POLITICA DE SEGURIDAD DE LA INFORMACION

Control e Historial de modificaciones

Fecha	Versión	Descripción de la modificación
05/05/2023	1.0	Documento Original
29/09/2023	2.0	- Reforma integral del documento - El Anexo 1 Acta de destrucción y el anexo 2 Bitácora de activos de información/documentos destruidos pasan a ser anexos del Manual para la Manipulación de soportes. - El Anexo 3 pasa a ser el Anexo 1 "Acta de entrega recepción de activos de la información" - El Anexo 4 Objetivos de seguridad se integra a los Objetivos del SIG.
25/1/2024	3.0	- Inclusión de la sección Política de uso de números empresariales
16/02/2024	4.0	- Inclusión de la sección Plan de Implementación a la Ley Orgánica de Datos. - Se actualiza formato control de documentación. - Se incluye cuadro para evidenciar la creación, revisión y aprobación de documentos.
01/10/2024	5.0	- Se incluye la sección Política de Gestión de Usuarios que prohíbe el uso de cuentas genéricas, promoviendo el uso de cuentas nominativas para cada persona que accede a los sistemas de la organización.
05/09/2025	6.0	- Actualización según controles ISO 27001:2022 - Se incluye el contenido de la Política de provisión de la información. - Actualización logo empresarial y encabezado.
19/12/2025	7.0	Actualización de la codificación según la estructuración de codificación de documentos de la metodología para la gestión por procesos. -
06/04/2026	8.0	- El anexo 1 Acta de entrega recepción de activos informáticos cambia a Anexo 1 Acta de entrega de activos informáticos - Se incluye el Anexo 2 Acta de recepción de activos informáticos
11/05/2026	9.0	- Actualización de la sección Activos de la información y sección Anexos
29/05/2026	10.0	Inclusión de la sección "Lineamiento para el Uso Responsable de Herramientas de Inteligencia Artificial"

Creado por:		Revisado y Aprobado por:
Validar únicamente en FirmaEC. Firmado electrónicamente por: GUILLERMO BERNARDO HERRERA MONTERO	Validar únicamente en FirmaEC. Firmado electrónicamente por: ANA CRISTINA CEVALLOS MONTERO	Validar únicamente en FirmaEC. Firmado electrónicamente por: PAUL ALEJANDRO NOBOA NARVAEZ
_____ Ing. Guillermo Herrera Jefe de TI	_____ Ing. Cristina Cevallos Jefe de Gestión Calidad	_____ Abg. Paúl Alejandro Noboa Gerente General

Contenido

INTRODUCCIÓN

La información se ha convertido en un activo substancial de organizaciones, toda vez cuando es completa, precisa y actualizada es fundamental en la toma de decisiones de las mismas. La importancia de la información se fundamenta en la teoría de la organización, la cual se define como un sistema conformado por personas, recursos materiales e información.

Sin embargo, dichos sistemas a medida que se consultan almacenan y generan información, ponen en riesgo la integridad de la misma; riesgos, que no solo provienen del exterior sino también del interior de ELTHON CEO. Estas amenazas constantes que atentan contra la información de cualquier organización pueden causar pérdidas considerables mismas que deben ser prevenidas y mitigadas. Como consecuencia, la seguridad de la información no es sólo cuestión de tener nombres de usuario y contraseñas, sino que requiere de reglamentos y diversas políticas de privacidad y protección de datos que imponen unas obligaciones para organizaciones.

Para todas las unidades de negocios de ELTHON CEO, la información es un activo esencial. Es crucial que toda la información sensible sea mantenida de manera confidencial, sea precisa y esté disponible, de la manera apropiada para cubrir las necesidades de los negocios. Será responsabilidad de cada individuo proteger adecuadamente la información que maneje durante el desempeño de sus actividades.

El Sistema de Gestión de la Seguridad (SGSI) de la información consiste básicamente en un conjunto de políticas para definir, construir, desarrollar y mantener la seguridad del equipo basado en hardware, recursos de software y gestión documental. Los SGSI bajo los requerimientos que exige la norma ISO 27001 :2022 y sus derivaciones, constituyen la base para la gestión de la seguridad de la información; dicha norma, define un SGSI que garantiza el conocimiento, apropiación, gestión y disminución de riesgos de seguridad de la información para la organización, de forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a cambios que se produzcan en los riesgos, entorno y tecnologías.

Cada empleado de ELTHON CEO será, consecuentemente, consciente de la responsabilidad de asegurar la información bajo su cargo y actuará para preservar la misma.

Esta Política regulará el comportamiento que deberá ser observado y cumplido por todos los funcionarios (regulares, tercerizados, temporales, pasantes, etc) de ELTHON CEO para lograr la seguridad de la información. Los terceros involucrados (proveedores, clientes, etc) serán incluidos en los requerimientos de esta Política de manera voluntaria o contractual.

1. Objetivo

Establecer un marco integral para la gestión de la seguridad de la información en ELTHON CEO de acuerdo con los requisitos de los controles de la norma ISO 27001:2022, definiendo las directrices y procedimientos para mantener la confidencialidad, disponibilidad e integridad de los activos de información y los sistemas de la organización contra posibles amenazas de seguridad, asegurando la continuidad de las operaciones y minimizando el riesgo de pérdidas que precisen destinar recursos informáticos y económicos para la recuperación de la información.

2. Alcance

Esta Política se aplica a todo el Sistema de Gestión Integral, en lo que contempla a la gestión del Software ELTHON.

La Política define los lineamientos de seguridad, los procesos de Tecnología de la Información y Administración de Riesgos, clasifica la información, responsabilidades y principios fundamentales para asegurarla el cumplimiento de los objetivos de seguridad definidos en el **Anexo Objetivos del Sistema Integrado de Gestión.**

Esta Política es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información de la organización con el objetivo de cumplir las leyes y regulaciones nacionales aplicables, cuando la política se vea afectada por dichas leyes y/o regularizaciones deberá ser actualizada a fin de cumplir con las exigencias de ELTHON CEO.

3. Responsables

La responsabilidad de la gestión de la información no recae plenamente en el responsable de Seguridad de la Información (Jefe TI), sino que le corresponde a cada uno de los funcionarios precautelar, velar por el cuidado y custodia de los activos de información.

Las políticas descritas en el documento son aplicables a todos los empleados de ELTHON CEO, contratistas, proveedores, socios y terceros que utilicen los sistemas de información de la organización.

4. Definiciones

Cadena de suministro de tecnología de la información y de las comunicaciones (TIC): se refiere al conjunto de procesos, actividades y recursos involucrados en la adquisición, desarrollo, implementación y gestión de productos y servicios relacionados con la tecnología de la información y las comunicaciones.

Confidencialidad: Característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Datos: Es cualquier forma de registro susceptible de ser capturado, almacenado, procesado y distribuido.
Disponibilidad: Característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

Información: Es cualquier forma de registro previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega.

Información crítica: Es la considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.

Incidente de seguridad de la información: Es el evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.

Políticas de seguridad de TI: son un conjunto de reglas, procedimientos y prácticas establecidas para proteger la información y los sistemas de una organización contra posibles amenazas, como virus informáticos, ataques de hackers, robo de datos y otros riesgos de seguridad.

Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de gestión de seguridad de la información: Parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Seguridades lógicas: Son los mecanismos de protección en el uso del software, de los datos, procesos y programas, que permiten el acceso autorizado de los usuarios a la información.

5. Documentos de referencia

- Norma ISO/IEC 27001:2022
- Norma ISO 27017:2021
- Norma ISO 27018:2019
- Norma ISO 27701:2019
- Objetivos del Sistema Integrado de Gestión
- Manual del Sistema Integrado de Gestión
- Política del Sistema de Gestión Integrado

6. Principios de Seguridad de la información

A continuación, se establece los principios de seguridad de la información:

1. **Confidencialidad:** La información se clasifica y protege de manera que solo las personas autorizadas tengan acceso a ella.
2. **Integridad:** La información se mantiene precisa y libre de modificaciones no autorizadas. Para lo cual, se aplicarán controles para garantizar que la información no sea alterada de manera indebida.
3. **Disponibilidad:** La información estará disponible y accesible para las partes interesadas autorizadas cuando sea necesario. El Jefe de TI establecerá medidas de redundancia y recuperación ante desastres.

