1. OBJETIVO

Establecer las medidas administrativas, técnicas y físicas a mantener de acuerdo con las necesidades creadas por la estrategia de negocio, reglamentos, legislaciones, contratos y entorno actual para proteger, garantizar los principios de la Seguridad de la Información y los establecidos en la Ley Federal de Protección de Datos Personales:

- Confidencialidad;
- Integridad;
- Disponibilidad;
- Licitud;
- Consentimiento;
- Información;
- Calidad;
- Finalidad;
- Lealtad;
- Proporcionalidad;
- Responsabilidad.

2. ALCANCE

Aplicable a todo el personal de las siguientes razones sociales:

- INTEGRADORES DE TECNOLOGÍA S.A. DE C.V.,
- INTERCONECTA S.A. DE C.V.,
- COOPSA AMBIENTAL S.A. DE C.V.,
- GA ENERGY SERVICES S.A.P.I. DE C.V.
- TELIKO SOLUTIONS S.A.P.I. de C.V.
- CUSTOM SOFT S.A.P.I. de C.V.
- INNOVACIÓN Y LIDERAZGO S de R.L.

Y a las partes interesadas de la organización que se consideren pertinentes.

3. DEFINICIONES

No.	Concepto	Descripción
1.	**Amenaza**	Causa potencial de un incidente no deseado, que puede resultar en daño a una organización del sistema.
2.	**CMDB**	CMDB por sus siglas en inglés Base de datos de la gestión de configuración, es un Repositorio de información donde se relacionan todos los activos de información.
3.	**CSIRT**	Computer Security Incident Response Team, por sus siglas en inglés, es un equipo especializado de profesionales de TI que se encarga de la gestión y respuesta a incidentes de seguridad informática en una organización
4.	**Seguridad de la información**	Es la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma
5.	**SIG**	Sistema Integrado de Gestión de la organización
6.	**Usuario (a)**	Persona que recibe, maneje, procese o transmite información por medios electrónicos o documentales.
7.	**Vulnerabilidad**	Debilidad presente en un activo de información que potencialmente permitirá que una amenaza lo impacte de manera negativa, con posibles afectaciones para la seguridad de la información dentro de la Organización.

4. CONTROLES ORGANIZACIONALES

4.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Alta Dirección

Justificación

La Dirección General establece y manifiesta su apoyo a la seguridad de la información y protección de datos personales, publicando y manteniendo el presente **MA-GPO-01** Manual del Sistema Integrado de Gestión, para los tratamientos:

I. Obtención;
II. Almacenamiento;
III. Acceso;
IV. Procesamiento;
V. Remisión;
VI. Transferencia;
VII. Bloqueo;
VIII. Cancelación;
IX. Supresión y
X. Destrucción.

Para tal efecto la Dirección define la **DE-GPO-01** Declaratoria Política del SIG, conforme lo siguiente:

*DNA International Group, comprometida con la prestación de servicios enfocados en la total satisfacción de sus clientes y partes interesadas, promueve entre su personal el cumplimiento de leyes, reglamentos, normativa aplicable y de su Política del Sistema Integrado de Gestión (SIG), orientada en resolver requisitos globales de calidad, protección ambiental, seguridad y bienestar laboral, tecnologías, seguridad de la información, continuidad del negocio, Antisoborno, Igualdad laboral y no discriminación, protección y cumplimiento a los deberes, obligaciones y requerimientos de la LFPDPPP y su reglamento, bajo los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, de acuerdo a lo establecido en el **MA-GPO-04** Manual de Aplicabilidad de Controles de Seguridad de la Información y Datos Personales en un ambiente de mejora continua, que le permita alcanzar sus objetivos y factores críticos de éxito a través de sus procesos estratégicos, primarios y de soporte.*

El **MA-GPO-01** Manual del Sistema Integrado de Gestión, **DE-GPO-01** Declaratoria Política del SGI y el **MA-GPO-04** Aplicabilidad de controles de seguridad de la información, deberán ser revisados al menos una vez al año o en caso de que ocurra algún cambio, de acuerdo con la necesidad actual de la operación y comunicarse a las partes interesadas.

4.2. ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Certificaciones

Justificación

Los procedimientos documentados del sistema de seguridad de la información deben identificar los roles y responsabilidades conforme a los siguientes elementos:

- **DE-GPO-03** Declaratoria responsables del SIG;
- **DE-GAL-08** Declaratoria de responsable del SGSDP;
- **FO-GTI-16** Asignación de roles y responsabilidades;
- **FO-GTI-43** Matriz de asignación de roles;
- **FO-GCH-33** Descriptivo de Puesto
- Manuales, procedimientos, políticas, anexos, instructivos, declaratorias, etc.

4.3. SEGREGACIÓN DE TAREAS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Recursos Humanos

Justificación

Con el objetivo de evitar que el personal de la organización puedan ser juez y parte en el ejercicio de sus funciones, cada procedimiento documentado específica los roles que intervienen al desempeñar cada actividad, según la fase del proceso que se desarrolla.

4.4. RESPONSABILIDADES DE GESTIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de: Administración de Personal; Capacitación; Certificaciones.

Justificación

Para el personal de nuevo ingreso, el Responsable de Administración de Personal debe asegurar la existencia de cláusula de confidencialidad en el contrato individual de trabajo, así como el **DE-GAL-05** Aviso de privacidad solicitud de empleo, **DE-GAL-17** Aviso de privacidad para colaboradores, debidamente firmado y resguardado en el expediente del personal conforme al **PR-GCH-01** Atracción de talento, contratación e inducción.

El Responsable de Capacitación debe impartir la inducción conforme al **PR-GCH-08** Capacitación asegurando que contenga los elementos básicos del SIG incluyendo temas de seguridad de la información.

El Responsable de Certificaciones debe diseñar e implementar un esquema para concientizar en materia de seguridad de la información conforme al **PR-GCH-05** Comunicación institucional.

4.5. CONTACTO CON LAS AUTORIDADES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de SASSO Gestor / Oficial de seguridad

Justificación

El Responsable de SASSO debe identificar y documentar en la **FO-GSS-22** Matriz de contacto con autoridades, la información necesaria para contactar o informar cualquier afección o daño a las instalaciones, personas, así como revisarla y mantenerla actualizada asegurando su revisión al menos una (1) vez al año.

En caso de vulneración a los activos de información o incidente de ciberseguridad el Gestor / Oficial de seguridad, deberá contactar a la policía cibernética, por los siguientes medios:
Teléfono: **5552425100** ext. **5086**
Correo electrónico: **policiacibernetica@ssc.cdmx.gob.mx**

En caso de vulneración a los datos personales, la Oficial de Cumplimiento debe notificar a la Secretaría Anticorrupción y Buen Gobierno al correo: **unidadtransparencia@buengobierno.gob.mx**

4.6. CONTACTO CON GRUPOS DE ESPECIAL INTERÉS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

El Gestor / Oficial de seguridad debe mantener contacto con grupos de especial interés a través de suscripciones con: consultorías, fabricantes o partners y publicaciones especializadas u otros foros de seguridad especializados.

- Identificar fuentes de información internas y externas para saber sobre las tendencias de amenazas que pudieran afectar a la organización.
- Las recomendaciones de seguridad deberán ser comunicadas a la organización
- Podrán solicitarse platicas de sensibilización a la Policía Cibernética al teléfono **5552425100** ext. **5666** o al correo: **prevencion.cibernetica@ssc.cdmx.gob.mx**

4.7. INTELIGENCIA SOBRE AMENAZAS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Detectivo Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

Se debe recopilar y analizar la información sobre las amenazas existentes o posibles.
El Gestor / Oficial de Seguridad debe:

- Revisar la información para comprender su nivel de significancia incluyendo el filtrado de falsos positivos.
- En el caso de Teliko, las vulnerabilidades identificadas deberán ser analizadas por el **CSIRT** para efecto de la toma de decisión en la iteración del riesgo diligente.
- Actualizar las firmas y listas de bloqueos de los controles de seguridad de la información. (firewall, entre otros) que pueda afectar a la infraestructura critica de la organización.

- El ciclo de vida de la inteligencia de amenazas deberá realizarse de acuerdo con los requisitos de las partes interesadas que se consideren pertinentes.

4.8. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Proyectos

Justificación

El Responsable del Proyecto debe:

- Asegurar que todo proyecto considere la definición de especificaciones y requerimientos de seguridad de la información de acuerdo con su tipo y naturaleza a través de la identificación, análisis y tratamiento de riesgo, tomando en cuenta el **AX-GTI-01** Lista de requisitos de seguridad y de acuerdo con lo solicitado por el cliente en el Anexo técnico o Contrato
- Establecer y acordar con las partes interesadas del servicio el acceso, tratamiento, almacenaje, comunicación o provisión de componentes a la infraestructura de TI.

4.9. INVENTARIO DE INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementada	Administrador de la CMDB / Gestor de activos y configuraciones Resp. de Telefonía Resp. de Procesos

Justificación

El Administrador de la CMDB / Gestor de activos y configuraciones, debe:

- Mantener el inventario de los activos de TI, asignación y estatus en la herramienta digital definida por la organización, de acuerdo con el **PR-GTI-08** Gestión de activos y configuraciones. Las líneas base de configuración deben mantenerse de acuerdo con lo establecido en el apartado 8.13 Respaldos de la información
- Resguardar las responsivas de asignación de activos al personal **FO-GTI-41** Carta responsiva de equipo de cómputo y otros activos asociados conforme el **PR-GTI-13** Altas y bajas de equipo de cómputo.
- Revisar periódicamente las bases de datos de los activos con el fin de validar que las personas que hayan causado baja no se encuentren en el listado de usuarios.

El Responsable de Procesos debe mantener actualizado el **FO-GPO-01** Lista maestra de documentos con base en el **PR-GPO-01** Control Documental.

4.10. USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

a) El Gestor / Oficial de Seguridad debe implementar y mantener controles (para el personal, terceros o proveedores) para efecto de prevenir la pérdida, modificación o divulgación de información que se encuentre en pantallas, escritorios, lugares de fácil acceso o en lugares de trabajo conforme a lo siguiente:

- Supervisar las áreas seguras para evitar actividades maliciosas que pongan en riesgo la información.
- Establecer mecanismos en áreas de trabajo asignadas que se encuentren desocupadas para resguardar la información como gavetas y escritorios con llave.

b) Queda prohibido el ingreso a las instalaciones de equipo de cómputo personal, el cual, no recibirá ninguno de los servicios proporcionados por el responsable de TI y tampoco existe responsabilidad alguna en caso de falla o problemas con los servicios que se presenten en los mismos.

c) El uso de las herramientas de trabajo (equipo de cómputo, internet, cuentas de correo), asignados al personal son estrictamente para funciones de interés de la organización por lo que deben:

- Asumir toda responsabilidad en el uso de las herramientas, dispositivos de almacenamiento externo, así como la información que maneja dentro de ellos.
- Monitorear la capacidad de almacenamiento del buzón (50 GB), depurándola constantemente.

d) Queda prohibido realizar cualquiera de las siguientes actividades:

- Usar las herramientas proporcionadas por la empresa para asuntos personales;
- Prestar o transferir el activo a cualquier persona distinta a quien fue asignado;
- Compartir sus cuentas y contraseñas;
- Generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola;
- Crear o reenviar cartas cadena o cualquier otro esquema de pirámide de mensajes;
- Enviar mensajes masivos (spam) para anunciar u ofrecer la venta o compra de cualquier bien o servicio para cualquier fin comercial, a menos que la organización brinde la autorización para realizarlo;
- Enviar información restringida o confidencial o datos personales que sea propiedad del cliente o socio de negocio sin su aprobación y que no sea requerida por la naturaleza de sus actividades. En caso de ser requerido, deberá solicitarse la autorización formal a su Líder inmediato y al Gestor / Oficial de seguridad;
- Difamar, abusar, acosar, hostigar y amenazar a personas por correo electrónico;
- Publicar, exponer, cargar, distribuir o diseminar cualquier tema, nombre, material o información inapropiados, religiosos, difamatorios, infractores, obscenos, inmorales o ilegales;
- Cargar archivos que contengan software u otro material protegido por las leyes sobre propiedad intelectual, a menos que se posea el control de los derechos sobre el mismo o se haya recibido todos los consentimientos necesarios para hacerlo;
- Cargar archivos que contengan virus, archivos dañados, programas que descarguen otros archivos, o cualquier otro programa o software que pueda perjudicar el funcionamiento de los equipos de otros;
- Anunciar, enviar, o emitir contenido del cual no se tiene el derecho de transmisión por ley o bajo relación contractual tal como información exclusiva o confidencial y/o información entregada como parte de las relaciones de empleo o bajo contratos de confidencialidad;

- Falsificar o eliminar alguna atribución de autor, aviso Jurídico u otro apropiado, designación o etiqueta de propiedad en el origen o la fuente del software u otro material contenido en un archivo que esté cargado;
- Recopilar y transmitir información acerca de otros, incluidas direcciones de correo electrónico;
- Crear una identidad falsa con el propósito de confundir a otros;
- Acceder y/o descargar contenido pornográfico;
- Descargar e instalar cualquier tipo de software sin la autorización respectiva;

e) La organización reserva el derecho de regular, filtrar y revisar la información contenida en mensajes y buzones de correo, así como información almacenada en One Drive, para atención de diferentes revisiones, auditorías, monitoreo y seguimiento del cumplimiento de las políticas de seguridad, lo anterior con base en que la información es propiedad de la organización.

f) Para los casos especiales o excluyentes deberá existir:

- Una justificación formal orientada a satisfacer los requerimientos y objetivos del negocio y sus partes interesadas;
- Una referencia a cada uno de los apartados del uso aceptable de los activos a ser excluidos;
- Un apartado que describa el nivel de riesgo existente por la exclusión del uso aceptable de los activos;
- Vigencia de la exclusión;
- Aprobación explícita por parte del Líder inmediato y del Gestor / Oficial de seguridad a través de un correo electrónico.

g) Daños al equipo de TI (Celular, laptop y monitores).

