Controles de Seguridad de la Información

(GES.1-POL)

Índice

1. Generalidades

1.1 Objetivo

El propósito de esta Política de Seguridad de la Información es proporcionar dirección en la gestión de la seguridad de la información, la cual en su más amplio sentido, se refiere al conjunto de medidas preventivas, detectivas y reactivas que permiten resguardar y proteger la información procurando la confidencialidad, la disponibilidad e integridad de los datos, en donde la primera se refiere a la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados, la disponibilidad se refiere a la característica de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones en el momento que se requiere, es decir, oportunamente y la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, y mantenerlos exactos y protegidos de ser manipulados o alterados por personas no autorizados.

Las políticas de seguridad contenidas en este documento han sido establecidas para cubrir información, datos, software, hardware y redes de comunicación utilizadas y operadas por Telikó.

El objetivo general de las "Políticas de Seguridad de la Información" es proporcionar orientación y dirección para la protección de la información, hardware, datos y programas de Telikó contra cualquier tipo de daño o destrucción accidental o deliberada. Asimismo, Telikó tiene la intención de garantizar que sus sistemas de información cumplan con las normas, leyes y reglamentos pertinentes.

Este documento de política establece el compromiso de gestión y establece el enfoque de Telikó para la gestión de la seguridad de la información y debe ser revisada y actualizada al menos anualmente, además de contar con el patrocinio y aprobación de la Dirección General.

Este documento proporciona el marco para garantizar la protección de los activos de Telikó para permitir el uso, acceso y divulgación de dicha información, así como la conformidad con las normas, leyes y reglamentos aplicables, a los que se refiere el Marco Normativo del documento “SAS.3-BAS Mecanismo Antisoborno”.

1.2 Alcance

Se aplicará a todos los empleados de Telikó, sus contratistas, sus consultores, clientes y otras personas afiliadas a terceros que tengan acceso a la información o activos de Telikó. A lo largo de este documento, la palabra "usuario" se utiliza para referirse colectivamente a todos estos individuos.

Este documento contiene un conjunto de políticas para la seguridad de la información propietaria de Telikó, la cual deberá ser aprobada por la alta dirección, dando seguimiento a la publicación y todas las partes interesadas.

El presente documento, tiene como propósito establecer las políticas generales y lineamientos específicos de seguridad de la información de Telikó, tomando como guía el estándar ISO/IEC 27001:2013, mismas que deberán cumplirse con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información de la empresa. Asimismo, esta política es difundida al personal interno, así como al personal externo para su conocimiento y cumplimiento.

1.3 Revisión

El Oficial de Seguridad de la Información en coordinación con la alta dirección, debe de realizar revisiones programadas a este documento o al generarse un cambio significativo para asegurar la eficiencia de las presentes políticas, garantizando que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos organizacionales.

2. Manifiesto de autorización

Por medio de la presente sección de firmas se pone de manifiesto que los que suscriben han leído, entendido y se encuentran de acuerdo con el contenido del presente documento —según su nivel de responsabilidad correspondiente (elaboración, revisión o autorización) —, adquiriendo con ello el compromiso de cumplir y hacer cumplir dicho contenido.

Hermilo Mendoza Bruno
Firma de autorización

Firmado digitalmente por Hermilo Mendoza Bruno
Fecha: 2021.03.10 13:21:49 -06'00'

3. Descripción de lineamientos.

3.1 Organización interna y contacto con autoridades

Planificar y realizar una auditoría interna del Sistema de Gestión por parte del responsable del sistema de gestión, así como determinar la frecuencia de las auditorías para adaptarlas a sus operaciones, considerando al menos una vez al año de manera obligatoria.

Debe ser asignado al rol de protección civil, un responsable como contacto con los grupos mencionados anteriormente para mantener relación con los responsables del edificio, asegurando cumplir las directrices de procesos y procedimientos internos, así como asegurar los medios de comunicación más ágiles posibles. Los medios de contacto deben ser el radio asignado, el medio de mensajería instantánea, así como el teléfono o la activación de las alarmas.