7. Políticas de seguridad

ELTHON, además de lo establecido en la Política del Sistema de Gestión Integrado, define y mantiene políticas de seguridad de la información con el propósito de:

- Proteger la información y los activos de la organización.
- Garantizar el cumplimiento de requisitos legales, regulatorios y contractuales.
- Gestionar riesgos de seguridad de la información de manera preventiva y correctiva.
- Fomentar una cultura organizacional basada en la seguridad.
- Establecer un marco para la toma de decisiones y la evaluación de la efectividad de los controles de seguridad.

Las políticas se desarrollan en alineación con los objetivos estratégicos de la organización, considerando los riesgos actuales, las amenazas emergentes y la normativa vigente.

Todo el personal está obligado a cumplir las disposiciones establecidas en estas políticas. La organización se reserva el derecho de modificarlas cuando sea necesario; cualquier actualización será comunicada de manera formal a través de la **Matriz de Comunicaciones**, bajo responsabilidad del Jefe de Gestión de la Calidad y/o el Jefe de TI.

La política y las políticas específicas de seguridad de la información deben ser:

- Definidas y aprobadas por el Gerente General.
- Publicadas y comunicadas al personal y partes interesadas relevantes.
- Reconocidas y aceptadas por quienes correspondan.
- Revisadas en intervalos planificados o ante cambios significativos.

8.1 Roles y Responsabilidades de Seguridad de la Información

Los roles y responsabilidades en materia de seguridad de la información se definen y asignan en el **Manual del Sistema de Gestión Integrado**, dentro de la sección Roles y Responsabilidades de la Organización.

Cada colaborador conoce las funciones que le correspondan en relación con la seguridad y protección de la información a través del **Contrato de Trabajo, Acta de Confidencialidad** y participación en **capacitaciones internas y externas**.

8.2 Responsabilidades de Gestión

La alta dirección es responsable de garantizar que la seguridad de la información se aplique en toda la organización, exigiendo el cumplimiento de:

- La Política de Seguridad de la Información.
- Las políticas y procedimientos específicos establecidos en el SGI.
- Los requisitos de seguridad aplicables a su área y funciones.

Asimismo, debe velar por la disponibilidad de recursos y la supervisión del cumplimiento de los controles de seguridad definidos a través de **Auditorías Internas, Minutas de revisión por la alta dirección**, entre otros.

8. Activos de la información

Los activos de la información se describen en el **Inventario de Activos** que incluyen datos, sistemas, aplicaciones, hardware, software, documentos y recursos humanos relacionados con la gestión y procesamiento de información. La responsabilidad sobre el uso, resguardo y gestión de los activos de información corresponde a cada propietario del activo, conforme al Inventario de Activos definido por la organización. Cada responsable deberá garantizar el uso adecuado de los activos asignados, velando por su confidencialidad, integridad y disponibilidad, así como reportar oportunamente cualquier debilidad o incidente de seguridad de la información al área de Tecnologías de la Información.

Los activos de información deberán ser utilizados exclusivamente para fines relacionados con las actividades y servicios de la empresa, bajo criterios de uso responsable, ético y seguro, conforme se establece en la **Política de Uso Aceptable de Activos de la Información**.

La Jefa de Gestión de Calidad es la delegada por Gerencia para validar las **Actas de entrega y Actas de recepción de activos;** y realizar el seguimiento correspondiente, asegurando su conformidad con los estándares establecidos. El apoyo operativo o logístico brindado por otros colaboradores, como el personal administrativo, se entenderá como un soporte al proceso, sin que ello implique la transferencia de esta responsabilidad de validación y seguimiento.

El Jefe de Gestión de Calidad, en coordinación con el Jefe de Tecnologías de la Información, tendrá un rol de acompañamiento, capacitación y verificación del cumplimiento de estándares relacionados con el uso adecuado de los activos, sin que esto implique la asunción de la responsabilidad directa sobre la gestión operativa de los mismos, la cual corresponde a cada propietario designado.

Para la gestión de activos de la información, se utilizará el **Anexo 1 – Acta de Entrega de Activos** cuando la empresa entregue activos al colaborador para el desarrollo de sus funciones laborales.

Por su parte, el **Anexo 2 – Acta de Recepción de Activos** será utilizado cuando la empresa reciba los activos asignados al colaborador o, de ser necesario, cuando dichos activos deban ser entregados temporalmente a un tercero autorizado debido a ausencias por vacaciones, permisos u otras situaciones debidamente justificadas.

9. Riesgos y amenazas

Los activos de la información pueden presentar una amplia variedad de amenazas que incluyen, pero no se limitan a:

Amenazas cibernéticas:

- **Hacking:** afecta a los activos de información y la propiedad intelectual.
- **Hacking social (phishing)**: se presenta en los activos humanos, afecta directamente a las personas, clientes como trabajadores de ELTHON CEO, se presenta cuando una persona tiene un acercamiento con intención de obtener información confidencial, como claves ya acceso al sistema. ELTHON CEO controla el Hacking Social a través de las cláusulas de confidencialidad del contrato con sus partes interesadas.
- **Malware:** incluye virus, troyanos, gusanos y ransomware.

Amenazas internas

- Acceso no autorizado de trabajadores a datos o sistemas a los que no deberían tener acceso.
- Negligencia: Acciones no intencionadas de trabajadores que pueden poner en riesgo la seguridad de la información, como la pérdida de dispositivos o la revelación accidental de datos confidenciales.

Desastres naturales

- Incendios, inundaciones, terremotos y otros desastres naturales que pueden dañar equipos físicos y documentos.

Robo o pérdida de dispositivos

- Robo o pérdida de ordenadores que contienen información confidencial.

Vulnerabilidades de Software

- Errores o debilidades en el software que pueden ser explotados por atacantes.

Acceso físico no autorizado

- Personas no autorizadas que obtienen acceso físico a las instalaciones del servidor físico.

La metodología para la evaluación de riesgos de seguridad de la información asociados a los activos de la información se describe en el **Manual para la evaluación y tratamiento de riesgos de seguridad de la información.**

10. Política de Clasificación de la Información

Se establece la **Política de Clasificación de la Información** para establecer lineamientos para la clasificación de la información de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.

11. Política de Gestión de medios de almacenamiento

Se establece el **Manual para la gestión de medios de almacenamiento** para establecer directrices y procedimientos para la gestión segura de los medios de almacenamiento que contienen información de la organización, a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización, con el fin de evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en estos medios de acuerdo con lo establecido en los controles de la norma ISO 27001:2022.

12. Gestión de la seguridad de la información

- El Gerente General o su delegado deberá revisar los objetivos de seguridad de la información establecidos en los **Objetivos del Sistema de Gestión Integral**, y deberá establecer nuevos en caso de requerirse. Además, se realizará la medición de objetivos de Seguridad de la Información al menos una vez al año.
- El Gerente General verificará el cumplimiento de todos los objetivos de seguridad a través de los indicadores de procesos de Tecnología de la Información y documentación del SGI.
- El Jefe de Gestión de la Calidad analizará y reportará al Gerente General el resultado de la medición como material de ingreso para la revisión por parte de la dirección.

- El Gerente General definirá la distribución de funciones y responsabilidades para controlar la implementación de la seguridad de la información; las funciones y responsabilidades estarán descritas en la Sección de Roles y Responsabilidades del **Manual del Sistema de Gestión Integrado.**
- El Jefe de TI establecerá la gestión de activos informáticos descritos en el Inventario de Activos para que éstos reciban un apropiado nivel de protección.
- Los propietarios de los activos de la información se asegurarán de que los datos y/o información cumplan con los niveles de autorización correspondiente para su utilización y divulgación.
- El Jefe de TI mantendrá los registros de auditoría (logs) de los eventos ocurridos referente al sistema y acciones que realicen las entidades financieras en el Software Elthon.
- El Jefe de TI mantendrá niveles de operación razonables en los activos de información.
- El Jefe de TI realizará la identificación y gestión de riesgos relacionados al ambiente tecnológico.
- Los registros de auditoría (logs de clientes) que se almacenan con fines de revisión deberán ser eliminados semestralmente, para que no afecten el rendimiento de los servicios.