Deberá cobrarse al colaborador responsable, el 100% del costo del equipo cuando:

- Por cualquier caída, golpe o derrame de líquidos, ya no funcione;
- Se haya perdido el equipo.

En caso de daño al equipo de TI (Celular, laptop y monitores) y que no aplique la garantía, el usuario se compromete a través de la firma de **FO-GTI-41** Carta responsiva de equipo de cómputo y otros activos asociados a realizar el pago establecido en este apartado.

En caso de robo del equipo de cómputo o telecomunicaciones, el personal debe presentar al área de Recursos Humanos con copia a la Dirección de Tecnologías de la Información, la constancia de hechos del Ministerio Público en la que señale marca, modelo y número de serie de cada uno de los equipos robados.
No se condonará el cobro de sustitución de equipo por robo cuando el equipo haya sido resguardado en un automóvil.

h) El Responsable de Procesos debe definir el manejo, tratamiento, almacenamiento y transmisión de la información de acuerdo con su clasificación conforme al **AX-GPO-07** Elaboración de documentos.

4.11. DEVOLUCIÓN DE ACTIVOS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementada	Administrador de la CMDB / Gestor de activos y configuraciones

Justificación

En el momento que cualquier persona, consultor o contratista termine su relación con la organización, toda propiedad de la organización debe ser devuelta, incluyendo, sin limitantes, computadoras portátiles, documentación, llaves de oficina, tarjetas de crédito, o cualquier activo de información que le haya sido conferido para el desempeño de sus actividades.

El Responsable de Recursos Humanos debe solicitar la recolección de activos de acuerdo con el **PR-GTI-13** Altas y bajas de equipo de cómputo al momento de la aplicación de la baja y el Administrador de la CMDB / Gestor de activos y configuraciones debe gestionar el cambio de contraseñas en el Directorio Activo y en los aplicativos a los que tuviera acceso el excolaborador, con la finalidad de evitar manipulaciones a los sistemas o a la información.

Las cuentas de correo electrónico seguirán activas 30 días hábiles después de aplicada la baja. Al termino de estos 30 días la cuenta de correo será eliminada en su totalidad. Si por razones necesarias para la organización requiere mantenerse activa, deberá comunicarse al área de TI con la justificación y el VoBo del Director del área.

4.12. CLASIFICACIÓN DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Procesos

Justificación

El Responsable de Procesos debe asegurar la clasificación de la información de acuerdo con los siguientes niveles:

Información	Descripción
Pública	Del dominio de internos y externos al negocio, no produce impacto su divulgación.
Interna	Gestionada únicamente entre las áreas que así lo requieren para el logro de sus funciones. Impacto moderado si la conocen Áreas ajenas a las que la originaron.
Confidencial	Generada por un Área, para su uso exclusivo como parte de sus funciones, bajo su criterio se reserva y responsabiliza de su acceso, transferencia o distribución, incluye datos personales. Impacto alto si se divulga hacia entidades no autorizadas
Reservada	Manejo exclusivo aprobado por Directivos, comúnmente para desarrollo de estrategias de nuevos negocios, incluye a la información de nuestros clientes. Impacto grave si se divulga hacia entidades no autorizadas.

Ver **AX-GPO-07** Elaboración de documentos.

4.13. ETIQUETADO DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Procesos

Justificación

El etiquetado de la información debe hacerse conforme en el **AX-GPO-07** Elaboración de documentos.

4.14. TRANSFERENCIA DE INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Administrador de la CMDB / Gestor de activos y configuraciones Oficial de Cumplimiento. Resp. AP, Jurídico.

Justificación

El Gestor de Activos y Configuraciones debe:

- Asegurar que toda información reservada o confidencial transportada en medios de almacenamiento legibles registrados en el inventario de activos, este cifrada.
- Utilizar procedimientos seguros como el cifrado TLS y el túnel VPN seguro cuando se intercambien los datos sensibles al cliente y de identificación personal.

El Oficial de Cumplimiento debe:

- Gestionar cualquier transferencia de información a través del procedimiento **PR-GAL-02** Transferencia o Remisión de Datos Personales y conforme al **FO-GAL-09** Inventario de datos personales, cualquier transferencia de información que contenga Datos personales.
- Asegurar que los avisos de privacidad de las páginas web de la organización estén dispuestos en las instalaciones de la organización o cualquier otro medio (físico o digital) y se encuentren actualizados.

El Responsable de Administración de Personal y todo el personal, deben:

- Asegurar el entendimiento y firma de las cláusulas de confidencialidad establecidas en el contrato al momento del ingreso y del **DE-GAL-17** Aviso de privacidad para colaboradores (en todas las contrataciones).

El Responsable de Jurídico debe:

- Establecer con proveedores / socios comerciales, el acuerdo de no divulgación a través de un convenio de confidencialidad unilateral (NDA) o integrando cláusulas de confidencialidad en los contratos.

El Responsable de Infraestructura debe asegurar que:

- Se realiza la operación del servicio de correo electrónico por medio de protocolo seguro.
- Se cuente con configuración de reglas en firewall para las transferencias o intercambio de información.

La información reservada o confidencial no cifrada solo debe ser enviada a través del correo electrónico institucional.

4.15. CONTROL DE ACCESO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Administrador de la CMDB / Gestor de activos y configuraciones

Justificación

Para el acceso lógico a la información y otros activos asociados:

El responsable de Infraestructura debe:

- Mantener actualizados los datos de los usuarios en el directorio activo, tales como puesto, área y ubicación conforme a la información que provea el área de Recursos Humanos.
- Asignar los permisos de acuerdo los perfiles de usuarios definidos cuando sus responsabilidades lo requieran.

Los responsables de los aplicativos deben:

- Registrar al personal como usuarios en los aplicativos de acuerdo con la naturaleza de sus funciones y mantener actualizado el **FO-GTI-60** Perfiles de Usuario y el **AX-GTI-01** Relación usuarios aplicativos.

Todo el personal que se le concede acceso a equipo de cómputo, sistemas o aplicativos en la red debe contar con una cuenta de usuario única y una clave de acceso personalizada, confidencial e intransferible, que le permita su identificación única para el uso y cumplimiento de sus funciones o facultades asignadas. Si llegase a prestar su usuario y contraseña deberá asumir la responsabilidad de las transacciones que hayan sido efectuadas con su usuario.

Para el acceso físico a las instalaciones de la organización:

El personal deberá portar su Identificación de colaborador de forma visible en todo momento.

Adicionalmente, en las instalaciones corporativas:

- Utilizar su código QR para el ingreso al edificio.

En las instalaciones de Teliko

- Utilizar su huella dactilar para el ingreso al edificio (dicho sistema es proporcionado por el arrendador del edificio).

En las instalaciones de CustomSoft

- Registrar su entrada en la bitácora de vigilancia Visitantes y Proveedores:

Para visitantes y proveedores:

- El responsable de recepción deberá:
  - Resguardar una identificación oficial durante la permanencia del visitante o proveedor, y hará entrega de un gafete que deberá portar de manera visible en todo momento.
  - Registrar a visitantes y proveedores de acuerdo con lo establecido en el **PR-SGE-11** Recepción, considerando: fecha, nombre completo, propósito del acceso y activos ingresados a las instalaciones y sitios en donde permanecerá.
- Para acceder a las zonas seguras tendrán que ser acompañados por lo menos por una persona de la Organización (responsable de la agenda).

4.16. GESTIÓN DE LA IDENTIDAD

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de infraestructura

Justificación

Con el fin de administrar adecuadamente el ciclo de vida de las identidades se establecen los siguientes lineamientos:

A) Creación de la identidad.

- Realizar la asignación de nuevas identidades de acuerdo con lo establecido en **PR-GTI-13** Altas y bajas de equipo de cómputo.
- Gestionar cualquier cambio de responsabilidades que el usuario requiera actualizar en el perfil de acuerdo con el **PR-GTI-11** Gestión de incidentes y solicitudes de servicios verificando el VoBo del Líder Inmediato.
- Documentar en el **FO-GTI-60** Perfiles de Usuario o el anexo **AX-GTI-01** Relación usuarios aplicativos los diferentes perfiles de accesos a los sistemas, aplicativos y redes y mantener actualizado.

B) Autenticación.

El proceso de autenticación para los sistemas y aplicativos de la Organización deberá ser de acuerdo al apartado **5.17 Información de Autenticación.**

C) Auditoría y cumplimiento.

Realizar monitoreo de los inicios de sesión a los sistemas de acuerdo a lo establecido en el **apartado 8.16 Monitoreo de Actividades.**

D) Retiro de accesos.

- Cancelar todos los accesos del personal hacia aplicativos cuando este sea dado de baja de acuerdo con lo establecido en el **PR-GTI-13** Altas y bajas de equipo de cómputo.

4.17. INFORMACIÓN DE AUTENTICACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

La contraseña de la cuenta de usuario debe ser asignada manera individual y es intransferible, de tal forma que el usuario tiene prohibido divulgar la contraseña.

Es responsabilidad de la persona a la cual se le asignó la cuenta genérica de usuario, todas las actividades realizadas con esta cuenta.

El Gestor / Oficial de seguridad debe:

- Informar únicamente al usuario que deberá cambiar la contraseña cuando ingrese a la infraestructura tecnológica por primera vez, la contraseña inicial solo se les brindará de manera presencial al momento de la entrega de los activos. La plataforma, automáticamente solicitará realizar el cambio de contraseña.
- Definir la configuración para que el personal cree contraseñas que cumplan con los requisitos de seguridad. Para los equipos de cómputo y cuentas de correo deberán ser: compuestos de al menos 8 caracteres, que contenga al menos una mayúscula, un número o carácter especial y que estas caduquen mínimo cada 60

días a través de una política de directorio activo. Para aplicativos como CONCUR la contraseña deberá ser de al menos 8 caracteres, alfanumérico y con al menos un carácter especial, las contraseñas solo se podrán reutilizar después de 4 cambios. Para SAP S/4 Hana y Success Factors deberá ser de al menos 8 caracteres, alfanumérico, que contenga una minúscula y una mayúscula y un carácter especial.

- Resguardar las contraseñas de los sistemas, aplicativos y redes en password safe o KeePass.
- Contar con una contraseña maestra para acceder a la cuenta de administrador local en caso de emergencia, bajo resguardo del líder, entregada previamente en un sobre cerrado.
- Contar con un super usuario para acceder a la cuenta de administrador de contraseñas en caso de emergencia, bajo resguardo de la Dirección de Tecnología de la Información.

4.18. DERECHOS DE ACCESO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Incidentes y Requerimientos

Justificación

El Gestor de Incidentes y Requerimientos deberá asignar derechos de accesos y registrarlos en el **FO-GTI-60** Perfiles de usuario y el **AX-GTI-01** Relación usuarios aplicativos

El Responsable de Procesos debe considerar la revisión del control de usuarios dentro del **FO-GPO-14** Plan de auditoría interna al sistema de gestión de seguridad de la información a intervalos planificados.

Todo ajuste, cambio, bloqueo o retiro de acceso a sistemas y servicios de red de la organización debe ser gestionado a través de una solicitud registrada en la herramienta de solicitudes de servicio de acuerdo con lo establecido en el procedimiento **PR-GTI-11** Gestión de incidentes y solicitudes de servicios y el procedimiento **PR-GTI-13** Altas y bajas de equipo de cómputo.

4.19. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Relaciones con Proveedores Responsable de Jurídico

Justificación

El responsable de infraestructura debe:

- Proporcionar acceso a los servicios de red con base en especificaciones y requerimientos del área a la que el proveedor esté proporcionando servicios.
- Asegurar que en los contratos se establezcan las obligaciones aplicables a los proveedores para proteger la información de la organización y sus partes interesadas.

El Administrador del catálogo de proveedores debe:

- Validar el correcto llenado del **FO-ADQ-10** Alta Proveedor de compras o el **FO-ADQ-11** Foreign Supplier Registratión (Según aplique) en el cual se integra la aceptación de la cláusula de confidencialidad entre el proveedor y la organización.

El Responsable de Jurídico debe:

- Asegurar que se ha formalizado la relación con los proveedores a través de un contrato de prestación de servicios o productos, de acuerdo con lo establecido en la **PO-ADQ-02** Administración de proveedores.