Se deben llevar a cabo sesiones periódicas de entrenamiento y concientización en temas de protección civil para el personal de Telikó.

3.2 Contacto con grupos de interés especial

Debe ser coordinado por los responsables de seguridad de la información y el equipo de cada uno de los seis servicios como sigue:

1. Anticipación de amenazas – José Martín Hernández Santiago
2. Cacería de amenazas – Fernando Guillermo Cruz Pérez
3. Monitoreo de seguridad - Hernán Montoya García
4. Gestión de Brechas/Forense - Fernando Guillermo Cruz Pérez
5. Respuesta a incidentes - Adán Plaza Mejía
6. Escaneo de Indicadores de Compromiso - José Martín Hernández Santiago

Asimismo, se debe considerar como parte del proceso de comunicación, la que debe mantenerse con grupos de interés especial, con previo análisis de la necesidad de contacto con estos grupos, entre los que se consideran.

1. Consultorías
2. Paladion networks (Fabricantes o partners).
3. Publicaciones especializadas.

En sus relaciones con los grupos de interés, los responsables asumen y promueven las siguientes responsabilidades básicas:

- Establece vías de comunicación con los Grupos de interés, con objeto de dar respuesta a sus necesidades y expectativas relacionadas con el negocio o servicio de los que forman parte.
- Mantener actualizado los contactos autorizados, matrices y medios de comunicación que consideren adecuados.

3.3 Seguridad de la información en la gestión de proyectos

La alta dirección debe de implementar los estándares funcionales, operativos y tecnológicos, que deben incorporarse en el desarrollo de proyectos, adquisición de servicios y componentes de tecnologías de información y comunicación.

Para todos los proyectos tanto internos como aquellos en los que se requiera del apoyo y soporte de un tercero, proveedor o contratista, se deben definir las especificaciones y requerimientos de seguridad de la información de acuerdo a su tipo y naturaleza así como integrar la identificación, análisis y tratamiento de riesgos, lo cual debe ser validado por el oficial de seguridad o la alta dirección para poder establecer y acordar con cada proveedor el acceso, tratamiento, almacenaje, comunicación, o provisión de componentes a la infraestructura de TI.

Referencias de la ISO 27001:2013

A.6.1.1

A.6.1.2

A.6.1.3

A.6.1.4

A.6.1.5

A.14.1.1

3.4 Dispositivos móviles

Los dispositivos móviles, que incluyen elementos como:

•Computadoras Portátiles
• Tabletas
•Tarjetas inteligentes
•Teléfonos inteligentes

Deben ser utilizados por los responsables quienes los tengan asignados y en uso, conforme a los siguientes lineamientos:

a. Establecer que sólo los dispositivos móviles proporcionados por Telikó deben utilizarse para guardar o procesar información clasificada en nombre de la organización.
b. Asignar los equipos previa autorización del jefe directo o la alta dirección y mantener un inventario de dispositivos y personal asignado, así como cartas de asignación y recepción.
c. Es responsabilidad del usuario, proteger los equipos que se le han asignado para el desempeño de sus funciones siguiendo las medidas de seguridad que a continuación se describen, como mínimo:

    - No exponer el equipo a condiciones de inseguridad física y/o ambiental, y en el caso de laptops, mantenerlas aseguradas con el candado proporcionado.
    - Proteger las claves de acceso que le han sido asignadas
    - No dejar el equipo desatendido en lugares públicos o en lugares donde pueda ser sustraído o dañado.

d. Asegurar que la pantalla del dispositivo se bloquee después de un corto período de tiempo de 10 minutos de no uso y requiera un código de acceso o contraseña para desbloquearlo. Las contraseñas utilizadas deben ser fuertes y difíciles de adivinar.
e. Se deben considerar, en los dispositivos que aplique, para conformar y utilizar la contraseña, al menos, los siguientes aspectos:
    - Al menos 8 caracteres de longitud
    - Utilizar letras y números
    - No utilizar datos de información personal

- Modificarla al menos cada 60 días
- No compartirla con nadie.
- No mantenerla escrita en un lugar visible.
- Utilizar diferentes contraseñas, definiendo una para cada sistema.