13. Requisitos de seguridad de la aplicación

ELTHON establece un marco para la identificación, especificación y aprobación de requisitos de seguridad de la información al desarrollar o adquirir aplicaciones. Estos requisitos se aplicarán a todos los activos de la información y sistemas con el fin de garantizar la protección, confidencialidad, integridad y disponibilidad de la información.

- Gestión de contraseñas
- Control de acceso
- Protección de datos personales
- Gestión de usuarios
- Administración de acceso lógico
- Desarrollo seguro
- Gestión de perfiles
- Respaldos de información y planes de recuperación
- Registros de auditoría (logs)
- Gestión de incidentes
- Cumplimiento contractual con clientes y proveedores

14. Subprocesos de seguridad de la información

ELTHON CEO dispone de procesos para la gestión de Seguridad de la Información mismos que se encuentra dentro del macroproceso de Tecnología de la Información; dichos procesos establecen responsables, tareas, criterios e implementan controles que se deben seguir para garantizar la seguridad de la información. Los subprocesos para la seguridad de la información se definen en función de:

1. Desarrollo
2. Pruebas y certificación
3. Producción y mantenimiento
4. Seguridad de la información

15. Política de Privacidad y protección de la información de identificación personal (PII)

ELTHON CEO se compromete a garantizar la privacidad y protección de los datos de carácter personal en conformidad con la legislación y regulación aplicables de los trabajadores y terceros que proporcionan información a la organización. La política de privacidad se cumplirá de acuerdo con la normativa de Ley de Protección de Datos vigente en el país.

La organización implementará medidas de seguridad técnicas y organizativas para proteger los datos personales contra el acceso no autorizado, pérdida, divulgación o destrucción, cómo:

1. La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales, para lo cual establece el **Plan de Implementación a la Ley Orgánica de Protección de Datos.**
2. La organización recopilará y utilizará datos de carácter personal únicamente para fines legítimos y específicos, y solo con el consentimiento del titular de los datos cuando sea necesario según lo establecido en los **Contratos del personal y Contrato de Licenciamiento y Uso no exclusivo del Software Elthon.**
3. La organización retendrá datos personales durante el tiempo necesario para cumplir con los fines para los que se recopilaron, y se eliminarán de manera segura cuando ya no sean necesarios, según lo establecido en el **Plan de Implementación a la Ley Orgánica de Protección de Datos.**
4. Registro de incidentes de seguridad relacionados con PII.
5. Capacitación al personal en protección de datos personales
6. Control de accesos (configuración de permisos en sistemas, registros de autenticación multifactor).
7. Cifrado en tránsito (TLS/SSL en comunicaciones) y en reposo (cifrado de bases de).
8. Backups y pruebas de restauración documentadas.
9. Sistemas de prevención de fuga de datos (bloqueo de descargas, restricción de dispositivos de almacenamiento, entre otros)
10. Logs de seguridad que evidencien monitoreo de accesos a datos sensibles.
11. Eliminación segura de información
12. Gestión de vulnerabilidades.

16. Seguridad de la información en las relaciones con los proveedores

ELTHON implementa procesos y manuales para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios de proveedores. La selección, evaluación y revaluación se describe en el **Manual de Gestión de Proveedores**. La protección de los activos de la organización que sean accesibles a los proveedores se asegura a través de los **Acuerdos de nivel de servicios (SLA)** y **contratos** documentados.

- Los acuerdos de nivel de servicio (SLA) describen los niveles de servicio que los proveedores deben cumplir, los términos, condiciones y requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización.
- Los SLA deben incluir pero no limitarse a:
  - Acuerdos de control de acceso que contemplen:
    - Métodos de acceso permitido, y el control uso de identificadores únicos
    - Procesos de autorización y perfiles de acceso de usuarios.
    - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
  - Controles que garanticen la protección contra software malicioso
  - Acuerdos de confidencialidad en los contratos.
  - En caso de efectuar procesamiento de información de las entidades, el proveedor deberá:
    - mantener la confidencialidad de la información entregada
    - aplicar procesos de encriptación
    - manejar procesos de transmisión segura
    - Una vez entregada la información el proveedor será directamente el responsable del destino de la información entregada.
    - ELTHON CEO será el responsable frente a la entidad, con relación a la información que procesa el proveedor.
- Los SLA deberán presentar controles para garantizar la recuperación o destrucción de información y los activos al finalizar el contrato o acuerdo, o durante la vigencia del mismo.
- Los SLA de Azure como proveedor de servicios en la nube se describen en el documento **Infraestructura tecnológica Especificaciones técnicas de ELTHON.** AZURE actualiza su certificado SLA mensualmente, se puede evidenciar en el siguiente link https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1**.**
- Los requisitos de seguridad para que los proveedores de Telconet y OpenSolutions puedan acceder, tratar, almacenar, comunicar o proporcionar componentes de la infraestructura de Tecnología de la Información se establecen en los SLA archivados en el Repositorio.

- El Jefe de TI en conjunto con el Jefe de Gestión de la Calidad, realizarán las evaluaciones y reevaluaciones de los proveedores de TIC para verificar el cumplimiento de los acuerdos y requisitos de seguridad.
- El Jefe de Gestión de la calidad documentará los resultados de estas evaluaciones.
- El Jefe de TI en conjunto con el Administración realizará la revisión, monitoreo de la efectividad y cumplimiento de los acuerdos de nivel de servicio con los proveedores.
- El Jefe de TI registrará los incidentes y las acciones tomadas, relacionados con la cadena de suministro de TIC, como brechas de seguridad o problemas con proveedores en el **Registro de Debilidades e Incidentes de Seguridad de la Información** vinculado al **Subproceso de Gestión de Incidentes de TI.**
- El Gerente General abordará los requisitos de seguridad de la información pertinentes en los acuerdos con los proveedores. Los requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos se describen en cada uno de los **Contratos con los proveedores.**
- Seguimiento, revisión y gestión de cambios de servicios de proveedores se realiza a través de evaluación, selección y reevaluación establecida en el **Manual de gestión para proveedores**. La cadena de suministro de tecnología de la información y de las comunicaciones abarca desde la adquisición de hardware y software hasta la implementación de sistemas, la gestión de servicios de tecnología, el soporte técnico y la disposición de equipos obsoletos. La gestión efectiva de la cadena de suministro de tecnología de la información y las comunicaciones (TIC)

17. Política de Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC)

- Elthon define e implementa procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC. Se asegura que los proveedores de productos y servicios de Tecnologías de la Información y la Comunicación (TIC) cumplan con los requisitos de seguridad de la información, privacidad de los datos personales y confidencialidad, de acuerdo con las normas ISO. Establece:
- Evaluación de proveedores antes de la contratación: Todo proveedor TIC debe es evaluado en cuanto a su cumplimiento en seguridad de la información y protección de datos antes de la firma del contrato, según lo descrito en el **Manual de gestión de proveedores.**
- Los contratos con proveedores incluyen compromisos de confidencialidad, protección de datos personales, uso seguro de la nube, obligaciones en caso de incidentes, continuidad del servicio, acceso a información sensible y cumplimiento normativo.
- Los proveedores TIC serán evaluados de forma anual para verificar el cumplimiento de los requisitos contractuales a través de las **Evaluación anual de proveedores.**
- Todo incidente de seguridad que involucre a un proveedor debe notificarse y gestionarse bajo el **Subproceso de gestión de incidentes.**
- Al terminar la relación contractual, Elthon solicitará por escrito a los proveedores la devolución o eliminación de manera segura toda la información de la organización.

18. Política de control de accesos

ELTHON CEO establece, documenta y revisa un sistema de control de acceso basado en los requisitos de negocio y de seguridad de la información para garantizar que solo las personas autorizadas puedan acceder a la información y recursos de la organización, con el fin de velar por la confidencialidad, integridad y disponibilidad de los activos de información.

Es responsabilidad de cada trabajador, entidad y cada usuario el proteger las contraseñas para evitar accesos indebidos al sistema, así como el uso adecuado de la información que se carga y se genera en el sistema. Los usuarios y claves son personales y no pueden ser compartidos con terceros.

Los activos de información y/o accesos son proporcionados a través de actas.

19.1 Controles de acceso lógicos

Los controles de acceso lógicos se refieren a las medidas y políticas de seguridad diseñadas para protección de registros, sistemas de tecnología de la información, redes y datos; contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada; mediante restricciones de acceso basadas en la identidad del usuario, roles y permisos.