- Resguardar convenios de confidencialidad de los proveedores.
- Dar a conocer a los proveedores el **DE-GAL-16** Aviso de privacidad.

4.20. ABORDAR LA SEGURIDAD DE LA INFORMACIÓN EN LOS ACUERDOS CON PROVEEDORES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Jurídico

Justificación

El responsable de Jurídico debe:

- Revisar y/o asegurarse que, cuando la naturaleza de los contratos celebrados con los proveedores / socios de negocios así lo permita, se establezca clausulado en materia de confidencialidad, protección de datos personales, transferencia de datos, entre otros que se consideren pertinentes.
- Dar a conocer y/o apegarse al aviso de privacidad correspondiente (cuando aplique)
- Establecer el Convenio de confidencialidad unilateral (NDA) u Orden de compra con clausulado (Según aplique) con los proveedores dentro de la cadena de valor.

El Gestor / Oficial de seguridad debe:

- Mitigar riesgos de proveedores sobre los activos de la organización conforme la valoración de riesgos de seguridad de la información en la **FO-GPO-49** Matriz de gestión de riesgos y oportunidades.

4.21. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA CADENA DE SUMINISTRO DE LAS TIC

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Jurídico

Justificación

El responsable de Jurídico debe asegurarse al iniciar y/o mantener una relación comercial con proveedores de TICs se establezca con un contrato, Aviso de Privacidad (cuando aplique) y convenio de confidencialidad o cláusula de confidencialidad.

Los riesgos y/u oportunidades relacionadas a los proveedores de TICs, deberán ser valorados de manera anual conforme el procedimiento **PR-GPO-09** Gestión de riesgos y oportunidades y la **FO-GPO-49** Matriz de gestión de riesgos y oportunidades.

4.22. GESTIÓN DE MONITOREO, REVISIÓN Y CAMBIOS A LOS SERVICIOS DE PROVEEDORES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Cambios

Justificación

El Gestor de cambios debe asegurar que todo cambio en la prestación de servicios de TI realizados por proveedores autorizados se realice como se establece en el **PR-GTI-09** Gestión de cambios.

El comprador responsable debe asegurar las adecuaciones a los contratos existentes con proveedores cuando surjan cambios de domicilio del proveedor, cambios en precios, y en caso de ser necesario se pueden realizar convenios modificatorios a los contratos para cambios que lleguen a ser críticos y necesarios en los servicios.

La revisión y evaluación en la entrega de servicio de proveedores deberá gestionarse de acuerdo con lo establecido en la **PO-ADQ-02** Administración de Proveedores.

4.23. SEGURIDAD DE LA INFORMACIÓN PARA SERVICIOS EN LA NUBE

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de Seguridad

Justificación

Para la adquisición de servicios en la nube, el Gestor / Oficial de seguridad de la Información debe:

- Revisar los informes de seguridad de la información (Informes SOC 3 de los proveedores para garantizar el cumplimiento de los requisitos de seguridad de la organización (cuando aplique);
- Identificar los riesgos asociados al tipo de servicios en la nube en el **FO-GPO-49** Matriz de Riesgos y Oportunidades, cuando se identifique alguno;
- Establecer controles de seguridad para reducir o mitigar los riesgos que no puedan ser controlados por el proveedor o por la organización.

Todo servicio en la nube debe:

- Tener una gestión de control de acceso del servicio en la nube;
- Tener soluciones de monitoreo y protección contra malware;
- Procesar y almacenar la información considerada como confidencial o restringida de la organización en lugares aprobados;
- Proporcionar soporte especifico en caso de un incidente de seguridad de la información en el entorno de servicios en la nube;
- Garantizar que se cumplen los requisitos de seguridad establecidos en este Manual en caso de que los servicios en la nube se subcontraten;
- Proporcionar soporte adecuado y disponibilidad de servicios durante un periodo de tiempo adecuado cuando la organización desee salir del servicio en la nube;
- Proporcionar la copia de seguridad requerida de los datos y la información de configuración y gestionar de forma segura las copias de seguridad, según corresponda en función de las capacidades del proveedor de servicios en la nube.

4.24. PLANIFICACIÓN, PREVISIÓN Y PREPARACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Seguridad Gestor de Incidentes

Justificación

Cuando se presente un incidente de seguridad de la información el Gestor / Oficial de Seguridad debe:

- Atender los incidentes conforme lo estipulado en el **PR-GTI-11** Gestión de incidentes y solicitudes de servicios.

- Seguir el escalamiento de acuerdo con lo establecido en el **FO-GTI-20** Matriz de Escalamiento Jerárquico y Funcional.
- Documentar las actividades realizadas por el proveedor, cuándo este participe en la solución de los incidentes y asegurar que entregue una memoria técnica.
- Mantener informado al solicitante sobre el progreso en la resolución de su incidente/solicitud.
- Identificar cuando uno o varios incidentes recurrentes estén ocasionando un problema para darle atención mediante el **PR-GTI-12** Gestión de problemas.
- Asegurar el contacto correspondiente con las autoridades competentes de acuerdo con el apartado 5.5 Contacto con Autoridades, cuando la naturaleza del incidente de seguridad así lo determina.
- Comunicar el **PR-GTI-11** Gestión de incidentes y solicitudes de servicios a toda la organización.

4.25. EVALUACIÓN Y DECISIÓN SOBRE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Detectivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Incidentes

Justificación

Para los eventos de seguridad de la información en la infraestructura interna el Gestor de incidentes debe clasificar y atender los eventos de seguridad a través de la definición establecida con en el **FO-GTI-61** Matriz de Incidentes de seguridad y decidir si es o no un incidente de seguridad.

4.26. RESPUESTA A LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de Seguridad

Justificación

Cuando se presente un incidente en la infraestructura tecnológica interna y en la entrega de soluciones y servicios el Gestor / Oficial de Seguridad debe dar atención, respuesta y seguimiento a las incidencias registradas de seguridad a través del **PR-GTI-11** Gestión de incidentes y solicitudes de servicios.

Para el caso de Teliko, cuando alguna incidencia afecte directamente a la organización o clientes de manera crítica, el Gestor de Incidentes deberá notificar al Oficial de Seguridad para la toma de decisiones que se consideren pertinentes.

4.27. APRENDER DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de incidentes

Justificación

El Gestor de incidentes y el Gestor / Oficial de seguridad deben utilizar el análisis y la resolución de incidentes para reducir la probabilidad o impacto de futuros incidentes y preservar la información que pueda servir como evidencia, con base al **PR-GTI-11** Gestión de incidentes y solicitudes de servicio.
Los conocimientos adquiridos en la resolución de incidentes internos deben ser documentados en el **FO-GTI-03** Base de Conocimiento

4.28. RECOPILACIÓN DE EVIDENCIA

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Eventos Gestor de Incidentes

Justificación

El Gestor de Eventos / Incidentes:

- Debe registrar todos los incidentes en la herramienta de gestión correspondiente y deberán ser gestionados de acuerdo con lo determinado en el **PR-GTI-11** Gestión de incidentes y solicitudes de servicios.
- Asegurar el acceso a los activos comprometidos en un incidente de seguridad de la información para evitar la propagación del virus.
- Comunicar al proveedor responsable de la recolección de evidencia el incidente y gestionar el servicio.

El proveedor de servicio de recolección de evidencia deberá apegarse a lo establecido en los siguientes lineamientos, los cuales se encuentran apegados a la legislación vigente:

Documentación de la escena del crimen electrónico: La documentación de la escena del crimen electrónico es necesaria para mantener un registro de todos los procesos de investigación forense realizados para identificar, extraer, analizar y preservar la evidencia.

- Búsqueda y Captura.
  - ❖ Buscar el consentimiento.
  - ❖ Obtención de firmas de testigos.
  - ❖ Obtención de orden de allanamiento.
  - ❖ Recopilación de información de incidentes.
- Búsqueda inicial de la escena.
- Aseguramiento y evaluación de la escena del crimen.
- Incautación de pruebas de la escena del crimen.
- Un plan de búsqueda e incautación debe contener los siguientes detalles:
  - ❖ Descripción del incidente.
  - ❖ Creación de un documento de cadena de custodia.
  - ❖ Ubicación del incidente.
  - ❖ Jurisdicción aplicable y legislación pertinente.
  - ❖ Determinar el alcance de la autoridad para registrar.
  - ❖ Detalles de los equipos a incautar.
  - ❖ Tipo de búsqueda de incautación (abierta/encubierta).
  - ❖ Aprobación de la dirección local.
  - ❖ Precauciones de salud y seguridad.
- Preservación de la evidencia.
  - ❖ Cualquier evidencia física y/o digital incautada debe ser aislada, asegurada y transportada y preservada para proteger su verdadero estado.
  - ❖ En el momento de la transferencia de pruebas, tanto el remitente como el receptor deben proporcionar información sobre la fecha y la hora de la transferencia en el registro de cadena de custodia.
  - ❖ Los procedimientos utilizados para proteger la evidencia y documentarla durante la recolección y el envío son los siguientes: Cuaderno de bitácora de proyecto, etiqueta para identificar de forma única cualquier evidencia y registro de cadena de custodia.

- Adquisición de datos.
- Los investigadores deben poder verificar la exactitud de los datos adquiridos y el proceso completo debe ser auditable y aceptable para el tribunal o autoridad correspondiente.
- Al recopilar evidencia, un investigador debe evaluar el orden de volatilidad de los datos según la máquina sospechosa y la situación:
  - ❖ Registros y caché.
  - ❖ Tablas de enrutamiento, tabla de procesos, estadísticas de Kernel y memoria.
  - ❖ Archivos temporales de sistema.
  - ❖ Disco u otro medio de almacenamiento.
  - ❖ Datos de registro y monitoreo remotos que son relevantes para el sistema en cuestión.
  - ❖ Configuración física y topología de red.
  - ❖ Medios de archivo.
- Reglas generales para la adquisición de datos:
  - ❖ No trabaje con evidencia digital original. Cree un flujo de bits/imagen lógica de una unidad/archivo sospechoso para trabajar.
  - ❖ Use medios limpios para almacenar las copias.
  - ❖ Producir dos o más copias del medio original.
  - ❖ Al crear copias de medios originales, verifique la integridad de las copias con el original.
- Análisis de datos. Esta fase incluye lo siguiente:
  - ❖ Análisis del contenido del archivo, fecha y hora de creación y modificación del archivo, usuarios asociados con la creación del archivo, acceso y modificación del archivo, y ubicación de almacenamiento físico del archivo.
  - ❖ Generación de línea de tiempo.
  - ❖ Identificación de la causa raíz del incidente.
- Análisis de caso.
  - ❖ Los investigadores pueden relacionar los datos probatorios con los detalles del caso para comprender como se produjo el incidente completo y determinar las acciones futuras como las siguientes:
  - ❖ Determinar la posibilidad de explorar otros procedimientos de investigación para recopilar evidencia adicional
  - ❖ Recopilar información adicional relacionada con el caso.
  - ❖ Considerar la relevancia de los componentes que está fuera del alcance de la investigación.
- Informes. Los siguientes son procedimientos para recopilar y organizar la documentación requerida:
  - ❖ Reúna todas las notas de las diferentes fases del proceso de investigación.
  - ❖ Identificar los hechos que se incluirán en él informa para respaldar las conclusiones.
  - ❖ Enumerar todas las pruebas para presentar el informe.
  - ❖ Enumerar las conclusiones que deben estar en el informe.
  - ❖ Organizar clasificar la información recopilada para crear un informe conciso y preciso.
- Redacción del informe de investigación:
  - ❖ Debe definir con precisión los detalles de un incidente.
  - ❖ Debe transmitir toda la información necesaria de manera concisa.
  - ❖ Debe ser técnicamente sólido y comprensible para el público objetivo.
  - ❖ Debe estar estructurado de manera lógica para que la información pueda localizarse fácilmente.
  - ❖ Debe ser capaz de resistir la inspección legal.
  - ❖ Debe adherirse a las leyes locales para ser admisible en tribunales.
- Testificar como testigo experto.

- La evidencia física deberá etiquetarse y mantenerse en la gaveta con llave designada para este fin, siguiendo el apartado Control de Acceso y Monitoreo Físico, bajo custodia del Gestor / Oficial de seguridad.
- El Gestor / Oficial de seguridad deberá mantener la evidencia relacionada con los eventos de seguridad de la información en el repositorio designado y mantenerla por un periodo máximo de 3 años.

4.29. SEGURIDAD DE LA INFORMACIÓN DURANTE LA INTERRUPCIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad Gestor de la Continuidad y Disponibilidad

Justificación

El Gestor / Oficial de seguridad y el Gestor de la Continuidad y Disponibilidad, deben establecer y utilizar el **AX-GPO-03** Plan de continuidad del negocio (BCP), así como el **AX-GPO-04** Plan de recuperación ante desastres (DRP), como un marco de referencia para clasificar todos los recursos de información, mediante el establecimiento de prioridades de recuperación que permitan que los recursos más críticos sean los primeros en ser recuperados.

La Alta Dirección debe proporcionar los recursos financieros, humanos, tecnológicos, necesarios para el desarrollo de las operaciones en casos de interrupción.

