede comprometer la confidencialidad, integridad y disponibilidad de los sistemas corporativos. Por esta razón, las credenciales asignadas son **personales, únicas e intransferibles**, y el colaborador que las recibe asume plena responsabilidad sobre su resguardo y correcto uso. La organización prohíbe de manera estricta cualquier práctica que implique compartir, delegar o divulgar credenciales, independientemente del cargo o nivel jerárquico.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL

	• Está **prohibido compartir contraseñas** con otros usuarios, incluyendo gerentes, supervisores, personal de TI o cualquier tercero, aun cuando exista autorización verbal o consentimiento. • Se prohíbe la **revelación de claves por cualquier medio**, ya sea oral, escrito, electrónico o mediante su almacenamiento en navegadores, macros, aplicaciones no autorizadas o herramientas externas. • Los colaboradores no pueden **utilizar cuentas ajenas**, aunque se trate de situaciones temporales o con autorización expresa del propietario. Cada acción realizada en los sistemas debe estar vinculada a la identidad real del usuario, para mantener trazabilidad y responsabilidad individual. • El incumplimiento de estas reglas se considera un **incidente de seguridad** y será gestionado mediante **CIA - Desk**. Según la gravedad del caso, puede derivar en **sanciones administrativas** conforme al Código de Convivencia de la organización e, incluso, en acciones disciplinarias mayores. Con estas disposiciones, la organización asegura que cada credencial se utilice de forma individual y controlada, garantizando la trazabilidad de todas las actividades realizadas en los sistemas y reforzando la cultura de responsabilidad personal en materia de seguridad de la información.	
4.2	**Complejidad y seguridad de las contraseñas** La organización establece que todas las contraseñas utilizadas en los sistemas corporativos deben cumplir con parámetros de complejidad suficientes para reducir el riesgo de adivinación, ataques de fuerza bruta o uso de información personal del colaborador. El área de Sistemas asegura la correcta aplicación de estas reglas mediante la configuración de políticas en Active Directory y revisiones periódicas en auditorías internas. • **Longitud mínima:** cada contraseña debe tener al menos **12 caracteres** para garantizar un espacio de búsqueda amplio en caso de intentos de descifrado. • **Combinación de caracteres:** se exige la inclusión obligatoria de **mayúsculas, minúsculas, números y caracteres especiales** (ejemplo: @, &, #, %), con el fin de elevar la entropía de la clave. • **Restricciones en patrones:** no se permite la repetición excesiva de caracteres, el uso de secuencias consecutivas (12345, abcde) ni patrones de teclado predecibles (qwerty, asdf). • **Prohibición de datos personales:** está prohibido utilizar contraseñas basadas en nombres propios, fechas de nacimiento, direcciones, nombres de familiares u otra información personal o de fácil asociación con el usuario.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL

	• **Historial y reutilización:** las últimas **tres contraseñas** usadas por el mismo usuario no podrán repetirse, lo que obliga a generar nuevas combinaciones en cada cambio. Con esta política de complejidad, CIASC asegura que las contraseñas de los usuarios cumplan estándares robustos, dificultando intentos de intrusión y asegurando el cumplimiento de los requisitos del **SGSI** y de la norma **ISO/IEC 27001:2022**.	
4.3	**Caducidad y cambios obligatorios** El control de caducidad de contraseñas es un requisito esencial para mitigar el riesgo de accesos indebidos prolongados y reducir el impacto en caso de que una clave sea comprometida. Por esta razón, la organización ha definido un procedimiento que regula la vigencia máxima de las contraseñas y establece los procedimientos a seguir para sistemas que no cuentan con mecanismos automáticos de expiración. • **Vigencia general:** todas las contraseñas tienen una vigencia máxima de **90 días**. Transcurrido este plazo, el sistema exige el cambio obligatorio para asegurar la renovación periódica de las claves. • **Sistemas con limitaciones técnicas:** en aplicaciones como **Opti-risks, ERP, FileMaker, SICOB, Aspel, Bonsaif, Presence y Bluemessaging**, que no permiten la caducidad automática, el área de Sistemas genera la contraseña inicial y la entrega de manera segura al usuario por correo electronico. Este último debe modificarla en su **primer inicio de sesión**, cumpliendo con los criterios de complejidad establecidos en este procedimiento. • **Cambios extraordinarios:** en caso de existir sospecha de que una contraseña ha sido comprometida (ejemplo: acceso desde una ubicación no habitual, notificación de intento de intrusión o reporte de phishing), el usuario está **obligado a cambiar su clave de inmediato** y notificar el incidente mediante **CIA - Desk**. • **Trazabilidad:** cada cambio de credenciales queda registrado en los logs del sistema correspondiente y, en sistemas sin control automático. De esta forma, CIASC asegura que todas las contraseñas, independientemente del sistema en que se utilicen, se renueven en ciclos definidos y bajo trazabilidad, manteniendo la confidencialidad y reduciendo la exposición a riesgos de seguridad	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL
4.4	**Sistemas corporativos y vinculaciones** La autenticación de los sistemas corporativos de la organización se encuentra centralizada en la infraestructura local de CIASC, bajo administración del área de Sistemas, lo que permite uniformidad en políticas de seguridad y eliminación del riesgo asociado al uso de servicios externos o en nube. De esta forma, todos los accesos se gestionan desde servidores propios y bajo control total de la organización.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL

	• **Sistemas integrados con Active Directory (AD):** En el caso de las estaciones de trabajo corporativas, el correo electrónico institucional y otros aplicativos integrados a AD, la autenticación se administra directamente en los **servidores locales de CIASC**, lo que permite aplicar de forma centralizada las políticas de complejidad, caducidad y bloqueo de cuentas. Este esquema garantiza consistencia y facilita la trazabilidad de accesos mediante logs y revisiones periódicas. • **Sistemas no integrados a AD:** Para plataformas como **Opti-risks, ERP, FileMaker, SICOB, Aspel, Bonsaif, Presence y Bluemessaging**, que no soportan autenticación con AD, las contraseñas son **generadas inicialmente por el área de Sistemas** y comunicadas de manera segura al usuario. Este último está obligado a **modificar la contraseña en su primer inicio de sesión**, asegurando el cumplimiento con los criterios de complejidad y caducidad definidos en este procedimiento.	
4.5	**Bloqueo de cuentas por intentos fallidos** El bloqueo automático de cuentas es un mecanismo preventivo contra ataques de fuerza bruta o intentos de acceso indebido. Este control permite reducir el riesgo de intrusión derivado de múltiples intentos consecutivos de adivinación de contraseña y asegura que los accesos fallidos queden registrados para su análisis. En CIASC, este control se aplica de manera centralizada en los servidores locales y se ajusta según la criticidad de cada sistema. • Criterio de bloqueo: las cuentas de usuario en Active Directory y en sistemas integrados quedan bloqueadas de manera automática tras tres intentos consecutivos fallidos de autenticación. Este umbral se definió con base en análisis de riesgo y prácticas recomendadas de seguridad. • Desbloqueo de cuentas: únicamente el área de Sistemas puede desbloquear una cuenta bloqueada. Para ello, se valida previamente la identidad del colaborador y se documenta la acción en CIA - Desk como evidencia de la gestión. • Sistemas no integrados en AD: en aplicaciones como ERP, FileMaker, SICOB, Aspel, Bonsaif, Presence y Bluemessaging, el área de Sistemas aplica manualmente las mismas políticas de bloqueo o desactivación de cuentas, de acuerdo con las capacidades técnicas de cada aplicación. En todos los casos, las acciones quedan documentadas en CIA - Desk. • Trazabilidad: cada bloqueo o intento de acceso fallido queda registrado en los logs del sistema y es revisado periódicamente conforme al LIS GSI 002 – Revisión de LOGS. Cualquier patrón anómalo (intentos desde IP desconocidas, cuentas de alta criticidad comprometidas) se gestiona como incidente de seguridad mediante el PRO GSI 020 – Gestión de Incidentes.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL
4.6	**Formalización y aceptación de credenciales** La entrega de credenciales a cada colaborador debe estar acompañada de un proceso formal que garantice que el usuario comprende y acepta las responsabilidades que	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI

	conlleva el uso de sus accesos. De esta forma, la organización asegura la trazabilidad de la asignación de privilegios, el compromiso explícito del colaborador y la disponibilidad de evidencia documental para auditorías internas y externas. • **Carta Responsiva FOR GSI 031**: al momento de la asignación inicial, el colaborador firma la carta donde reconoce los activos asignados (PC, laptop, celular, correo, cuentas de sistemas) y acepta el resguardo de sus credenciales bajo confidencialidad. • **Autorización de Accesos FOR GSI 032**: se utiliza para documentar y autorizar los accesos otorgados al usuario según su rol en la organización. Este formato se actualiza cada vez que exista una modificación de permisos o privilegios, manteniendo evidencia histórica de todos los cambios. • **Registro en GLPI**: tanto la creación de la cuenta como la asignación de activos y credenciales se registra en el inventario centralizado, vinculando al colaborador con los equipos y sistemas bajo su responsabilidad. • **Aceptación de responsabilidades**: con la firma de los formatos y la recepción de credenciales, el colaborador acepta expresamente que: o Sus credenciales son personales e intransferibles. o El uso indebido de las mismas será considerado un incidente de seguridad. o Está obligado a cumplir con las políticas de complejidad, caducidad y uso seguro de contraseñas definidas en este procedimiento.	Colaboradores en GRAL
5	**Gestión de Claves del Usuario**	
5.1	**Generalidades** La gestión de claves de usuario es uno de los controles más relevantes del SGSI, dado que de su correcta administración depende la seguridad de todos los sistemas críticos de la organización. El área de Sistemas administra el ciclo de vida completo de las credenciales, asegurando que cada cuenta esté asociada a un colaborador legítimo, que cumpla con los criterios de complejidad definidos, que tenga trazabilidad en los sistemas de gestión y que sea deshabilitada oportunamente en caso de incidentes o bajas.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL
5.2	**Entrega inicial de credenciales** Cuando se da de alta un usuario en los sistemas corporativos, el área de Sistemas genera una contraseña inicial temporal para habilitar su primer acceso. La entrega de estas credenciales debe realizarse bajo un esquema de **doble canal seguro**, evitando que tanto el usuario como la contraseña viajen por el mismo medio de comunicación.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL

	• La **primera parte (usuario y nombre de cuenta)** se envía por **correo institucional seguro** al colaborador, dirigido únicamente a la dirección validada y registrada en Recursos Humanos y GLPI. • La **segunda parte (contraseña inicial temporal)** se comunica por **llamada telefónica directa** al colaborador, previa verificación de identidad mediante datos personales y laborales registrados en el expediente del empleado. • El colaborador debe modificar la contraseña asignada en su **primer inicio de sesión**, siguiendo las políticas de complejidad establecidas en el punto 4.2 de este procedimiento. • El proceso de entrega queda documentado en **CIA - Desk**, y el colaborador firma la **Carta Responsiva FOR GSI 031** como evidencia de aceptación y compromiso de confidencialidad. Con este esquema de entrega en dos canales diferenciados (correo seguro + llamada telefónica), la organización asegura que ninguna credencial viaje de manera completa por un solo medio, reduciendo la probabilidad de intercepción y fortaleciendo la postura de seguridad en la fase más crítica del ciclo de vida de los accesos: su creación inicial.	
5.3	**Cambios periódicos y caducidad** La política corporativa establece que todas las contraseñas deben ser renovadas cada **90 días** como máximo. Esto permite reducir la ventana de exposición en caso de que una clave sea comprometida y no se detecte de inmediato. • En sistemas integrados con **Active Directory**, la caducidad se aplica automáticamente mediante políticas locales (GPO) en los servidores de CIASC, sin depender de servicios externos. • En sistemas que no cuentan con expiración automática (ERP CIASC, SICOB, Aspel, FileMaker, Presence, Bluemessaging, Bonsaif), el área de Sistemas genera la contraseña inicial y el usuario debe modificarla en su primer acceso, quedando registrado en CIA - Desk para auditoría.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL
5.4	**Seguridad y almacenamiento** El resguardo seguro de contraseñas es indispensable para protegerlas de ataques de diccionario, fuerza bruta o robo mediante malware. • Durante el inicio de sesión, las contraseñas **nunca son visibles en pantalla**; todos los sistemas están configurados para mostrar caracteres enmascarados.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL

	• En el backend, los sistemas almacenan los **hashes de contraseñas en servidores locales de CIASC**, aplicando algoritmos de cifrado robustos, lo que evita que se conserven en texto plano. • El área de Sistemas nunca almacena ni comunica contraseñas por medios no autorizados; toda interacción queda registrada en **CIA - Desk** como parte de la evidencia. • Los intentos de autenticación se registran en **logs**, y ante tres intentos fallidos consecutivos se aplica el bloqueo automático, como se describe en el punto 4.5 de este procedimiento.	
5.5	**Cuentas con credenciales de fábrica** Todo hardware o software que ingrese a la red corporativa debe ser sometido a un proceso de **hardening inicial**, el cual incluye la sustitución de contraseñas de fábrica antes de que el equipo quede en operación. • Este control se aplica en switches, firewalls, access points, aplicaciones nuevas o reinstaladas, evitando vulnerabilidades derivadas de contraseñas conocidas públicamente. • El cambio debe realizarse siguiendo las políticas de complejidad establecidas en este procedimiento. • En auditorías internas, se revisa que ningún dispositivo en red opere con credenciales de fábrica y que todo cambio haya sido gestionado en tiempo y forma por el área de Sistemas.	Gerente Administrativo Coordinador TI Desarrollador Auxiliar TI Colaboradores en GRAL
5.6	**Cuentas de emergencia** Existen cuentas de emergencia diseñadas para situaciones de contingencia, como pérdida de conectividad, bloqueo generalizado de cuentas o recuperación de desastres. • Estas cuentas son creadas en **servidores locales de CIASC** y no son administradas por el área de Sistemas, sino custodiadas directamente por la **Dirección General**, para limitar el riesgo de uso indebido. • Su uso está estrictamente restringido a escenarios extraordinarios, bajo autorización de Dirección General, y debe documentarse en **CIA-Desk** como incidente de seguridad.	Dirección General Gerente Administrativo Coordinador TI
5.7	**Custodia de claves críticas en Keeper**	Dirección General Gerente Administrativo

	Además de las políticas generales de gestión de contraseñas de usuario, la organización mantiene bajo control centralizado en la herramienta **Keeper** todas las **credenciales críticas, llaves maestras y accesos de administración** que no pueden ser gestionados de forma manual o individual. • Keeper actúa como un **repositorio cifrado** de contraseñas y secretos, bajo infraestructura local administrada por el área de Sistemas y supervisada por la Dirección General. • Las credenciales almacenadas incluyen, entre otras, las llaves maestras de cifrado, usuarios privilegiados de administración de servidores y accesos de servicio de sistemas críticos. • El acceso a Keeper está restringido a la dirección general y gerencia administrativa, con autenticación multifactor y trazabilidad de cada ingreso. • Keeper asegura que ninguna credencial crítica quede almacenada en archivos locales, hojas de cálculo o repositorios inseguros, eliminando uno de los principales riesgos en la gestión de secretos corporativos.	
6	**Inicio de sesión segura**	
6.1	**Generalidades** El inicio de sesión en los equipos corporativos es un control fundamental que garantiza que únicamente usuarios legítimos y equipos autorizados accedan a la red de la organización. Con este mecanismo, CIASC evita intentos de suplantación, intercepción de credenciales o ejecución de programas maliciosos que pretendan capturar usuarios y contraseñas durante el arranque del sistema. Todas las estaciones de trabajo y portátiles están configuradas bajo un esquema de **inicio de sesión segura**, reforzado con controles técnicos adicionales que aseguran la integridad del dispositivo y la identidad del usuario antes de habilitar la conexión a los recursos internos.	Gerente Administrativo Coordinador TI Colaboradores en GRAL
6.2	**Combinación obligatoria** Todos los equipos requieren que el usuario presione la secuencia **Ctrl+Alt+Supr** antes de introducir sus credenciales de Active Directory. Este mecanismo asegura que el proceso de autenticación se ejecute directamente en el sistema operativo, evitando que aplicaciones maliciosas simulen pantallas de inicio de sesión para robar credenciales.	Gerente Administrativo Coordinador TI Colaboradores en GRAL

6.3	**Validación del endpoint** Además de la autenticación del usuario, los equipos deben cumplir con los requisitos de postura mínima definidos por la organización. Esto incluye tener habilitado **BitLocker para el cifrado de disco**, **SentinelOne en operación** como sistema de protección avanzada contra malware, y un **certificado SSL corporativo válido** instalado en el endpoint. Si alguno de estos controles no está activo, el equipo no puede establecer conexión a la red corporativa.	Gerente Administrativo Coordinador TI Colaboradores en GRAL
6.4	**Seguridad reforzada en red** Una vez autenticado, todo el tráfico generado por el equipo se canaliza obligatoriamente a través de la **VPN Printunl** y es inspeccionado por las políticas de Fortinet (firewall, IPS, inspección SSL, filtrado web, control de aplicaciones). Con ello se asegura que la sesión de usuario esté cifrada y controlada desde el primer momento de conexión.	Gerente Administrativo Coordinador TI Colaboradores en GRAL
6.5	**Registro y trazabilidad** Cada intento de inicio de sesión queda registrado en los **logs de Active Directory**, los cuales son revisados cada 15 días conforme a este procedimiento y los resultados se documentan en el formato **LIS GSI 002 – Revisión de LOGS**. Los hallazgos, como intentos fallidos repetitivos o accesos en horarios no habituales, se documentan y gestionan como incidentes en **CIA-Desk**.	Gerente Administrativo Coordinador TI Colaboradores en GRAL
7	Usuarios Privilegiados o con excepciones	
7.1	La asignación de privilegios para personal diferente al del área de sistemas puede hacerse en dos casos: • **Privilegios o excepciones inherentes al puesto**: Son aquellos privilegios, que por la naturalidad del puesto se deben tener para poder desarrollar las actividades del colaborador y están declarados en el formato **excepciones por puesto FOR SIS 009.** • **Solicitud de asignación de privilegios**: son aquellos que se solicita el supervisor o gerente del área a través de la plataforma CIA - Desk, cuando al personal se le asignan nuevas actividades temporales o definitivas. Nota: la solicitud de privilegios únicamente la puede hacer el gerente o supervisor del área y esta será autorizada por dirección general y/o gerente administrativo.	Dirección General Gerente Administrativo Coordinador TI
7.2	Asignación de privilegios o excepciones inherentes al puesto.	Dirección General Gerente Administrativo