- **Control de acceso basado en roles**, donde el Jefe de TI y/o Jefe de Gestión de la Calidad otorgará acceso a la información únicamente a las personas autorizadas de acuerdo con sus funciones laborales y responsabilidades. Cada trabajador es responsable de precautelar el uso de usuarios y contraseñas.
- **Protocolo de contraseñas seguras:** los usuarios deben establecer contraseñas según el protocolo descrito en el **Manual de Gestión y Manejo de Contraseñas,** de esta manera se garantiza el proceso seguro de inicios de sesión.
- **Cifrado de datos:** El Jefe de TI protegerá los datos e información mediante cifrado, lo que garantiza que solo personas autorizadas puedan descifrar y acceder a la información.
- **Autenticación de usuarios**: todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el equipo de TI antes de poder usar la infraestructura tecnológica de la ELTHON CEO, mediante la introducción de un nombre de usuario y una contraseña.
- **Registro de actividades de acceso**, autenticación y autorización para la detección de actividades sospechosas o no autorizadas.
- Cada usuario que acceda al Software ELTHON debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios.
- Los usuarios y trabajadores son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

19.2 Política de gestión de usuarios

El Jefe de TI es responsable de la implementación, revisión y cumplimiento de Política de Gestión de usuarios, esta política establece directrices claras para la gestión de cuentas de usuario, prohibiendo el uso de cuentas genéricas y promoviendo el uso de cuentas nominativas para cada individuo que accede a los sistemas de la organización.

Esta política aplica a todos los empleados, contratistas y terceros que utilizan sistemas y recursos tecnológicos de la organización.

- **Prohibición de Cuentas Genéricas**: Queda estrictamente prohibido el uso de cuentas genéricas o compartidas, como "Admin", para acceder a los sistemas y recursos de la organización.
- **Uso de Cuentas Nominativas**: Cada usuario debe tener una cuenta nominativa única que lo identifique personalmente en el sistema. Estas cuentas deben estar asociadas a los privilegios adecuados según su rol y responsabilidades.
- **Autenticación Segura**: Todas las cuentas nominativas deben estar protegidas con mecanismos de autenticación robustos, incluyendo el uso obligatorio de doble factor de autenticación (2FA) para cuentas con privilegios elevados.

19.3 Creación y deshabilitación de perfiles y usuarios

Respecto a la gestión con clientes se establece las siguientes actividades para el control de accesos.

ELTHON CEO genera el **Acta entrega Acceso Sistema vinculado al Subproceso de Administración de Entidades**, donde consta:

- La recepción de credenciales de la Entidad para el usuario reportería y usuario administrador. la entrega de usuarios Sistemas Elthon.
- Recepción de credenciales adicional en el caso de que la entidad lo requiera.
- Entrega de usuario para acceso a la Plataforma virtual.

De esta manera el cliente, será responsable de los mecanismos de control de acceso que le sean proporcionados.

El proceso de creación y uso de contraseñas segura se detalla en el **Manual de Gestión y Manejo de Contraseñas** de ELTHON CEO donde se establece un protocolo de contraseñas seguras y el manejo de contraseñas respecto al cambio, recuperación y acceso.

ELTHON CEO, dispone de usuarios para acceso al entorno del cliente como soporte para la aplicación de reportería y administrador; dichos usuarios son autorizados por el cliente. La creación y eliminación de usuarios se registra en el **Anexo Creación y bloqueo de usuarios a petición de las entidades vinculado al Subproceso de Administración de Perfiles y usuarios.**

Si se diera por terminado el contrato de licenciamiento entre el cliente, ELTHON CEO suscribe un acta de terminación respectiva y se deshabilita el usuario de acuerdo a lo descrito en el **Manual de Gestión y Negociación de Clientes.**

19.4 Administración y uso de contraseñas

La política de control de acceso también se ocupa de la gestión de contraseñas y de la autenticación de usuarios, asegurando que solo los usuarios autorizados puedan acceder a los recursos de la organización. Además, se establece lo siguiente:

- Se aplica un estándar de creación de contraseñas seguras para el acceso de usuarios según lo descrito en el **Manual de Gestión de Contraseñas.**
- La asignación de contraseñas se realiza de forma individual por lo que el uso de contraseñas compartidas está prohibido.
- En el caso de cliente, cuando un usuario olvide, bloquee o extravié su contraseña deberá solicitar al Especialista de Soporte Funcional que le proporcione una nueva contraseña si es el caso o desbloquee su contraseña existente.
- En el caso de trabajadores, cuando un usuario olvide o bloquee su contraseña deberá solicitar al Jefe de TI que le proporcione una nueva o desbloquee de contraseña.
- El Software ELTHON está configurado de tal manera que permita al usuario cambiar su clave obligatoriamente cuando ingresa por primera vez al sistema.
- Los usuarios deben cambiar inmediatamente la contraseña al sospechar o detectar que ha sido vista por terceras personas.
- Todo el personal debe mantener sus equipos de trabajo diario con contraseña de acceso segura cuando no estén trabajando en ellas.

19.5 Revisión de los derechos de acceso de usuario

Para la gestión de perfiles y usuarios de clientes, se dispone del **Subproceso de Administración de perfiles y usuarios** donde se establece el registro y retirada de usuarios lo que permitirá una asignación efectiva de los derechos de acceso a la información.

Mientras que la gestión de perfiles y usuarios de trabajadores está a cargo del Jefe de Gestión de la Calidad y Jefe de TI.

Los propietarios de los activos en conjunto con el Jefe de Gestión de la Calidad otorgan acceso a los activos de información basándose en roles y actividades específicas asignadas de los trabajadores.

El Jefe de TI en conjunto con el Administrador deberán definir el flujo de autorización para el acceso y el nivel de privilegios para los activos de Aplicación, sistemas y base de datos en la nube.

Esta revisión garantizará que los derechos de acceso sigan siendo adecuados para las responsabilidades y tareas de cada usuario.

El Software ELTHON genera un reporte de usuarios creados para el manejo, control y revisión de los mismos, el reporte de usuarios se genera del sistema administrador.

19.6 Política de uso de utilidades con privilegios del sistema

ELTHON CEO restringe y controla rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación a través del usuario Súper Administrador.

El Jefe de TI será el responsable de administrar el control y permisos para el funcionamiento de las entidades en los ambientes de reportería y administración.

19.7 Control de acceso al código fuente de los programas

Se restringe el acceso al código fuente de los programas, las herramientas de desarrollo y las bibliotecas de software al equipo de TI liderado por el Jefe de Ti, bajo la supervisión del Administrador, tal como se menciona en los Requerimientos de Seguridad del **Manual de Desarrollo Seguro.**

Cada dispositivo de los desarrolladores de ELTHON CEO maneja una IP única para el acceso a los ambientes de desarrollo y servicios de Azure, en caso de ambiente de desarrollo se dispone una llave SSH del dispositivo y en caso de Azure la IP del dispositivo.

19. Adquisición, desarrollo y mantenimiento de los sistemas de información

ELTHON CEO garantiza que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Para lo cual establece los siguientes lineamientos:

20.1 Análisis de requisitos y especificaciones de seguridad

La organización ha documentado el **Subproceso de Implementación del Sistema de Gestión de Seguridad** que establece actividades para ejecutar y controlar la implementación de los requisitos en la evaluación y mejora de procesos de TI relacionados con la seguridad de la información.

Además, se ha establecido la **Metodología de evaluación y tratamiento de riesgos** que incluye pasos específicos para identificar los requisitos, evaluar su impacto en la seguridad. El registro incluye la lista de amenazas, vulnerabilidades y riesgos identificados, así como las estimaciones de impacto y probabilidad. Cada riesgo está vinculado a los requisitos de seguridad pertinentes.