El Gestor de la continuidad y disponibilidad debe:

- Ser responsable de mantener actualizado el **AX-GPO-01** Análisis de impacto al negocio (BIA), **AX-GPO-04** Plan de recuperación ante desastres (DRP) y el **AX-GPO-03** Plan de continuidad del negocio (BCP).

4.30. DISPONIBILIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC)

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Correctivo	Disponibilidad	Implementado	Gestor / Oficial de seguridad Gestor de la Continuidad y Disponibilidad

Justificación

El Gestor / Oficial de seguridad y el Gestor de la Continuidad y Disponibilidad, deben determinar sus planes de redundancia del enlace de internet, Directorio activo, energía eléctrica y del servicio de Office 365.

Se deben realizar pruebas de continuidad y disponibilidad de los sistemas e infraestructura críticos, de acuerdo con lo establecido en:

- **AX-GPO-01** Análisis de impacto al negocio (BIA)
- **AX-GPO-03** Plan de Continuidad del negocio (BCP)
- **AX-GPO-04** Plan de recuperación ante desastres (DRP)

La Alta Dirección debe proporcionar los recursos financieros, humanos, tecnológicos, necesarios para el desarrollo de las operaciones en casos de interrupción.

4.31. REQUISITOS LEGALES, ESTATUTARIOS, REGULATORIOS Y CONTRACTUALES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Oficial de cumplimiento

Justificación

El Oficial de Cumplimiento y el Gestor / Oficial de seguridad deben:

- Identificar la legislación derogada, abrogada o adicionada a través de la consulta de diversas fuentes (Ley Federal de Trabajo, Constitución Política, Ley de Adquisiciones, Bases de Licitación, Ley Federal de protección de datos personales en posesión de particulares, los reglamentos de autorregulación vinculante, el reglamento de la ley, propiedad intelectual, propiedad industrial, etc.) así como los controles criptográficos que pudieran impactar y actualizar la **FO-GAL-07** Matriz de identificación y evaluación de requisitos legales para determinar el nivel de cumplimiento, de acuerdo con el procedimiento **PR-GAL-17** Identificación y evaluación de requisitos legales y otros, definir los medios de cumplimiento legal asociados a los requisitos operativos.

El Gestor de relaciones con el negocio debe:

- Canalizar al área jurídica los requisitos legales imputables a los contratos de prestación de servicios para monitoreo respecto de los incumplimientos que se puedan generar, así como saber el actuar en caso de una disputa con un proveedor.

El Gestor / Oficial de Seguridad, debe:

- Mantener implementado un canal seguro de a través de Redes Privadas Virtuales (VPN).
- Contar con un servicio de correo electrónico seguro y dedicado por medio del protocolo seguro.

4.32. DERECHOS DE PROPIEDAD INTELECTUAL

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Activos y Configuraciones Responsable Jurídico

Justificación

El Gestor de Activos y configuraciones debe seguir los lineamientos establecidos en las licencias en el Control de software.

El Responsable de Jurídico debe:

- Vigilar el cumplimiento de los derechos de propiedad intelectual establecidos en contratos con el Personal.
- Asegurar la inclusión de una cláusula de propiedad intelectual en aquellos contratos que por su naturaleza les sea aplicable.

Todo el personal debe apegarse a lo establecido en el apartado 8.4 “Protección de los bienes” en el **AX-GAL-03** Código de conducta y ética empresarial para efecto de proteger la propiedad intelectual, mantener su confidencialidad e integridad.

4.33. PROTECCIÓN DE REGISTROS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Procesos

Justificación

El Responsable de Procesos debe asegurar:

- Que toda la documentación de proceso considere en la sección “REGISTROS GENERADOS” la protección electrónica y física con base en su clasificación.

4.34. PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE IDENTIFICACIÓN PERSONAL

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementada	Oficial de Cumplimiento

Justificación

El Oficial de Cumplimiento en conjunto con el Comité de Integridad, deben gestionar toda solicitud de derechos ARCO de acuerdo con el procedimiento **PR-GAL-01** Reclamación de derechos ARCO, registrando cada solicitud en la **FO-GAL-10** Solicitud de derechos ARCO, así como cumplir con lo establecido en la **PO-GAL-03** Política de protección de datos personales.

Adicional la organización dispone del **DE-GAL-04** Aviso de privacidad para personal indicando el tipo de dato recabado, finalidad del tratamiento y destinatario en caso de una transferencia o remisión.

4.35. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Implementada	Responsable de Certificaciones.

Justificación

La organización se somete a revisiones independientes efectuadas por organismos de certificación por lo menos una vez al año, mismas que deben ser gestionadas por el área de Certificaciones.

Para la revisión se debe considerar el alcance del SGSI así como personas, procesos y tecnologías que interactúan bajo el contexto organizacional.

4.36. CUMPLIMIENTO CON POLÍTICAS, REGLAS Y ESTÁNDARES PARA LA SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementada	Responsable de Certificaciones.

Justificación

El Responsable de Certificaciones debe realizar auditorías internas al menos una vez al año de acuerdo con el **PR-GPO-04** Auditoría Interna y dar continuidad al seguimiento de no conformidades con base al **PR-GPO-05** Acciones correctivas y de mejora.

En cada evaluación el equipo de auditoría debe:

- Revisar el cumplimiento a la política del SGSI y a este manual.
- Procedimientos operativos de seguridad de la información.
- Clasificación de la información y protección de los registros.

4.37. PROCEDIMIENTOS OPERACIONALES DOCUMENTADOS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Procesos.

Justificación

El responsable de Procesos debe asegurar que todos los procedimientos utilizados en la organización sigan la estructura determinada por el **AX-GPO-10** Elementos para la elaboración de documentos, así como el registro en el **FO-GPO-01** Lista maestra de documentos.

Para la administración de cambios en los documentos se debe contar con la autorización del líder de área con el objetivo de evaluar el impacto hacia otros procesos de negocio.

5. CONTROLES DE PERSONAS

5.1. INVESTIGACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de reclutamiento.

Justificación

El Responsable de Reclutamiento debe:

- Notificar a todos los candidatos que sus antecedentes serán investigados como parte del **PR-GCH-01** Atracción de talento, contratación e inducción a través de un proveedor de estudios socioeconómicos y para candidatos foráneos las referencias laborales o cruzadas.
- Asegurar que durante el proceso de contratación no debe revelarse información confidencial de la organización a los candidatos.

5.2. TÉRMINOS Y CONDICIONES DEL EMPLEO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de reclutamiento y AP.

Justificación

El Responsable de Reclutamiento y Administración de Personal deben asegurar que todo el personal a contratar, firmen el **DE-GAL-05** Aviso de privacidad solicitud de empleo; el **DE-GAL-17** Aviso de privacidad para colaboradores con la organización y el **AX-GCH-04** Carta de adhesión al SIG.

5.3. CONCIENTIZACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Capacitación

Justificación

El Responsable de Capacitación debe proporcionar al personal la capacitación necesaria a través de lo establecido en el **PR-GCH-08** Capacitación, la cual debe ser relacionada con la tendencia actual en seguridad de la información cuando sea relevante para sus funciones de trabajo o con base en solicitudes de las áreas.

El Gestor / Oficial de seguridad debe asegurarse de mantener al personal actualizado en los cambios a los controles de Seguridad de la Información de acuerdo con lo establecido en el **FO-GCH-18** Programa de capacitación y asegurar la concientización de acuerdo con lo establecido en la **FO-GCH-01** Matriz de Comunicación.

5.4. PROCESO DISCIPLINARIO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de Seguridad

Justificación

El Gestor / Oficial de Seguridad debe fungir como el órgano colegiado responsable de:

- Brindar asesoría técnica a cualquier parte interesada en materia de seguridad de la información.
- Vigilar el cumplimiento, sensibilizar entre el personal y mantener vigente los lineamientos de uso de sistemas informáticos (correo electrónico, internet, SharePoint, entre otros) establecidos en este Manual
- Evaluar de manera prioritaria y oportuna cualquier posible violación o violación real a las políticas de seguridad de la información a través de implementar medidas administrativas, técnicas, físicas y/o financieras para garantizar la seguridad de la información.
- Establecer, mantener, dar a conocer entre el personal y ejecutar (cuando sea requerido) el proceso disciplinario **PR-GAL-03** Sanciones administrativas, para tomar acciones / medidas en caso de posibles actos o actos reales de violaciones a las políticas de seguridad de la información.

5.5. RESPONSABILIDADES EN LA TERMINACIÓN O CAMBIO DE EMPLEO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Personal de la organización.

Justificación

Todo personal, consultor o contratista que termine su relación con la organización debe devolver toda propiedad otorgada, incluyendo, sin limitantes, computadoras portátiles, documentación, llaves de oficina, tarjetas de crédito, o cualquier activo de información que le haya sido conferido para el desempeño de sus actividades.

5.6. ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Jurídico

Justificación

La información confidencial o restringida bajo la custodia de la organización no debe ser divulgada a terceros a menos que estos terceros firmen un acuerdo de confidencialidad aprobado por el área Jurídica. Antes de divulgarse cualquier información propia a un tercero, este debe firmar un Convenio confidencialidad o establecer un Clausulado específico de confidencialidad en el contrato de prestación del servicio (cuando aplique).

A través de estos controles, la organización se asegura del cumplimiento de los principios de consentimiento, calidad, lealtad, finalidad y proporcionalidad.

5.7. TRABAJO REMOTO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI

Justificación

El Gestor / Oficial de Seguridad debe:

- Asegurar que todo servicio de conexión externa a los servidores sea a través de VPN, permitiendo acceso remoto únicamente a usuarios que por la(s) función(es) de su cargo o por requerimientos justificados y autorizados y de acuerdo con lo establecido en el **IT-GTI-19** Instalación y manejo de cliente VPN.
- Vigilar que los puertos de configuración y diagnóstico remoto que permitan realizar mantenimiento y soporte remoto a los equipos de la red, servidores y estaciones de trabajo, sean de uso exclusivo y estén restringidos al personal responsable de la administración de la red y servidores, que deberá estar facultado para su uso, los cuales están segmentados dependiendo el área y uso.

Los usuarios finales deberán permitir que se tome el control remoto de sus equipos para resolver situaciones o atender a requerimientos que demande el acceso remoto por parte del personal de soporte, teniendo en consideración que no se deben exponer archivos con información sensible a la vista y que no deben desatender el equipo, mientras se tenga el control remoto de un equipo.

Recomendaciones de seguridad para el trabajo remoto

- Trabajar en un sitio aislado y que cuente con cerradura;
- No trabajar en lugares públicos como plazas, cafeterías, entre otros;
- Hacer uso de redes domésticas configuradas con contraseña segura en el modem, haciendo uso de WPA2;

- Hacer uso de la VPN en todo momento para las conexiones que así lo requieran;
- Únicamente se podrá laborar con los equipos provistos por la Organización.

5.8. REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Detectivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

La organización mantiene un mecanismo para informar oportunamente los acontecimientos de seguridad de la información observados o sospechosos a través del **PR-GTI-11** Gestión de incidentes y solicitudes de servicios.

Los incidentes o actividades sospechosas durante su jornada de trabajo, que atenten contra las políticas de seguridad de la información, deben registrarlo con base en lo documentado en el **PR-GTI-11** Gestión de incidentes y solicitudes de servicios.

El Gestor de Incidentes debe:

- Contar con una base de conocimientos.
- Contar con un correlacionador de eventos de seguridad para el monitoreo.

6. CONTROLES FÍSICOS

6.1. PERÍMETROS DE SEGURIDAD FÍSICA

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Servicios Generales

Justificación

El Responsable de Servicios Generales debe asegurar y gestionar los siguientes elementos:

- Perímetros de seguridad para proteger las áreas donde se conserve, resguarde o procese información. Actualmente se cuenta con:
- Personal de vigilancia intramuros;
- Sistema de video vigilancia CCTV;
- Política de control de acceso (Ver apartado 5.15);

Adicional para Teliko aplica:

Sistema de detección biométrico y CCTV para el control de acceso a las instalaciones, ambos proporcionados por el arrendador del edificio.

Adicionalmente se cuenta con el **FO-SGE-03** Bitácora de acceso para el registro de colaboradores, visitantes y proveedores.

6.2. ENTRADA FÍSICA

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Recepción

Justificación

El inmueble debe contar con la asignación de un área de abastecimiento, la cual debe estar aislada de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Actualmente se cuenta con un área de recepción en la planta baja.

El responsable de Recepción deberá considerar los siguientes lineamientos:

- En cuanto a la atención de personas externas a la organización que por motivos laborales visitan las instalaciones, el horario permitido es de 9:00 am a 18:00 pm, de lunes a viernes.
- Todos los visitantes temporales deberán proporcionar una identificación y portar en todo momento el gafete temporal proporcionado a su ingreso por el personal de recepción.

En caso de que un visitante llegue fuera de estos horarios, es responsabilidad de vigilancia informar los horarios de acceso a las instalaciones y deberá estar acompañado por al menos una persona de la organización.