	Cuando ingrese un nuevo colaborador, el personal de sistemas verificará que el usuario no tenga privilegios asignados, de acuerdo al **formato excepciones por puesto FOR SIS 009**, cuando el puesto tenga privilegios autorizados, el personal de sistemas los asignará y el colaborador deberá firmar la **carta responsiva de excepciones FOR GSI 051**.	Coordinador TI
7.3	Solicitud de asignación de privilegios Cuando el personal de sistemas reciba una solicitud de privilegios a través del portar CIA - Desk, el personal de sistemas solicitará la autorización de la Dirección general y/o Gerente administrativo en formato **excepciones FOR GSI 047**, una vez aprobada, signará los privilegios al usuario y dará a firmar al usuario y al supervisor o gerente de área la **carta de autorización FOR GSI 032** con el objetivo de hacerlos responsables por el buen manejo de este. Nota: los privilegios deben durar máximo 3 meses, después de culminar ese tiempo deberán renovarse o en caso de ya no requerirlos se deberán revocar.	Dirección General Gerente Administrativo Coordinador TI
7.4	Cambio de privilegios temporales a permanentes. El Gerente Administrativo asignará como privilegios permanentes o inherentes al puesto en el formato de **excepciones por puesto FOR SIS 009**, cuando se haya renovado tres veces consecutivas el formato de **excepciones FOR GSI 047**, es decir, el personal requiera más de 9 meses consecutivos los privilegios o excepciones solicitadas. Cuando los privilegios pasen de temporales a permanentes, el personal de Sistemas realizará las actividades descritas en la sección 7.2.	Dirección General Gerente Administrativo Coordinador TI
7.5	El departamento de sistemas por la naturaleza de sus operaciones debe operar con usuarios privilegiados (administradores), este usuario privilegiado será creado y gestionado por la Dirección General y/o el Gerente Administrativo, a fin de poder restringir el uso deliberado en servidores y/o aplicativos de la misma, este usuario deberá ser registrado y el usuario firmará la **carta de autorización FOR GSI 032** de accesos a fin de hacerse responsable por el buen manejo de este. Cuando ingrese un colaborador nuevo al departamento de sistemas, el Coordinador de Sistemas TI deberá solicitar, mediante correo electrónico o sistema de tickets CIA - Desk a la Dirección General y/o al Gerente Administrativo, un usuario privilegiado con restricciones a fin de que este pueda desarrollar sus actividades, la Dirección General y/o el Gerente Administrativo serán los encargados de emitir las nuevas credenciales al correo corporativo del colaborador.	Dirección General Gerente Administrativo Coordinador TI
7.6		Dirección General Gerente Administrativo

	En cuanto se notifique la baja de algún colaborador del departamento de sistemas, la dirección general y/o el gerente administrativo deberá de deshabilitar los accesos del colaborador que esté causando baja. La dirección general y/o el gerente administrativo serán los encargados de revisar el visor de eventos cada 30 días, para verificar las acciones de los usuarios privilegiados a fin de asegurar el buen manejo de estos por parte del personal de sistemas y se registrará en el formato **Revisión de visor FOR GSI 053**, en caso de identificar alguna falta o mal manejo de los usuarios privilegiados, la dirección general y/o el gerente administrativo actuarán en apego al código de convivencia, a fin de sancionar al colaborador que haya realizado la falta, estas faltas quedarán documentadas por correo electrónico involucrando al departamento de recursos humanos para la actuación de la sanción.	Coordinador TI