20.2 Servicios a través de redes públicas

La organización ha establecido controles lógicos para proteger la información involucrada en aplicaciones que pasan a través de redes públicas, de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas, según lo descrito en la S**ección Controles de Accesos Lógicos de la presente política.**

20.3 Protección de las transacciones de servicios de aplicaciones

La información involucrada en las transacciones de servicios de aplicaciones será protegida por los sistemas nativos en la nube que adoptan microservicios para construir aplicaciones modernas. La arquitectura de microservicios es distribuida y ligeramente acoplada, por lo que un error en un componente no interrumpe toda la aplicación. Por lo tanto, los servicios deben interactuar mediante un protocolo de comunicación entre procesos como HTTP, AMQP o un protocolo binario como TCP, en función de la naturaleza de cada servicio, tal como se describe en el **Infraestructura Tecnológica y Especificaciones Técnicas del Software.**

20.4 Planificación y aceptación del sistema

- El Administrador estará a cargo de las actualizaciones en el contexto externo que puedan requerir actualización del sistema, y notifica al Gerente General para su actualización.
- El Jefe de TI efectuará el monitoreo de las necesidades de capacidad de los servicios en producción (sistemas) y proyectará nuevas necesidades, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta los nuevos requerimientos de los servicios, así como las tendencias actuales en el procesamiento de la información de ELTHON CEO para el período estipulado de vida útil de cada componente.
- El Jefe de TI deberá especificar los criterios de aceptación para un nuevo sistema o servicio tecnológico a implementar en ELTHON CEO. Debe considerar los siguientes puntos basados en el COBIT:
  - Verificar el impacto en el desempeño y requerimientos de capacidad en los equipos informáticos.
  - Garantizar la recuperación ante errores.
  - Garantizar la implementación acorde a las normas de seguridad establecidas.
  - Asegurará que la nueva implementación no afectará negativamente a los sistemas existentes.
  - Considerar el efecto en la seguridad con la nueva implementación.

20. Política de desarrollo seguro

Para garantizar la seguridad en el desarrollo y en los procesos de soporte, se ha diseñado e implementado en el ciclo de vida de desarrollo de software y la gestión de los sistemas de información el uso de parches y de releases.

El parche se da en una actualización de mantenimiento, si el resultado fue algún error o bug (cuando aparece un error y se desconoce la razón, datos no bien tratados, sistema no está buscando bien la información, aparece error de la nada) y el realeases se da por un cambio grande en el sistema o por afectaciones en nuevos requerimientos.

Se establece el **Manual de Desarrollo Seguro** donde se define las reglas para el desarrollo seguro de software, incluyendo aquellos elementos de configuración y de documentación necesarios para la implantación, administración y operación del sistema.

El control de cambios a lo largo del ciclo de vida del desarrollo se realiza según lo descrito en el **Subproceso de Ensamblaje, Certificación y Puesta en Producción**.

Las pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones se realizarán según lo descrito en el Subproceso de Ensamblaje, Certificación y Puesta en Producción haciendo uso del **Formato Pruebas en Certificación.**

Las pruebas de la seguridad funcional durante el desarrollo se realizan según lo descrito en el **Subproceso de Pruebas unitarias y de vulnerabilidad** la salida será el **Informe de resultados de análisis y escaneo con SonarQube.**

Los datos de prueba se seleccionan con cuidado y deberán estar protegidos y controlados, para lo cual se establece un ambiente de pruebas seguro y controlado para garantizar que los requisitos del proyecto se cumplan eficientemente según lo descrito en el **Manual de Desarrollo Seguro.**

21. Política de Autenticación segura

Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso, las cuales se describen en el **Manual de Desarrollo Seguro.**

22. Política de Monitoreo de Seguridad física

Elthon no implementa seguridad física en oficinas y salas, ya que sus actividades se realizan bajo la modalidad de Teletrabajo. Las siguientes consideraciones no aplican a ELTHON CEO ya que los trabajadores ejecutan sus actividades vía teletrabajo.

- Seguridad de oficinas, despachos y recursos.
- Protección contra las amenazas externas y ambientales.
- Trabajo en áreas seguras.
- Áreas de carga y descarga.
- Traslado de información en formato físico o en dispositivos.

Sin embargo, al disponer de un Servidor Físico, se apoya del contratos, proceso y SLA del proveedor Telconet para monitorear continuamente para el acceso físico no autorizado.

Además, Elthon evaluará al proveedor de servicios de alojamiento o centro de datos en función de su capacidad para proporcionar un entorno seguro que cumpla con los requisitos de seguridad de la información según lo descrito en el **Manual de Gestión de Proveedores.**

Los requisitos incluyen controles de entrada adecuados, para asegurar que únicamente se permita el acceso al personal autorizado de ELTHON. El Jefe de TI y el Administrador son las únicas personas que pueden ingresar a las instalaciones físicas del Servidor Físico según lo menciona el **Manual de Infraestructura Tecnológica - Servidor Físico.**

23. Política de seguridad de los equipos

Esta política aplica a los equipos descritos en el **Inventario de Activos**; con el objetivo de mantenerlos de forma segura y protegida, así evitar la pérdida, daño, robo y la interrupción de las operaciones de la organización.

Para el emplazamiento y protección de equipos, así como la eliminación segura o reutilización de estos, Elthon dispone del **Manual de gestión de medios de almacenamiento.**

En el caso, del servidor físico el emplazamiento y protección de equipos, instalaciones de suministro, seguridad del cableado y mantenimiento del servidos se rige según el **Contrato, procedimientos y SLA del proveedor** Telconet. Para el mantenimiento lo realizará Telconet físicamente y los asesores de Elthon lógicamente.

Además se establece la Política de Teletrabajo y la Política de uso aceptable de activos de la información donde se ha establecido los lineamientos para para la protección y seguridad de activos en el contexto de teletrabajo.

El Jefe de Gestión de la Calidad podrá realizar inspecciones virtuales de los entornos de trabajo de los empleados que realizan teletrabajo. Esto implica verificar que los equipos estén ubicados en lugares seguros y que se sigan las pautas de seguridad.

24.1 Política de mantenimientos de equipos

Con la finalidad de proporcionar a los empleados de ELTHON CEO una guía detallada para la configuración y el mantenimiento adecuado de los equipos asignados por la empresa, con el fin de optimizar su rendimiento, seguridad y garantizar una experiencia óptima de teletrabajo se ha establecido el **Instructivo para Configuración y Mantenimiento de equipos**.

24. Política de seguridad de las operaciones

25.1 Procedimientos de operación

Los subprocesos de operación se han documentado de acuerdo con lo descrito en el **Manual de Gestión por Procesos** y se mantienen en el Repositorio Documental para el uso de los trabajadores.

25.2 Gestión del cambio

- Los cambios en las instalaciones de procesamiento de información y los sistemas de información, procesos, instalaciones de tratamiento de la información, los sistemas y los cambios en el ambiente de producción que afectan a la seguridad de la información se controlan a través del **Registro de Cambios en Producción vinculado al Manual de Gestión de Cambios en Producción.**
- Los procedimientos de control de cambios a los sistemas operativos deberán contemplar lo siguiente:

  - Tipo de error o cambio
  - Respuesta HTPP
  - Descripción del cambio
  - Fecha del cambio
  - Solución aplicada
  - Descripción de solución
  - Fecha de solución
  - Responsable de solución.
  - Rama de cambios

25.3 Separación de los recursos de desarrollo, pruebas y producción

- Todo servicio deberá ser probado y verificado su funcionamiento en un ambiente de pruebas según lo descrito en el **Subproceso de Requerimientos Tecnológicos** y el **Manual de Desarrollo Seguro.**
- Los servicios que se estén probando para su operación también deberán pasar pruebas de seguridad.
- La Gestión de capacidades se describe en el **Manual de Tecnología de la Información**.

25.4 Controles filtrado web

Los controles de detección, prevención y recuperación que sirvan como protección el acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso según lo descrito en **Infraestructura tecnológica y especificaciones técnicas del software.**

25. Copias de seguridad de la información

El Jefe de TI realizará copias de seguridad de la información, el software y los sistema para garantizar la disponibilidad de la información crítica en caso de una falla o interrupción del sistema, para ello Elthon dispone de:

- Desarrollo de estrategias de continuidad y Plan de respaldo de datos (backups) descritos en el **Plan de Continuidad del Negocio.**
- Uso de un servidor físico como respaldo de la información en la nube.
- El registro de los backups se realiza en el Anexo **Registro de Backups y restauración** vinculada al **Subproceso de Generación y recuperación de respaldos de información**.