6.3. ASEGURAMIENTO DE OFICINAS, HABITACIONES E INSTALACIONES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Servicios Generales

Justificación

El Responsable de Servicios Generales debe establecer una zona segura para el resguardo, protección y manejo de los activos de información.

Se debe contar con un lay out de las instalaciones, el cual muestre la distribución y los puntos de interés ante una emergencia, así mismo se debe contar con alarma sísmica, alarmas contra incendio y extintores de acuerdo con lo establecido en la **PO-GSE-01** Servicios generales.

6.4. MONITOREO DE SEGURIDAD FÍSICA

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Detectivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de Servicios Generales

Justificación

El Responsable de Servicios Generales debe asegurar:

- Delimitar un perímetro de seguridad física para proteger las áreas donde se conserve, resguarde o procese información.
- Contar con una puerta de acceso para el resguardo del SITE.
- Que todos los proveedores, usuarios o visitantes hagan el registro en el área de recepción del edificio.
- Contar con un área de recepción.
- Contar con un sistema de identificación de accesos, como biometría o detectores de contacto.
- Protección ante amenazas externas y ambientales como fuego, sismos, siniestros u otro.
- Lineamientos de prohibición de consumo de bebidas alcohólicas, así como fumar.
- Espacios específicos para el consumo de alimentos.
- Tener sistemas de video vigilancia, como circuitos cerrados de televisión, para ver y grabar el acceso a zonas sensibles dentro y fuera de las instalaciones.

6.5. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI. Responsable SASSO. Servicios Generales.

Justificación

El Gestor de Infraestructura debe:

- Asegurar la disponibilidad de los videos del CCTV del inmueble.
- Administrar el software de monitoreo.

El Responsable SASSO debe:

- Contar con un **AX-GSS-01** Plan de respuesta a emergencias.

El Responsable de Servicios Generales debe asegurar:

- Que se cuente con un **FO-SGE-06** Bitácora rutina Mensual Preventiva de Extintores.
- Que se cuente con un sistema de alarmas contra incendios y de alarma sísmica.
- La limpieza periódica del suelo, paredes, racks.
- Que se cuente con un sistema de alimentación ininterrumpida para todas las instalaciones críticas que procesan datos.
- Que se cuente reguladores de voltaje para proteger de fluctuaciones de voltaje.

6.6. TRABAJO EN ÁREAS SEGURAS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable de protección civil Gestor / Oficial de seguridad

Justificación

El Gestor / Oficial de seguridad, el Responsable de Servicios Generales y el Responsable SASSO, debe reforzar la seguridad implementando controles para el personal o terceros, conforme a lo siguiente:

- Las áreas seguras deben ser supervisadas para evitar actividades maliciosas que pongan en riesgo la información.
- Las áreas de trabajo que se encuentren desatendidas deben contar con mecanismos para resguardar la información como gavetas, escritorios con llave, etc.
- Bloquear físicamente y revisar periódicamente las áreas seguras desocupadas.
- Dar mantenimiento a las instalaciones de acuerdo con el **FO-SGE-02** Programa Anual de Mantenimiento, conforme a lo establecido en el **PR-SGE-06** Mantenimiento
- Asegurar la limpieza de las instalaciones conforme con lo establecido en el **PR-SGE-12** Servicio de limpieza de corporativo.
- Mantener las buenas prácticas y mecanismos en materia de seguridad y salud con el fin de evitar accidentes, enfermedades y contaminación al medio ambiente, conforme el **AX-GSS-09** Plan integral de seguridad, salud y medio ambiente.

6.7. PANTALLA Y ESCRITORIO LIMPIO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI Usuarios

Justificación

Se deben mantener los escritorios limpios y libres de información impresa, así como de medios de almacenamiento removibles (memorias USB, microSD, discos duros externos, CD o DVD) a menos que la información esté siendo utilizada durante la jornada laboral.

Fuera del horario normal de trabajo: no deben de dejarse directorios o documentos con información sensible en los escritorios.

Toda información comercial sensible o critica (en papel o medios de almacenamiento) deber ser resguardada en las gavetas asignadas y fuera de horario laboral estas deben permanecer cerradas con la llave correspondiente

Es responsabilidad del personal la protección de los dispositivos de punto final a su cargo, con el fin de minimizar la exposición de la información sensible conforme a lo siguiente:

- Proteger los equipos contra fallos de alimentación y alteraciones causadas por fallos en los suministros.
- Para evitar dejar papeles en las bandejas de impresoras, se debe sensibilizar a los usuarios a través de ayudas visuales.

El Gestor de TI deberá asegurarse a través de políticas en el directorio activo de: Que el sistema operativo al dejar de usarse se bloquee automáticamente después de 5 minutos y al volver a utilizarse deberá solicitar de nuevo la contraseña de ingreso al usuario.

6.8. UBICACIÓN Y PROTECCIÓN DE EQUIPO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Responsable SASSO Responsable de Servicios Generales
Justificación			

El Responsable de SASSO debe:

- Documentar, establecer e implementar el **AX-GSS-01** Plan de repuesta a emergencias, así como las acciones y lineamientos que permitan dar una respuesta eficiente por medio de recursos humanos y materiales en caso de una emergencia, la cual puede presentarse en cualquier instante durante el desarrollo de actividades.

El responsable de Servicios Generales debe:

- Contar con un **FO-SGE-06** Bitácora rutina Mensual Preventiva de Extintores
- Asegurar que se cuente con un sistema de alarmas contra incendios y de alarma sísmica.
- Limpieza periódica del suelo, paredes, racks.

6.9. SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Toda la organización. Gestor de TI.
Justificación			

Para proteger los equipos portátiles cuando son utilizados fuera de las instalaciones, el personal debe cumplir con los siguientes lineamientos:

- Trasladar el equipo físico bajo su responsabilidad y de acuerdo con su asignación;
- Ser transportadas discretamente;
- Evitar utilizar el equipo de cómputo (Laptop) en lugares públicos;
- Durante viajes, no deben ser tratados como equipaje;
- Se debe registrar la salida de los activos en el **FO-SGE-34** Salida de Activos a excepción de los equipos de cómputo, los cuales se registran en el **FO-SGE-31** Bitácora de Vigilancia
- En caso de siniestro, pérdida o robo, el responsable del equipo debe notificar inmediatamente al líder inmediato y al Gestor / Oficial de seguridad para efecto de seguir los lineamientos y procedimientos con respecto a este incidente.

El Gestor de TI debe asegurar que el equipo cuente con:

- Bloqueo de protector de pantalla con un tiempo de espera configurado. (300 s)
- Contraseñas de inicio de sesión.

6.10. MEDIOS DE ALMACENAMIENTO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI Usuarios

Justificación

En la organización solo están permitidos los dispositivos de almacenamiento externo suministrados por la organización, quedando prohibido el uso de dispositivos personales dentro de las instalaciones o en equipos de trabajo.

Todo medio debe ser almacenado en un entorno seguro haciendo uso de almacenamiento de discos duros, servidores y/o gavetas bajo llave asignadas al personal.

Todo dispositivo de almacenamiento (Disco Duro, Memoria USB, Disco Externo, etc.), así como la información que en él se resguarda, es propiedad de la organización.

Para la eliminación segura de equipos de cómputo que sean destinado a destrucción final o que sean de posiciones críticas el equipo de soporte deberá hacerlo conforme: **IT-GTI-35** Borrado seguro.

Para la eliminación de activos deberá contarse con un certificado, acta o evidencia fotográfica o de video que asegure el correcto borrado o eliminación de la información.

6.11. SERVICIOS PÚBLICOS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Detectivo	Integridad Disponibilidad	Implementado	Responsable de Servicios Generales Responsable SASSO

Justificación

El Responsable de Servicios Generales, debe asegurar que el inmueble cumpla con:

- Las especificaciones del fabricante para los dispositivos electrónicos de la organización.
- Una fuente UPS que funcione como respaldo de 20 kW.
- Una planta de emergencia que suministre energía eléctrica alterna.

El Responsable SASSO debe:
Documentar, establecer e implementar el **AX-GSS-01** Plan de repuesta a emergencias, así como las acciones y lineamientos que permitan dar una respuesta eficiente por medio de recursos humanos y materiales en caso de una emergencia, la cual puede presentarse en cualquier instante durante el desarrollo de actividades.

6.12. SEGURIDAD DEL CABLEADO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Disponibilidad	Implementado	Responsable de Servicios Generales

Justificación

El Responsable de Servicios Generales debe asegurar:

- Realizar un mantenimiento de cableado eléctrico y de telecomunicaciones cuando se solicité por parte de la organización.
- Proteger los cables de las líneas y redes de telecomunicaciones de acceso no autorizado y daños.
- Separar los cables de alimentación de los cables de comunicaciones para evitar todo tipo de interferencia.
- Etiquetar los cables en cada extremo para permitir la identificación física y la inspección del cable.

El responsable de mantenimiento debe ejecutar los servicios solicitados y/o programados en el **FO-SGE-02** Programa anual de mantenimiento conforme al **PR-SGE-01** Mantenimiento.

6.13. MANTENIMIENTO DEL EQUIPO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Infraestructura Responsable de Mantenimiento.

Justificación

El Responsable de infraestructura debe gestionar el mantenimiento preventivo y correctivo de los equipos de acuerdo con los intervalos recomendados por el fabricante, especificaciones y planificación interna considerando que se realicen en el mes de diciembre dada la baja en las actividades de la organización y registrarlos en el **FO-GTI-52** Memoria técnica.

El mantenimiento debe considerar controles de protección del equipo ante campos electromagnéticos, altas temperaturas, humedad, fluctuaciones de potencia, entre otros.

Cuando el mantenimiento sea realizado por parte de un proveedor el Gestor / Oficial de seguridad debe asegurar la protección de los datos integrados en el equipo.

El responsable de mantenimiento debe elaborar el **FO-SGE-02** Programa anual de mantenimiento el último trimestre del año inmediato anterior e incluir los servicios de mantenimiento a la infraestructura que serán ejecutados por personal de la organización y los que requieran contratar a un proveedor.

6.14. DISPOSICIÓN O REUTILIZACIÓN SEGURA DEL EQUIPO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI

Justificación

Para reutilizar o eliminar los equipos el responsable de Soporte debe considerar lo siguiente:

- Todos los equipos para reasignar deben ser formateados de manera segura y verificar que ya no cuenten con información confidencial o exclusiva.
- Cuando existan cambios de área, se deberán respaldar los equipos y medios de almacenamiento en la nube, previo al formateo y re asignación y el respaldo deberá entregarse al líder del colaborador que sufrirá el cambio.
- Todos los componentes del equipo que contengan medios de almacenamiento, por ejemplo, discos duros fijos, deben revisarse para asegurar que cualquier información confidencial o exclusiva y licencia de software se ha eliminado antes del retiro.

Los equipos estropeados que contengan información confidencial o exclusiva pueden requerir un análisis de riesgos para determinar si los componentes son destruidos, reparados o retirados.

7. CONTROLES TECNOLÓGICOS

7.1. DISPOSITIVOS DE PUNTO FINAL DE USUARIO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de activos

Justificación

El gestor de activos debe asegurar que todo dispositivo:

- Robado o extraviado sea gestionado de acuerdo con el **PR-GTI-13** Altas y bajas de equipo de cómputo.
- Tenga mecanismos especiales de bloqueo como contraseñas, pines, patrones o huella digital.
- Únicamente cuente con los accesos a la información de acuerdo con los estipulado en el apartado 5.15 Control de accesos
- Se encuentre registrado en el inventario de activos de acuerdo con el apartado 5.9 Inventario de activos de TI y otros activos asociados

El usuario es responsable de:

- Cerrar la sesión activa de los equipos cuando no se encuentren realizando actividades
- Seguir los lineamientos establecidos en el apartado 5.10 Uso aceptable de la información y otros activos asociados y en el 6.7 Trabajo a distancia.

En la organización se prohíbe el uso de dispositivos personales para la ejecución de sus funciones.

Para reutilizar los equipos el Gestor de TI debe considerar lo establecido en el control 7.14 Disposición o reutilización segura del equipo.

7.2. DERECHOS DE ACCESO PRIVILEGIADO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI

Justificación

El Director de TI es responsable de la asignación de los derechos de acceso privilegiado como: de administrador, súper usuario, que serán gestionados y monitoreados de acuerdo con los permisos establecidos en el **FO-GTI-60** Perfiles de Usuarios y en el **FO-GTI-43** Matriz de asignación de roles.

7.3. RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI

Justificación

Todo acceso a servicios de red y aplicaciones de la organización está sujeto al perfil de usuario descrito en el **FO-GTI-60** Perfiles de Usuarios y en el **FO-GTI-43** Matriz de asignación de roles.

7.4. ACCESO AL CÓDIGO FUENTE DEL PROGRAMA

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI

Justificación

El Gestor de TI debe seguir los lineamientos aplicables para el control de aplicaciones y código fuente como:

- Bloquear o restringir el acceso a las librerías dentro de los sistemas operativos de acuerdo con el apartado 8.2 Derechos de acceso privilegiados.
- Resguardar las líneas de código y sus respaldos.
- Autorizaciones ante cualquier cambio o modificación apegándose a lo establecido en el **PR-GTI-09** Gestión de cambios.