26. Política de evaluación y decisión sobre eventos de seguridad de la información.

Elthon evalúa los eventos de seguridad de la información y decide si se clasificarán como incidentes de seguridad de la información, para lo cual se cataloga como incidente a cualquier evento que afecte directamente a la seguridad de la información y a los servicios de ELTHON CEO de acuerdo con las siguientes categorías:

-
    - Virus de todo tipo
    - Ataques
    - Hacking social
    - Suplantación de Identidad
    - Detección de vulnerabilidades
    - Explotación vulnerabilidades conocidas
    - Violación de políticas
    - Accesos no Autorizados
    - Robo de Información
    - Alteración de la Información
    - Pérdida de datos

26.1 Recolección de evidencia

Elthon establece e implementa procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información. Se tiene:

- El Jefe de TI deberá realizar el **Reporte de debilidades e incidentes de TI** y comunicará directamente al Gerente General para realizar correctivos de ser el caso.
- Todos los incidentes ingresados en el área de Tecnología, se debe remitir el acuse de recibo al usuario indicando el estado y tiempo de solución.
- Los reportes de incidentes de seguridad de la información y vulnerabilidades y los informes ejecutivos son de carácter confidencial.
- El Jefe de TI deberá remitir las estadísticas de los incidentes y vulnerabilidades atendidas por el área de Tecnología haciendo uso de la **Matriz de Indicadores Clave.**

- El proceso y responsabilidades establecidas para la Gestión de Incidentes de seguridad de la información, se aplicará de igual manera para la gestión de incidentes vinculados a la información de las entidades. El proceso que aplicar se encuentra detallado en el **Subproceso de Gestión de Incidentes de SI.**
- El Jefe de TI comunicará al personal sobre la gestión de incidentes que presentan una amenaza para la seguridad de la información, pudiendo ser intencionados, como ataques cibernéticos, o no intencionados, como errores humanos o desastres naturales, pero todos ellos representan una amenaza para la seguridad de la información de una organización, haciendo uso de la **Matriz de Comunicaciones**

26.2 Evaluación y decisión sobre eventos de seguridad de la información

La figura1 muestra el monitoreo de gestión de la información en las bases de datos arrojado por Microsoft Azure, donde se detecta si es grave el incidente, siempre y cuando entre en el catálogo de crítico de Microsoft Azure.

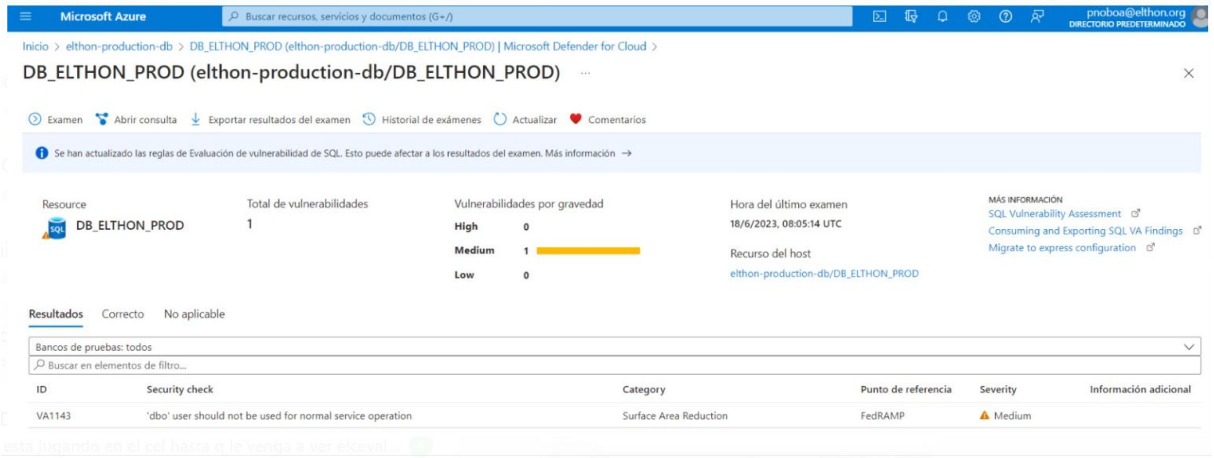

FIGURA 1

ELTHON CEO en relación con la provisión de información sobre la verificación de cumplimiento técnico establece el objeto, los métodos, la frecuencia, los resultados y las acciones correctivas en caso de incumplimientos.

26.2.1 Métodos

ELTHON CEO utiliza los siguientes métodos para cumplir con la provisión de información sobre la verificación de cumplimiento técnico:

- Establece políticas y principios descritas en el **Manual de Desarrollo Seguro**, que deben cumplir tanto el proveedor como la entidad.

- Utiliza herramientas como Jira para rastrear y registrar qué desarrollador realizó cada requisito, y SonarQube para realizar revisiones de código en busca de vulnerabilidades y buenas prácticas.

26.2.2 Frecuencia

La frecuencia dependerá de la criticidad y sensibilidad de los datos y servicios proporcionados en la nube, la provisión de información sobre la verificación de cumplimiento técnico se llevará a cabo de manera mensual.

26.2.3 Resultados

ELTHON CEO establece el **Instructivo Manejo de Vulnerabilidades con SonarQube** con los registros claros y detallados de los resultados de la verificación de cumplimiento técnico. Estos registros serán utilizados para evaluar el estado de cumplimiento y realizar mejoras continuas.

26.2.4 Acción correctiva

En caso de incumplimientos, ELTHON CEO aborda de manera oportuna y eficiente, tomando las medidas necesarias para corregir y mitigar los riesgos asociados, los cuales se comunican al personal involucrado a través de los medios de comunicación establecidos.

26.3 Informes de eventos de seguridad de la información

Elthon proporciona un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.

- Todos los trabajadores deberán informar al área de TI cualquier evento o situación no deseada que puede comprometer la confidencialidad, integridad o disponibilidad de la información, los sistemas, los activos de la información o los procesos relacionados, por los diferentes canales de comunicación habilitados.
- Todo el personal deberá seguir lo descrito en el **Subproceso de Gestión de Eventos** y **Subproceso de Gestión de Incidentes de SI** donde se establece las actividades para realizar el reporte de incidentes, eventos y vulnerabilidades de seguridad de la información que puedan tener impacto en el Software ELTHON
- El Jefe de TI establecerá la existencia de debilidades o amenazas que puedan afectar a la gestión de la información haciendo uso del **Registro de Debilidades e Incidentes de Seguridad de la información** correspondientes al Subproceso de Gestión de Incidentes de Seguridad de la Información

27. Política de Gestión de la configuración

Elthon establece, documenta, implementa, monitorea y revisa las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes a través de los Subprocesos de Tecnología y Seguridad de la Información.

28. Prevención de fuga de datos

Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

ELTHON asegurará la protección de la información en las redes y los recursos de tratamiento de la información, para lo cual establece:

29. Seguridad en redes

- Los controles de red se describen en la **Sección Capa de Seguridad del documento Infraestructura tecnológica y especificaciones técnicas del Software**, donde menciona el uso de:
  - Seguridad nativa que proporciona AZURE para los servicios de AZURE Spring Apps, SQL Server, REDIS, AZURE Blobs y Web Apps, significa que estos servicios ya cuentan con medidas de seguridad implementadas por defecto, como autenticación y encriptación de datos.
  - Seguridad de acceso en los sistemas Elthon, basada en perfiles y claves seguras. Esto significa que cada usuario tiene un perfil de acceso por entidad definido que le permite realizar únicamente las acciones necesarias para su trabajo el acceso a los módulos está limitado en el contrato de la entidad, evitando así que se acceda a información o funcionalidades que no le corresponden.
  - Se exige el cambio periódico de las claves para evitar el acceso no autorizado.
- ELTHON usará Azure Spring Apps que cumple con los estándares de seguridad y cumplimiento más estrictos para la seguridad de servicios de red.

30.1 Segregación en redes

ELTHON realizará la segregación de redes como una estrategia de seguridad fundamental para proteger la infraestructura de red, los datos, grupos de servicios de información, usuarios y sistemas de información.

Los grupos de servicios de información, los usuarios y los sistemas de información serán segregados en redes distintas según lo descrito en la sección de **Funcionalidades de seguridad de la arquitectura de Azure y Arquitectura Azure spring Apps (Microservicios de Elthon) del documento de Infraestructura y especificaciones tecnológicas del Software.**

30.2 Intercambio de información

ELTHON mantendrá la seguridad de la información que se transfiere dentro de la organización y con cualquier entidad externa a través de los siguientes lineamientos:

- No está permitido realizar envío de información mediante cualquier tipo de sistema de mensajería instantánea, el envío de información se realizará a través de correo electrónico con cuentas de empresa Gmail como la solución de mensajería interna principal.
- ELTHON utiliza como gestor de correos electrónicos la herramienta Outlook el cual implementa características de seguridad en la nube según lo descrito en la **Sección Mensajería Outlook con Gmail del documento Infraestructura tecnológica Especificaciones Técnicas Elthon.**
- La gestión del tratamiento de la información y los medios de transferencia para personas externas se realiza a través de la plataforma Owncloud según lo descrito en la sección Gestión de **Tratamiento de la Información del documento Infraestructura tecnológica y especificaciones técnicas del Software.**
- El Gerente General preparará y mantendrá **Acuerdos de Confidencialidad** con los trabajadores cuyas funciones involucren acceso a la información confidencial. Estos acuerdos se firmarán antes de que los trabajadores comiencen sus funciones y según lo descrito en las Políticas de Incorporación descritas en el **Manual de Talento Humano.**
- Los trabajadores deberán cumplir con los términos y condiciones del **Acuerdo de Confidencialidad y la Política de Clasificación de la Información**. El incumplimiento de lo descrito puede resultar en acciones disciplinarias, incluyendo la terminación del empleo y posibles acciones legales.
- El Jefe de Gestión de la Calidad archivará los Acuerdos de Confidencialidad en el File de cada trabajador.
- El Jefe de TI y/o Jefe de Gestión de la Calidad dará acceso al personal a la información necesaria según permisos de su perfil y cargo.

30.3 Política de uso de números empresariales

Esta política se aplica a todos los empleados y terceros que utilicen números empresariales o se involucren en comunicaciones relacionadas con la operación y gestión de la empresa.

1. El Jefe de Gestión de la Calidad registrará los números empresariales en el Inventario de Activos de la información, que incluye la clasificación, tipo, propietario, localización, descripción y valoración del activo en función de la confidencialidad, disponibilidad y la integridad.
2. Los números empresariales se considerarán información pública; sin embargo, los números de contacto e información de clientes serán de tipo confidencial y se manejarán conforme las Políticas de Seguridad de la Información.

3. Las comunicaciones que involucren números empresariales se considerarán información confidencial, y cualquier divulgación no autorizada estará sujeta a medidas disciplinarias establecidas en el Contrato.
4. Los trabajadores seguirán lo descrito en la **Política de Uso Aceptable de Activos de la Información** donde se establece las actividades permitidas y prohibidas para garantizar el cumplimiento con las políticas de seguridad de la información.
5. El Administrado, cuando sea necesario, podrá solicitar a la Operadora un registro de comunicaciones para garantizar la transparencia y responsabilidad del correcto uso de los números empresariales; y detectar o prevenir actividades no autorizadas, garantizando la seguridad de la información. El Jefe de Gestión de la Calidad conservará los registros de acuerdo con las políticas de retención de información.
6. La operadora no tendrá acceso a información confidencial, sensible o crítica, lo que significa que su papel no es fundamental para la seguridad de la información y la continuidad del negocio. En consecuencia, su inclusión como proveedor en el Sistema de Gestión no se considerará prioritaria. El enfoque se centrará en aquellos proveedores que representan riesgos más significativos para la seguridad de la información de la organización.
7. El Gerente General podrá solicitar contratos y acuerdos formales con la operadora que reflejen los requisitos de seguridad de la información que incluye cláusulas sobre la confidencialidad, protección de datos y medidas de seguridad específicas.

30. Política de actividades de seguimiento

ELTHON CEO monitorea redes, sistemas y aplicaciones para detectar comportamientos anómalos y que toma acciones ante posibles incidentes, a través de:

- Todos los mensajes de correo electrónico, tanto los enviados, como los recibidos pueden ser sujetos a monitoreo de forma esporádica por parte del Gerente General o su delegado. EL Jefe de TI, a pedido del Gerente General puede acceder al contenido de los mensajes para asegurar el cumplimiento de las medidas de seguridad.

- Registro y monitoreo de logs de seguridad.

- Registro de incidentes de seguridad de acuerdo a lo descrito en el **Subproceso de Gestión de Incidentes de Seguridad.**

31. Política uso de controles criptográficos

Elthon establece directrices y principios para el uso de controles criptográficos con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información. La implementación de los controles criptográficos se describe en el **Manual de Tecnología de la Información.**

La gestión de claves, su uso y protección se describen en el **Manual de Gestión de Manejo de contraseñas**.

32. Política de trabajo remoto (teletrabajo)

Elthon implementa las siguientes medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene.

Todo el personal del ELTHON CEO desempeña sus actividades bajo la modalidad de Teletrabajo de acuerdo con lo establecido en el **Contrato de trabajo**, por lo que Elthon CEO no dispone de infraestructura física para la ejecución de las actividades relacionadas al desarrollo y control del sistema del software.

ELTHON CEO entrega dispositivos de cómputo autorizados por la administración, a través del anexo 1 **"Acta de Entrega de activos"** en la cual se asignará el propietario del activo.

Los mecanismos de acceso seguro mediante contraseñas que el personal de ELTHON CEO deberá aplicar se describen en el **Manual de Gestión y Manejo de Contraseñas.**

Los trabajadores reconocen que toda la información a la que se puede tener acceso en el marco del contrato y de sus funciones, ya sea relacionada con el Software ELTHON o información, tienen carácter confidencial. Para lo cual el trabajador firma un **Acuerdo de confidencialidad vinculado al Manual de Talento Humano**; de esta forma, acepta no divulgar y mantener la más estricta confidencialidad respecto de dicha información. Además, el trabajador deberá seguir lo descrito en la **Política de uso aceptable de activos de la información** y en el **Instructivo para la configuración y mantenimiento de equipos.**

El trabajador cumplirá de forma obligatoria las Políticas de Seguridad de la información y Ley de Protección de Datos que establezca ELTHON CEO, es decir, no podrá reproducir, modificar, compartir, duplicar, copiar y/o hacer pública o divulgar a terceros la información sin previa autorización.

El trabajador no podrá manejar información o realizar actividades propias de ELTHON CEO fuera de los equipos otorgados para tal fin.

El trabajador no podrá hacer uso de dispositivos y medios de almacenamiento, seguirá lo descrito en el **Manual para la Gestión de medios de almacenamiento.**

El Jefe de TI deberá controlar las aplicaciones y recursos instalados en los equipos informáticos asignados a cada usuario, para lo cual dependerá del rol que desempeñen en la empresa. De forma adicional, las aplicaciones colaborativas y de teleconferencia permitidas para llevar a cabo reuniones con las entidades y empleados será a través de la plataforma Zoom o la que el Gerente General autorice para el efecto.

El Jefe de TI o su delegado deberá configurar la seguridad en los dispositivos informáticos para mantener el control del sistema operativo, antivirus, actualizaciones y entre otros aspectos de acceso y conexión de dispositivos.

El Jefe de TI o su delegado deberá monitorear de forma permanente las operaciones ejecutadas por el trabajador a través de la conexión VPN.

El Jefe de TI capacita al personal de ELTHON CEO en aspectos claves de la ciberseguridad para que sean capaces de entender el tema a profundidad, qué métodos se utilizan para los ataques y cómo protegerse con el fin de precautelar la seguridad de la información, para lo cual usará la **Matriz de Comunicaciones.**

El Gerente General establece como falta grave que da lugar a la terminación con justa causa de la relación laboral, cualquier uso ilegal o inadecuado de los recursos, cualquier conducta que atente contra normas de seguridad de la información, o de la utilización de la cuenta de correo electrónico, el acceso de la red de Internet y de cualquier medio dispuesto por la empresa para fines distintos a la labor para la cual fue contratado.

Una vez finalizadas las relaciones laborales, el trabajador realiza la entrega de los activos informáticos bajo su custodio al Gerente General o su delegado haciendo uso del **Anexo 2 Acta de recepción de activos**. En caso de existir daños, pérdidas o no devolución de los activos informáticos, el Gerente General tomará las medidas correctivas para salvaguardar dicho daño o pérdida a través de la liquidación del trabajador.