7.5. AUTENTICACIÓN SEGURA

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de Seguridad

Justificación

Para asegurar que los inicios de sesión de los usuarios a los sistemas y aplicaciones son seguros, el Gestor / Oficial de Seguridad debe restringir y controlar los accesos conforme lo siguiente:

- Identificar y verificar la identidad del personal a través de su usuario y contraseña.
- Validar la información de la conexión al completarse la totalidad de los datos de entrada.
- Después de tres intentos consecutivos fallidos para introducir la contraseña el identificador de usuario (nombre de usuario) debe ser bloqueado (donde sea posible), previniendo la adivinación de la contraseña.

- Brindar protección contra el acceso no autorizado de usuarios a software del sistema operativo.
- El sistema operativo al dejar de usarse se debe bloquear automáticamente después de 300 segundos y al volver a utilizarse deberá solicitar de nuevo la contraseña de ingreso al usuario.
- Generar los registros de auditoría que contengan excepciones y eventos relativos a la seguridad. Estos deben mantenerse durante un periodo de tiempo definido para poder acceder a futuras investigaciones o monitoreo de control de accesos.
- Revisar periódicamente el resultado de las actividades de monitoreo con base a la criticidad de los procesos y aplicaciones y al valor o criticidad de la información involucrada.
- Tener un método de sincronización de relojes para garantizar la exactitud de los registros de auditoría de acuerdo con los establecido en el apartado 8.17 Sincronización de relojes.
- Todo acceso a servicios de red, aplicaciones y sistemas de información debe ser a través de usuarios y contraseñas.

7.6. GESTIÓN DE CAPACIDAD

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Detectivo	Integridad Disponibilidad	Implementado	Gestor de la Capacidad y la Demanda.
Justificación			
El gestor de la capacidad y la demanda debe monitorear los recursos y hacer proyecciones de los requisitos futuros de capacidad para garantizar el desempeño requerido de los sistemas de acuerdo con el **PR-GTI-05** Gestión de la demanda y capacidad.			

7.7. PROTECCIÓN CONTRA MALWARE

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Detectivo Correctivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI
Justificación			
Toda persona que perciba la existencia de un virus debe apagar inmediatamente el computador correspondiente, desconectarlo de todas las redes, llamar al Gestor de incidentes y al Gestor / Oficial de seguridad y apegarse a lo establecido en el procedimiento **PR-GTI-11** Gestión de incidentes y solicitudes de servicios. El Personal no debe intentar eliminar los virus de sus equipos, a menos que lo hagan mientras estén en comunicación con el Gestor de TI, Gestor de incidentes u Gestor / Oficial de seguridad. El Gestor de TI debe: • Utilizar por lo menos un paquete de software para rastreo de virus en los archivos recibidos, archivos adjuntos de correo electrónico, descargas y páginas web para detectar malware. • Asegurar que todos los equipos de escritorio, móviles (laptops) y servidores utilizados en la red de la Institución, tengan instalado software de protección y mantener el cliente actualizado. • Implementar controles en firewall que restrinjan el acceso a sitios web catalogados como maliciosos o sospechosos de acuerdo con lo establecido en el apartado 8.23 Filtrado Web.			

7.8. GESTIÓN DE VULNERABILIDADES TÉCNICAS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

El Gestor / Oficial de seguridad debe:

- Considerar la realización de Análisis de Vulnerabilidades, analizando y evaluando el alcance de estas; con una periodicidad anual.
- Revisar la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- Atender las recomendaciones de remediación de vulnerabilidades de nivel crítico que se tenga conocimiento que están siendo explotadas en el ciberespacio y aquellas de día cero.
- Validar a través de un segundo análisis de vulnerabilidades que las remediaciones fueren efectivas.

7.9. GESTIÓN DE LA CONFIGURACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de la CMDB

Justificación

El Gestor de la CMDB debe:

- Establecer plantillas de configuraciones de dispositivos de red, de virtualización, así como plantillas de servidores de equipos virtuales y equipo de cómputo de acuerdo con el apartado 8.19 Instalación de software en sistemas operativos.
- Cargar las plantillas de configuraciones en la carpeta definida, el acceso se deberá segregar de acuerdo con los roles establecidos.
- Respaldar las plantillas de configuración periódicamente.
- Asegurar que los usuarios mantengan actualizadas las plantillas de acuerdo con nuevas versiones software o parches de seguridad.

Los cambios en las configuraciones deben ser gestionados a través del **PR-GTI-09** Gestión de cambios.

7.10. ELIMINACIÓN DE INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad	Implementado	Gestor de Solicitudes

Justificación

La eliminación de la información confidencial o restringida, cuando ya no sea necesaria deberá ser de acuerdo con lo establecido en el **IT-GTI-35** Borrado seguro.

Para la eliminación de soportes con externos deberá contarse con un certificado, acta o evidencia fotográfica o de video que asegure el correcto borrado o eliminación de la información.

7.11. ENMASCARAMIENTO DE DATOS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad	Implementado	El personal

Justificación

La información restringida debe ser enmascarada cuando surja la necesidad de compartirla a las partes interesadas tomando en cuenta cualquier requisito legal o reglamentario.

Para la información de carácter personal y considerada sensible se debe decidir sobre su enmascaramiento, en adición a lo estipulado en el apartado 5.34 Privacidad y protección de información de identificación personal.

La técnica de enmascaramiento deberá ejecutarse con el software de cifrado adoptado por la organización previamente instalado de acuerdo con el 8.19 Instalación de software en sistemas operativos.

El envío de la información y gestión de llaves de cifrado deberá ser de acuerdo con el **IT-GTI-38** Uso de software de cifrado.

7.12. PREVENCIÓN DE FUGA DE DATOS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad	En progreso	Responsable de Procesos. Gestor de Configuraciones. Gestor / Oficial de seguridad

Justificación

El Responsable de Procesos debe:

- Asegurar la clasificación de la información de acuerdo con la establecido en el apartado 5.12 Clasificación de la Información.

El Gestor de Configuraciones debe:

- Configurar los sistemas para evitar el movimiento, copia o eliminación de las carpetas en las que se encuentre la información de acuerdo con el apartado 5.15 Control de accesos.

El Gestor / Oficial de seguridad debe:

- Monitorear y supervisar la implementación de las políticas en la herramienta de prevención de fuga de datos de la organización, las cuales deben incluir:
  - ❖ Monitorear información del catálogo de palabras establecido en el DLP.
  - ❖ Identificar y notificar cuando esta información sea cargada un canal de transferencia de información (Por ejemplo, USB, correo electrónico, entre otros).
  - ❖ Bloquear la actividad maliciosa.

Toda transferencia de información que contenga datos personales se debe de gestionar conforme el **PR-GAL-02** Transferencia o remisión de datos personales y a lo establecido en el control 5.14 Transferencia de información.

7.13. RESPALDOS DE LA INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Correctivo	Integridad Disponibilidad	Implementado	Gestor de TI

Justificación

Se deben realizar respaldos de equipos virtuales, configuraciones de los activos que forman parte de la operación interna y externa, así como realizar pruebas periódicas de la integridad de estos.

En todo caso, es responsabilidad del Gestor de Telecomunicaciones, realizar los respaldos de los servidores u otros equipos de comunicaciones, en caso de que se presente una falla, con una recuperación de información, para lo cual debe:

- Contar con un programa donde se indique la frecuencia en que se realizará el respaldo de cada tipo de información registrando en el **FO-GTI-44** Bitácora de respaldos.
- Validar a intervalos planificados la ejecución de los respaldos y si dicho respaldo fue exitoso, descrito en el **FO-GTI-44** Bitácora de respaldos.
- La información alojada en el sitio Microsoft office 365 es respaldada y protegida por el proveedor de acuerdo con lo establecido en el apartado "Descripción del servicio" (https://learn.microsoft.com/es-es/office365/servicedescriptions/office-365-service-descriptions-technet-library)
- La información alojada en el sitio Microsoft Exchange Online es respaldada y protegida por el proveedor de acuerdo con lo establecido en el apartado "Descripción del servicio". (https://learn.microsoft.com/es-es/office365/servicedescriptions/exchange-online-service-description/exchange-online-service-description)
- El DA deberá contar con un respaldo espejo en la nube (azure), desde el cual podrá continuar la operación.
- El ERP se deberá respaldar (incremental) diariamente a las 11 pm y 2 am dependiendo el servidor y resguardar el respaldo en la máquina virtual de AWS con 7 días de antigüedad.
- Deberán realizarse pruebas de integridad del respaldo semestral.

7.14. REDUNDANCIA DE LAS INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Disponibilidad	Implementado	El Gestor de la Continuidad y Disponibilidad

Justificación

El Gestor de la Continuidad y Disponibilidad debe:

- Determinar los planes de redundancia a través del **AX-GPO-04** Plan de recuperación ante desastres (DRP);
- Ejecutar pruebas con base al **AX-GPO-11** Plan de pruebas de continuidad**,** para validar la efectividad de los planes de redundancia;
- Contar con una red secundaria;
- Contar con un Directorio Activo para redundancia;
- Contar con fuentes de alimentación redundantes;
- Contar con un sitio alterno (Descrito en el **AX-GPO-11** Plan de pruebas de continuidad);

El servicio en la nube de correo y almacenamiento con el que cuenta la organización, se replica en un data center en espejo en EE.UU.

7.15. REGISTRO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Detectivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI

Justificación

El Gestor de TI debe:

- Asegurar que todos los sistemas de computación y aplicaciones de producción monitoreen como mínimo, actividades de sesiones de usuarios incluyendo su identificador de usuario, fecha y hora de inicio y cierre de la sesión, incluyendo aquellos no exitosos.
- Llevar uno o más registros que rastreen las actividades importantes de seguridad de un usuario específico por un período de tiempo razonable.
- Registrar la identidad de cada usuario que acceda a la información privada contenida en los sistemas informáticos.

7.16. MONITOREO DE ACTIVIDADES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Disponibilidad	Implementado	Gestor de TI

Justificación

El Gestor de TI debe:

- Monitorear las Endpoints para detectar comportamientos anómalos de seguridad, a través del DLP.
- Establecer un sistema de alertamiento de eventos de seguridad de acuerdo con la severidad del comportamiento anómalo.
- Se monitorea mediante una herramienta, el alcance al sistema de administración Microsoft 365.

Todo evento anómalo detectado deberá ser gestionado a través del **PR-GTI-11** Gestión de incidentes y solicitudes de servicios.

Las redes son monitoreadas de acuerdo con la configuración establecida.

7.17. SINCRONIZACIÓN DEL RELOJ

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Detectivo	Integridad	Implementado	Gestor de TI

Justificación

Todos los equipos conectados a la red interna deben mantener la hora actual reflejada en sus relojes internos y sincronizadas con el reloj.

Los relojes de todos los sistemas de procesamiento de información relevantes dentro de la organización deben sincronizarse con una única fuente de tiempo de referencia o manteniendo el mismo huso horario oficial correspondiente al UTC (horario GMT) de Ciudad de México (CDMX) para garantizar el correcto registro de eventos de manera general pudiendo se utiliza un protocolo de Internet para sincronizar los relojes de los sistemas informáticos (NTP). **[ntp.crya.unam.mx]** y **[mx.pool.ntp.org].**

7.18. USO DE PRIVILEGIOS DE LOS PROGRAMAS DE UTILIDADES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI

Justificación

El responsable de infraestructura debe:

- Implementar controles de usuarios (lectura (L), escritura (E) y ejecución (EX) (en los casos que aplique) con base a lo autorizado por el líder del área o el Gestor / Oficial de seguridad.
- Garantizar que las salidas de los sistemas de aplicación que administran información confidencial o exclusiva contengan solo la información que resulte pertinente para el uso de la salida y la misma deberá ser enviada a las terminales y ubicaciones autorizadas.
- Definir y documentar los niveles de autorización para utilerías internas, conforme al tipo de usuario documentado en el **FO-GTI-60** Perfiles de Usuario

Aquellos sistemas que sean críticos o que contengan información confidencial o exclusiva requieren un trato especial para evitar pérdidas potenciales por lo que el Gestor de la Continuidad y Disponibilidad debe considerar lo siguiente:

- Identificar y acordar con el supervisor de las aplicaciones cuando ésta ha de ejecutarse en un ambiente compartido notificando los sistemas de aplicación con los cuales ésta compartirá recursos.
- Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.

7.19. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERACIONALES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI

Justificación

El equipo de soporte debe asegurar que todos los equipos cuenten con un paquete de software conforme a lo siguiente de manera enunciativa más no limitativa:

- Microsoft Windows Pro
- Microsoft Office Desktop
- Adobe Acrobat Reader
- Cytomic
- 7 Zip
- Google Chrome
- Agente kyocera print
- Global Protect
- Password Safe
- Cliente TEAMS
- Google Chrome
- Agente kyocera print
- Sensor DLP
- Sensor EDR (aplica solo para Teliko)

- Agente correlación(sensor) (aplica solo para Teliko)
- Forticlient (aplica solo para Teliko)
- Software de cifrado (aplica solo para Teliko)

Cuando se requiera un software adicional, deberá gestionarse conforme a **PR-GTI-11** Gestión de incidentes y solicitudes de servicios y actualizarse el **FO-GTI-41** Carta Responsiva de equipo de cómputo y otros activos asociados.