33. Política de preparación de las TIC para la continuidad del negocio

Elthon planifica, implementa, mantiene y prueba la preparación de las TIC en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC. Para lo cual se establece las siguientes fases para la continuidad de seguridad de la información:

34.1 Planificación

1. Identificar los activos y procesos críticos para determinar su impacto en caso de interrupción o pérdida, a través del **Subproceso Análisis del Impacto BIA.**
2. Realiza una evaluación de los riesgos y amenazas que podrían afectar la continuidad de la seguridad de la información como desastres naturales, fallas del sistema, ciberataques, etc.
3. Desarrolla estrategias y medidas de mitigación para reducir los riesgos identificados, a través del **Manual para la Evaluación y Tratamiento de Riesgos de Seguridad de la Información.**
4. Establece un **Plan de Continuidad del negocio** que incluye la implementación de sistemas de respaldo y recuperación, establecimiento de planes de contingencia, y la adopción de prácticas de seguridad robustas.

34.2 Implementación

1. Se ha documentado cómo adaptará e implementará sus procesos de seguridad en situaciones de interrupción, los **Subprocesos de Continuidad del Negocio** se encuentran en el Repositorio Documental.

2. Se realiza copias de seguridad, almacenamiento seguro de datos y pruebas de restauración descritos en el **Plan de Continuidad del Negocio.**
3. Se capacita al personal relacionado en las actividades de contingencia con el fin de mantener la confidencialidad, integridad y disponibilidad de la información durante interrupciones, haciendo uso de la **Matriz de comunicaciones.**
4. Realice un **Análisis de Impacto de Negocio (BIA**) para determinar los objetivos de Recuperación (RTO) y Puntos de Recuperación (RPO).
5. Establece estrategias y procedimientos de respuesta y recuperación TIC antes, durante y después de una interrupción en el **Plan de Continuidad del Negocio.**

34.3 Evaluación

El Jefe de TI comprobará los controles establecidos e implementados para gestionar de manera eficiente la continuidad de negocio a través de pruebas, los resultados se reportarán en el **Informe de Pruebas del Plan de Continuidad del Negocio vinculado al Subproceso de Gestión de pruebas del plan de continuidad del negocio**

El Gerente General gestionará la realización de auditorías internas y/o externas anuales o de acuerdo con la necesidad para evaluar el cumplimiento de las políticas y procedimientos de seguridad de la información en la continuidad del negocio.

Toda vez que ocurran incidentes de seguridad relevantes, éstos serán investigados y solucionados. El Jefe de TI documentará lo ocurrido y tomará medidas para evitar situaciones similares.

34.4 Redundancias

Los recursos para el tratamiento de la información serán implementados con el uso de Azure Blobs Storage que es un servicio de almacenamiento en la nube y permite almacenar grandes cantidades de descrito en el documento de **Infraestructura tecnológica y especificaciones técnicas del software.**

ELTHON CEO deberá realizar la restauración de la información almacenada únicamente cuando se presenten eventos críticos que representen un riesgo en la continuidad del negocio (eventos catastróficos). Se deberá considerar factores para restaurar y disponer de la información de las entidades, los cuales abarcan la naturaleza y el alcance de la información que se va a disponer, si hay o no metadatos asociados con la información y las características físicas del medio en el que se almacena la información.

El Jefe de TI realizará la restauración de la información con previa autorización del Administrador.

15.13 Política de seguridad de la información para el uso de la computación en la nube

ELTHON CEO define niveles aceptables de seguridad de la información, así como los activos de información que son directamente vinculantes en la administración software en la nube, en el cual se encuentra almacenada la información de la entidad.

El Jefe de TI es el responsable del acceso y gestión para preservar la confidencialidad y seguridad, así como de realizar la actualización del **Inventario de activos de la información** y la **Gestión de capacidades de activos de la Información - Servicios y base de datos en la nube**.

El Jefe de TI será el único usuario autorizado para el acceso a la nube para la administración de la información, de esta manera se prevé la presencia de eventos relacionados a incidentes de seguridad de la información.

La gestión de la información en la nube puede ser realizada bajo el enfoque de la entidad a través del acceso del ambiente de Administración, para lo cual la entidad podrá asignar un usuario privilegiado para la administración y generación de los registros almacenados en la nube, por medio de los LOGS de auditoría.

ELTHON CEO establece los niveles de seguridad de la información y las especificaciones del servicio con base en los acuerdos de nivel de servicio contratados con Microsoft Azure, así para garantizar que los servicios estén disponibles para las entidades y que cumplan normativas de seguridad; con ello las entidades aceptan dichos acuerdos de seguridad para la prestación del servicio del software ELTHON.

34. Política de Seguridad de la información en la gestión de proyectos

Implementar medidas de Seguridad de la Información en la Gestión de Proyectos utilizando la plataforma JIRA. Mediante la adopción de buenas prácticas y el cumplimiento de estándares de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información en todo el ciclo de vida del proyecto, de acuerdo con lo establecido en el **Manual de Seguridad de la información en la gestión de proyectos.**

35. Gestión de las vulnerabilidades técnicas

Elthon verifica el proceso de análisis automático del software con el uso de la herramienta SonarQube para identificar información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización a tales vulnerabilidades y tomar las medidas apropiadas según lo descrito en el **Instructivo Gestión de Vulnerabilidades técnicas.**

36. Lineamientos para el uso responsable de herramientas de Inteligencia Artificial

ELTHON reconoce que las herramientas de Inteligencia Artificial (IA) constituyen tecnologías emergentes que pueden contribuir al fortalecimiento de la productividad, innovación, eficiencia operativa y mejora continua de los procesos

En consecuencia, se autoriza su utilización como herramienta de apoyo para las actividades laborales, siempre que su uso se realice de manera responsable, ética y alineada con los objetivos estratégicos de la organización.

Para tal efecto, el trabajador deberá observar los siguientes lineamientos:

1. Utilizar herramientas de inteligencia artificial como mecanismo de apoyo para el análisis, generación de ideas, elaboración de borradores, automatización de tareas y otras actividades que contribuyan a la mejora del desempeño organizacional.
2. Mantener en todo momento la responsabilidad sobre los resultados obtenidos mediante herramientas de inteligencia artificial, asegurando la revisión, validación y aprobación humana del contenido antes de su utilización, comunicación o publicación.
3. Verificar la exactitud, pertinencia y confiabilidad de la información generada por herramientas de inteligencia artificial, evitando su uso automático o sin validación previa.
4. Utilizar las herramientas de inteligencia artificial de forma ética, responsable, evitando prácticas que puedan afectar la integridad, calidad, transparencia o reputación de la organización.
5. Proteger la información durante el uso de herramientas de inteligencia artificial, absteniéndose de incorporar información clasificada como confidencial o interna, cuya divulgación no haya sido previamente autorizada por la organización.
6. Promover el aprendizaje continuo y el desarrollo de competencias relacionadas con el uso seguro y eficiente de tecnologías emergentes, contribuyendo a la transformación digital y mejora continua de la organización.

ELTHON promoverá la adopción responsable de tecnologías emergentes, evaluando los riesgos, oportunidades y beneficios asociados a su utilización, con el fin de fortalecer la competitividad, innovación y sostenibilidad de sus operaciones.

37. Comunicación de la Política

El Jefe de TI en conjunto con el Jefe de Gestión de la Calidad se asegurarán de que todos los trabajadores de ELTHON CEO estén familiarizados con esta Política para lo cual harán uso de los diferentes canales de comunicación habilitados para tal fin y registrados en la **Matriz de comunicaciones**

38. Validez y gestión de documentos

El Jefe de TI en coordinación con el Jefe de Gestión de Calidad deben verificar que el documento esté vigente y actualizado.

Al evaluar la efectividad y adecuación de este documento, ELTHON CEO podrá revisar y/o reformar las políticas de seguridad y sus procedimientos basándose en los resultados de la auditoría interna o externa, o cuando se produzcan cambios significativos según los siguientes criterios:

- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del SGSI.
- Responsabilidades ambiguas para la implementación del SGSI.
- ELTHON CEO establece un compromiso de mejora continua del sistema de gestión de la seguridad de la información.

39. ANEXOS

Anexo 1 Acta de entrega de activos
Anexo 2 Acta de recepción de activos