7.20. SEGURIDAD DE LAS REDES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Detectivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

El Gestor / Oficial de seguridad debe asegurar lo siguiente:

- Monitorear todas las computadoras de la organización conectadas a las redes para detectar virus, mediante el uso de un software de antivirus o un EDR (Endpoint Detection and Response).
- Monitorear el tráfico en Internet utilizado por el personal y las transmisiones enviadas o recibidas.
- La configuración de reglas en firewall.
- La segmentación de la red VLANs.
- Contar con reglas de configuración en switches.

7.21. SEGURIDAD EN LOS SERVICIOS DE RED

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de Seguridad

Justificación

El Gestor / Oficial de Seguridad debe asegurar:

- Monitorear los servicios de red a través de las políticas de configuración en firewall;
- Definir los medios para acceder a algunos aplicativos (por ejemplo, el uso de una red privada virtual (VPN) o una red inalámbrica);
- Gestionar el acceso a la red a través de una red de invitados para proveedores y visitantes;
- El control de acceso a los diferentes sistemas es de acuerdo con lo establecido en el control 5.15 Control de accesos;
- Los puertos no utilizados de los equipos de red deben permanecer deshabilitados;
- El control de comunicaciones entre VLANS debe hacerse a través de firewall;
- Las conexiones hacia la red interna de la organización, desde fuera de las instalaciones deben hacerse a través de una VPN;
- En cuanto un colaborador genere baja se deberá gestionar el cambio de contraseñas al DA y a los aplicativos;
- Los servidores de la organización publicados hacia internet deben estar protegidos por un firewall.

Está prohibido conectar equipos de red no autorizados (Hubs, switches, routers, etc) en los nodos asignados para endpoints.

7.22. SEGREGACIÓN EN REDES

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

El Gestor / Oficial de seguridad debe:

- Asegurar el control y segregación de los accesos a los servicios de red a través de las políticas aplicables en el firewall, conforme a las áreas de trabajo y servicios proporcionados.

7.23. FILTRADO WEB

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

El Gestor / Oficial de seguridad debe implementar controles en firewall que permitan bloquear el acceso a los siguientes tipos de sitios web:

a) Tienen función de carga de información a menos que este permitido y documentado por razones de negocio.
b) Maliciosos que sean conocidos o sospechosos.
c) Cualquier sitio que comparta contenido ilegal.

Cualquier solicitud de desbloqueo a algún sitio web deberá ser solicitado de acuerdo con lo establecido en **PR-GTI-11** Gestión incidentes y solicitudes de servicios previa autorización del líder inmediato y documentar el riesgo en el **FO-GPO-49** Matriz de riesgos y Oportunidades

Se debe controlar las comunicaciones con redes externas y destinos autorizados a través de firewall de acuerdo con el control 8.7 Protección contra malware.

Todo acceso a servicios de red y aplicaciones de la organización está sujeto al perfil de usuario, así como todo el personal debe hacer uso aceptable de la información y otros activos asociados conforme al control 5.10 Uso aceptable de la información y otros activos asociados.

7.24. USO DE CRIPTOGRAFÍA

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de Seguridad

Justificación

El Gestor / Oficial de Seguridad debe asegurar:

- La evaluación de riesgos asociados a la información clasificada como confidencial y reservada, registrarlos en la **FO-GPO-49** Matriz de gestión de riesgos y oportunidades e implementar controles criptográficos que disminuyan riesgos asociados cuando aplique.
- Que la transferencia de información en redes no protegidas sea mediante la autenticación para una comunicación segura a través de Internet entre múltiples redes y endpoints, usando tecnologías como IPsec y de capa de sockets seguros (SSL) o red privada virtual (VPN) con algoritmos de cifrado como advanced Encryption Estándar (AES).

- Para el servicio de correo electrónico garantizar la seguridad a los usuarios a través de una conexión web (HTTPS) segura o transferencia segura de datos (Canal cifrado) para el tráfico de información sensible.
- Para el establecimiento de VPNs site to site el pre-shared key debe ser compartido por un medio diferente al medio por el cual se comparten las configuraciones de la VPN.
- Utilizar programa de cifrado de información de acuerdo con los requisitos legales, contractuales y conforme a los requisitos de las partes interesadas y de acuerdo con los establecido en:
  - **IT-GTI-37** Instalación y configuración de software de cifrado
  - **IT-GTI-38** Uso de software de cifrado
- Las claves criptográficas creadas para los diferentes servicios en los casos que apliquen deben ser resguardadas y almacenadas de manera segura.
- Se debe contar con un repositorio de llaves públicas.
- Cuando un usuario cause baja se debe mantener su llave publica en resguardo al menos 3 meses
- No deben revelarse a consultores, contratistas o terceros las claves de cifrado a reserva de una aprobación formal por el Gestor de TI o el Gestor / Oficial de seguridad.

7.25. CICLO DE VIDA DE DESARROLLO SEGURO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Relación con Proveedores Gestor / Oficial de seguridad

Justificación

La organización actualmente no desarrolla software. En caso de que se contraten servicios de desarrollo, el Gestor / Oficial de seguridad, así como cuando la organización integre en los servicios el desarrollo de software, deben asegurar que:

- El desarrollo de software deberá cumplir con las practicas recomendadas establecidas por NIST (National Institute of Standards and Technology) en su publicación: Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities;
  - Preparar a la Organización
  - Proteger el Software
  - Producir Software Seguro
  - Respuesta a Vulnerabilidades
- Contar y resguardar un Convenio Confidencialidad Unilateral (NDA).
- Revisar y proteger los logs en los sistemas utilizados.
- Implementar controles para la restricción de instalación de software en la infraestructura utilizada para la prestación del servicio.
- Segregar las redes.
- Implementar controles para asegurar que el entorno de desarrollo de software es seguro.
- Implementar controles para el aseguramiento de los datos de prueba.

7.26. APLICACIÓN DE REQUISITOS DE SEGURIDAD

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de TI Gestor / Oficial de seguridad

Justificación

El Gestor de TI y el Gestor / Oficial de seguridad deben:

- Asegurar el análisis de vulnerabilidades y/o ejecución de pruebas de Hackeo Ético de la infraestructura expuesta a internet.
- Proteger los servicios de aplicación que pasan a través de redes públicas contra la actividad fraudulenta, la disputa de contratos y modificación no autorizada.
- Asegurar la integridad y confidencialidad a través de VPN y firewall.

Ver 5.8 Análisis y especificaciones de requisitos de seguridad de la información.

En la organización no se ejecutan funciones de desarrollo, sin embargo, cuando exista la necesidad se debe considerar por lo menos los siguientes lineamientos:

- Separar ambientes de desarrollo, pruebas y producción.
- Integrar herramientas para la detección de malware en la infraestructura.
- Contar y resguardar con un Convenio confidencialidad unilateral (NDA).
- Revisar y proteger los logs en los sistemas utilizados.
- Implementar controles para la restricción de instalación de software en la infraestructura utilizada para la prestación del servicio.
- Segregar de las redes.
- Implementar controles para asegurar que el entorno de desarrollo de software es seguro.
- Definir en el FO-GTI-60 Perfiles de usuario, los permisos asignados a cada responsable que participe en el
- desarrollo
- Llevar un control de versiones del desarrollo
- Generar respaldos, dependiendo en donde se aloje el ambiente.

7.27. PRINCIPIOS DE ARQUITECTURA E INGENIERÍA EN SISTEMAS SEGUROS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	-

Justificación

En la organización no se ejecutan funciones de desarrollo por lo tanto no se tiene acceso al código fuente de las aplicaciones, sin embargo, cuando exista la necesidad se debe considerar por lo menos los siguientes lineamientos:

- Todos los accesos que se hagan a los sistemas deben ser validados.
- Debe evitarse generar código que resulte ser innecesario.
- La información almacenada en dispositivos móviles debe ser la mínima.
- Todo cambio debe ser documentado.
- El código no debe de contar con rutinas de prueba, comentarios o cualquier mecanismo que pueda facilitar un acceso indebido.

- Implementar mecanismos de prevención de fuga de datos.
- Revisar el diseño del desarrollo para ayudar a identificar las vulnerabilidades de la información para garantizar que se especifiquen los controles de seguridad y cumplir los requisitos.
- Emplear un enfoque de “nunca confiar y siempre verificar” para el acceso a los sistemas de información.

Los principios de ingeniería de seguridad deben aplicarse a través de los contratos y otros acuerdos vinculantes con proveedores de servicio.

Se deben revisar los requisitos de seguridad descritos en el **AX-GTI-01** Listado de requisitos de seguridad, periódicamente para garantizar que se mantengan activos contra cualquier amenaza potencial, así como a los avances tecnológicos.

7.28. CODIFICACIÓN SEGURA

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	-

Justificación

En la organización no se ejecutan funciones de desarrollo por lo tanto no se tiene acceso al código fuente de las aplicaciones, sin embargo, cuando exista la necesidad se deben considerar los siguientes principios de codificación en tres etapas:

Planificación y antes de la codificación:

- Definir para cada tipo de sistema los lineamientos aplicables para el control de aplicaciones y código fuente, como bloquear o restringir el acceso a las librerías dentro de los sistemas operativos.
- Definir técnicas de codificación segura como el desarrollo basado en pruebas.

Durante la codificación:

- Prohibir el uso de técnicas de diseño inseguras, por ejemplo, el uso de contraseñas codificadas, ejemplos de código no aprobado y servicios web no autenticados.

Revisión y mantenimiento:

- Realizar un análisis de los errores de programación más comunes y documentar que estos sean mitigados.

7.29. PRUEBAS DE SEGURIDAD PARA EL DESARROLLO Y ACEPTACIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad Gestor de Cambios

Justificación

En la organización no se ejecutan funciones de desarrollo por lo tanto no se tiene acceso al código fuente de las aplicaciones, sin embargo, cuando exista la necesidad el Gestor / Oficial de seguridad debe considerar por lo menos los siguientes lineamientos:

- Todo nuevo sistema implementado en la organización sea sujeto a pruebas de seguridad, funcionalidad, capacidad, requisitos de seguridad, como autenticaciones, comunicación con otros componentes, procesamiento y uso de protocolos.
- Toda prueba de software diseñada para manejar información privada debe llevarse a cabo con información de prueba.

El Gestor de cambios debe asegurar que todo nuevo sistema implementado en la organización sea sujeto a pruebas de aceptación de acuerdo con el **PR-GTI-09** Gestión de cambios y el **PR-GTI-10** Gestión de liberaciones y entregas.

7.30. DESARROLLO DE SUBCONTRATACIÓN (OUTSOURCING)

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo Detectivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad

Justificación

El Gestor / Oficial de seguridad debe realizar un monitoreo periódico para supervisar las actividades realizadas por el tercero en cuanto al desarrollo de los sistemas.
Para ello debe considerar lo siguiente:

- Contar con acuerdos de licenciamiento y de derechos del autor del código para ratificar que el sistema y código es propiedad de la organización, así como se tendrá todo el soporte y mantenimiento (actualizaciones, cambios, mejoras) correspondiente por parte del tercero.
- Definir los requerimientos contractuales para las prácticas de diseño seguro, codificación y pruebas que deberá cumplir el tercero.
- Solicitar que se documenten las pruebas de aceptación, calidad y funcionamiento del sistema.
- Solicitar que sean ejecutadas pruebas regulares que validen que el nuevo sistema no cuenta con contenido malicioso (intencional o no intencional) antes de su liberación.
- Solicitar al tercero que sean documentadas todas las fases de desarrollo de sistema indicando el detalle necesario del nuevo sistema.

7.31. SEPARACIÓN DE ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor / Oficial de seguridad Gestor de Cambios

Justificación

El Gestor de Cambios debe:

- Revisar y probar en conjunto con el usuario funcional todas las aplicaciones del negocio cuando se cambien las plataformas operativas y garantizar que no hay un impacto adverso, se debe tomar en cuenta lo determinado en el **PR-GTI-10** Gestión de liberaciones y entregas.
- Establecer, documentar, mantener y aplicar principios de ingeniería para sistemas seguros.
- Proteger apropiadamente los entornos de desarrollo seguro.
- Usar base de datos dummies para realizar pruebas.

El Gestor / Oficial de seguridad debe verificar que todo proveedor de desarrollo cumpla con:

- La separación de ambientes de desarrollo.
- Control de acceso al entorno de desarrollo.
- El control de cambios.
- Asegurar, que la información involucrada en servicios de aplicaciones, que pasa por redes públicas esté protegida de actividades fraudulentas, disputas contractuales y exposición no autorizada y modificación.
- Cuando se restrinja algún servicio, sistema o aplicación, debe notificar al personal por medio de un comunicado para que tomen las medidas necesarias.

7.32. GESTIÓN DEL CAMBIO

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Cambios

Justificación

El Especialista Técnico debe:

- Apegarse a lo mencionado en el **PR-GTI-09** Gestión de cambios y el **PR-GTI-10** Gestión de liberaciones y entregas, para garantizar que el cambio está autorizado por el CAB.
- Asegurar la realización de las pruebas (cuando sea posible) para verificar que los cambios son exitosos de acuerdo con el **PR-GTI-09** Gestión de cambios.
- Asegurar que los riesgos asociados al cambio están identificados por el CAB o por el Gestor / Oficial de seguridad.
- Comunicar los cambios a las partes interesadas.

El Gestor de cambios debe asegurar que todos los cambios a plataformas e infraestructura sean controlados por medio del **PR-GTI-09** Gestión de cambios considerando:

- Evitar cambios en software empaquetado, en caso de requerirse deberá solicitarse autorización al proveedor.
- Conservar versiones anteriores a la modificación como mecanismo de contingencia.
- Contar con personal autorizado y capacitado para realizar los cambios.

7.33. INFORMACIÓN DE PRUEBAS

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad	Implementado	Gestor / Oficial de seguridad

Justificación

El Gestor / Oficial de seguridad debe asegurar que toda:

- Prueba realizada en instalaciones o con infraestructura del proveedor o cliente, debe hacerse con uso de base de Datos Dummies, Bases de Datos ficticias o Base de Datos desasociadas.
- Información utilizada o generada con las pruebas debe ser eliminada antes de comenzar la operación del sistema o herramienta.

7.34. PROTECCIÓN DE SISTEMAS DE INFORMACIÓN DURANTE AUDITORÍA

Tipo de Control	Propiedades de Seguridad de la Información	Estatus	Responsabilidad
Preventivo	Confidencialidad Integridad Disponibilidad	Implementado	Gestor de Activos y Configuraciones Responsable de Certificaciones

Justificación

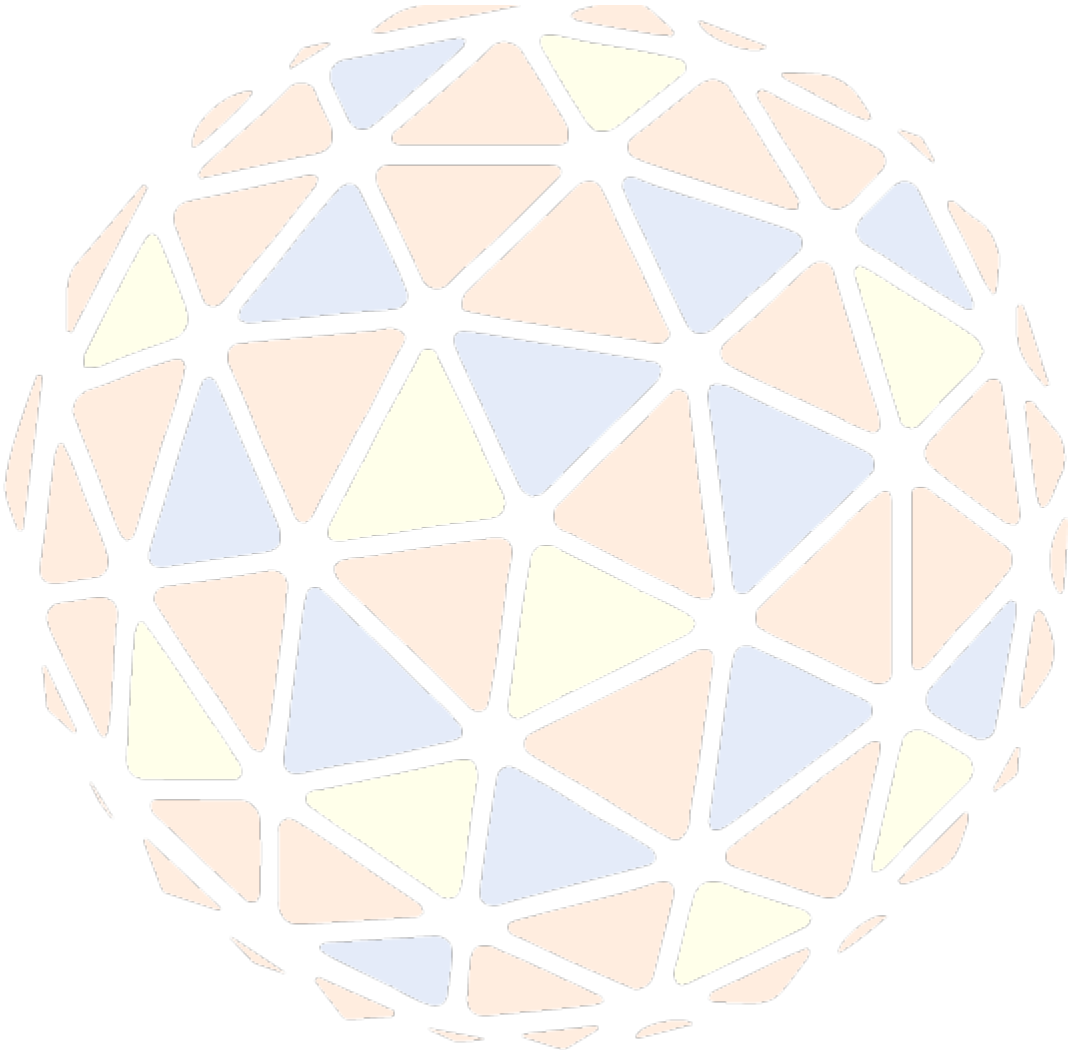
El Gestor de Activos y Configuraciones debe considerar los siguientes requerimientos para el aseguramiento de la integridad de la información en la infraestructura auditada:

- Asegurar que se cuente con los accesos lógicos y físicos necesarios, conforme al alcance de la auditoria.

- Tener la aprobación del Gestor / Oficial de seguridad.

El Responsable de Certificaciones debe:

- Programar las actividades en horarios que no afecten la operación de la organización.



8. DOCUMENTOS RELACIONADOS

Clave	Documento
MA-GPO-01	Manual del Sistema Integrado de Gestión
PO-ADQ-02	Administración de proveedores
PO-GSE-01	Servicios generales
PR-GPO-01	Control documental
PR-GPO-04	Auditoría interna
PR-GPO-05	Acciones correctivas y de mejora.
PR-GPO-09	Gestión de riesgos y oportunidades
PR-GCH-01	Atracción de talento, contratación e inducción
PR-GCH-05	Comunicación institucional.
PR-GCH-08	Capacitación
PR-GAL-01	Reclamación de derechos ARCO
PR-GAL-02	Transferencia o remisión de datos personales
PR-GAL-03	Sanciones administrativas
PR-GAL-17	Identificación y evaluación de requisitos legales y otros
PR-SGE-01	Mantenimiento
PR-SGE-11	Recepción
PR-SGE-12	Servicio de limpieza del corporativo
PR-GTI-05	Gestión de la demanda y capacidad
PR-GTI-08	Gestión de activos y configuraciones
PR-GTI-09	Gestión de cambios
PR-GTI-10	Gestión de liberaciones y entregas.
PR-GTI-11	Gestión de incidentes y solicitudes de servicio
PR-GTI-12	Gestión de problemas
PR-GTI-13	Altas y bajas de equipo de cómputo
AX-GPO-01	Análisis de impacto al negocio (BIA)
AX-GPO-03	Plan de continuidad del negocio (BCP).
AX-GPO-04	Plan de recuperación ante desastres (DRP)
AX-GPO-07	Elaboración de documentos
AX-GPO-11	Plan de pruebas de continuidad
AX-GAL-03	Código de conducta y ética empresarial
AX-GTI-01	Lista de requisitos de seguridad.
AX-GTI-01	Relación usuarios aplicativos
AX-GSS-01	Plan de respuesta a emergencias
AX-GSS-09	Plan integral de seguridad, salud y medio ambiente
DE-GPO-01	Declaratoria Política del SIG
DE-GAL-04	Aviso de privacidad para personal
DE-GAL-05	Aviso de privacidad solicitud de empleo
DE-GAL-08	Declaratoria de responsable del SGSDP
DE-GAL-17	Aviso de privacidad para colaboradores
IT-GTI-35	Borrado seguro
IT-GTI-37	Instalación y configuración de software de cifrado
IT-GTI-38	Uso de software de cifrado
N/A	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

9. REGISTROS GENERADOS

Clave	Registro	Responsable	Protección electrónica	Protección física	Retención	Eliminación
FO-ADQ-10	Alta Proveedor de compras	Responsable de Compras	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-ADQ-11	Foreign Supplier Registratión	Responsable de Entrega de Soluciones y Servicios	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-ESS-19	Evaluación de riesgos y problemas	Responsable de Sistemas	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GAL-07	Matriz de identificación y evaluación de requisitos legales	Responsable de Jurídico	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GAL-09	Inventario de datos personales	Responsable de Jurídico	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GAL-09	Aviso de privacidad	Responsable de Jurídico	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GAL-10	Solicitud de derechos ARCO	Responsable de Jurídico	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GCH-01	Matriz de comunicación	Responsable de Recursos Humanos	Pública - NA	No aplica	Permanente	Borrado
FO-GCH-18	Programa de capacitación	Responsable de Recursos Humanos	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GCH-33	Descriptivo de puesto	Responsable de Recursos Humanos	Interna - Restricción acceso	No aplica	Permanente	Borrado
FO-GPO-01	Listado maestro de documentos	Responsable de Procesos	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GPO-14	Plan de auditoría interna	Responsable de Procesos	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GPO-49	Matriz de Gestión de Riesgos y Oportunidades	Responsable de Procesos	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GSS-22	Matriz de contacto con autoridades	Responsable SASSO	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GTI-03	Base de Conocimiento	Responsable de Sistemas	Interna - Restricción acceso	No aplica	Permanente	No aplica

Clave	Registro	Responsable	Protección electrónica	Protección física	Retención	Eliminación
FO-GTI-16	Asignación de roles y responsabilidades	Responsable de Sistemas	Confidencial - Contraseña	No aplica	Permanente	No aplica
FO-GTI-20	Matriz de Escalamiento Jerárquico y Funcional.	Responsable de Sistemas	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GTI-41	Carta responsiva de equipo de cómputo y otros activos asociados	Responsable de Sistemas	Interna - Restricción acceso	Gaveta	3 años	Borrado y Triturado
FO-GTI-43	Matriz de asignación de roles	Responsable de Sistemas	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GTI-44	Bitácora de respaldos.	Responsable de Sistemas	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GTI-50	Matriz de Autorizadores de Desbloqueo de Puertos USB	Responsable de Sistemas	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GTI-52	Memoria técnica	Responsable de Sistemas	Interna - Restricción acceso	No aplica	1 año	No aplica
FO-GTI-60	Perfiles de usuario	Responsable de Sistemas	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-GTI-61	Matriz de Incidentes de seguridad.	Responsable de Sistemas	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-SGE-02	Programa anual de mantenimiento	Responsable de Servicios Generales	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-SGE-03	Bitácora de acceso	Responsable de Servicios Generales	Interna - Restricción acceso	Archivero	1 año	Triturado
FO-SGE-05	Bitácora de Servicios Generales	Responsable de Servicios Generales	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-SGE-06	Bitácora rutina Mensual Preventiva de Extintores	Responsable de Servicios Generales	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-SGE-12	Responsiva de telefonía móvil, reasignación y pago de telefonía móvil	Responsable de Servicios Generales	Interna - Restricción acceso	No aplica	Permanente	No aplica

Clave	Registro	Responsable	Protección electrónica	Protección física	Retención	Eliminación
FO-SGE-19	Base de datos de telefonía	Responsable de Telefonía	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-SGE-31	Bitácora de Vigilancia	Responsable de Servicios Generales	Interna - Restricción acceso	No aplica	Permanente	No aplica
FO-SGE-34	Salida de Activos	Responsable de Servicios Generales	Interna - Restricción acceso	No aplica	Permanente	No aplica

10. CONTROL DE CAMBIOS

Fecha	Alcance del cambio	Descripción del cambio	Versión
17/04/2025	Actualización al contenido del documento.	Se realiza la integración del Manual de Teliko y Custom Soft Se actualizan controles de acuerdo con la operación actual.	05
28/11/2023	Actualización al contenido del documento.	Se actualiza el numeral 5.10 Uso aceptable de la información y otros activos asociados, se integra un apartado relacionado al daño y cobro de equipo. Se elimina el control de bloqueo de puertos USB.	04
06/07/2023	Actualización al contenido del documento.	Se ha realizado una revisión total de los controles de acuerdo con la versión 2022 de la ISO 27001, ha habido una reestructuración y reagrupación de controles con el objetivo de minimizar los controles y agruparlos de una forma más lógica y fácil de entender. Hay un total de 11 nuevos controles y 24 se han fusionado. Se ha actualizado a la plantilla actual de la Organización.	03
01/07/2022	Actualización al contenido del documento.	Revisión total de los lineamientos, realizando los ajustes aplicables conforme a la realidad operativa actual de la organización.	02
01/06/2021	Actualización al contenido del documento.	Emisión inicial del documento. Se asigna clave del área de Procesos, sustituye al MA-GTI-01	01