f. Se deben establecer sesiones seguras en los dispositivos que aplique, de tal forma que incluya una contraseña robusta en el dispositivo.
g. No eliminar ninguna marca de identificación en el dispositivo, como una etiqueta de activo de la empresa o un número de serie.
h. Asegurar que el dispositivo del tipo laptop, tablets, memoras externas, entre otros que aplique, esté guardado bajo llave y de que la llave no sea fácilmente accesible para cualquier persona, manteniéndose protegida por el usuario.
i. No añadir hardware periférico ni software al dispositivo sin la aprobación por escrito del departamento del al menos el CISO o alta dirección.
j. Mantener un respaldo, al menos semanalmente, de la información institucional.
k. Mantener medidas de protección criptográfica instalados en los equipos.

Referencias de la ISO 27001:2013

A.6.2.1

3.5 Teletrabajo

Este control se debe de aplicar a todos los sistemas, personas y procesos que constituyen los sistemas de información de la organización, incluidos los miembros de la junta directiva, directores, empleados, proveedores y otros terceros que tengan acceso a los sistemas de TELIKÓ S.A.P.I. de C.V.

Deben ser seguidas los siguientes lineamientos:

- Los equipos de la empresa, no deben ser conectados a redes inalámbricas públicas.
- Se debe mantener actualizado el antivirus.
- Se debe procurar mantener bloqueado los puertos para dispositivos externos, a menos que se cuente con la autorización del CISO y de la Alta Dirección.
- La configuración de los accesos en componentes involucrados para el teletrabajo (como: ruteadores, firewall, switches, etc.) debe ser endurecida de acuerdo con la política de seguridad de la organización.
- Minimizar la posibilidad de que otros dispositivos se conecten al enlace del usuario, restringiendo el acceso mediante la protección de un clave de red endurecida.
- Se utilizará una Red Privada Virtual (VPN) para asegurar que todo el tráfico de la red, desde el usuario hasta los servidores de la organización, esté cifrado de acuerdo con los estándares de la organización, las cuales deben ser preautorizadas por la alta dirección.
- Se debe utilizar un algoritmo de cifrado seguro.
- El área de TI debe proporcionar el software de Antivirus adecuado en caso de aplicar al sistema operativo correspondiente.
- Cada usuario es responsable de resguardar el equipo y/o material y asegurar que la actualización del servicio de antivirus se realice correctamente de manera periódica, en caso que no sea actualizado correctamente es su responsabilidad ponerse en contacto con el área de TI para su solución.
- Se debe de devolver el activo tecnológico cuando haya rescisión de contrato para el usuario antes de concluir la relación laboral con la empresa o sea solicitado por el área de TI.
- En caso de robo del equipo de cómputo o telecomunicaciones, el usuario debe presentar al área de Recursos Humanos, la constancia de hechos del Ministerio Público en la que señale marca, modelo y número de serie de cada uno de los equipos.

- Toda la información involucrada en los servicios del SOC que pasan por redes públicas debe protegerse de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas.

Referencias de la ISO 27001:2013

A.6.2.2

A.14.1.2

3.6 Concienciación y formación en seguridad de la información.

Se debe programar y gestionar las sesiones adecuadas de formación y sensibilización sobre la seguridad de la información por parte del oficial de seguridad, gerente de entrega de servicio y la alta dirección.

Se debe incluir en esta formación temas como los requisitos de seguridad de la organización, las políticas y procedimientos de seguridad de la organización, las amenazas y preocupaciones de seguridad, las responsabilidades legales y los controles empresariales, así como el uso correcto de las instalaciones de procesamiento de la información.

Se deben realizar programas anuales con el objetivo de mantener informados a los usuarios de las nuevas amenazas a la seguridad, así como de las actualizaciones o nuevos lineamientos en las políticas y procedimientos de seguridad de la información, además de resguardar todos los registros de asistencia o participación de los usuarios asistentes.

Referencias de la ISO 27001:2013

A.7.2.2

A.6.1.1

3.7 Seguridad de la información para el recurso humano

Se debe cumplir por parte de cualquier empleado todos los requisitos y reglas correspondientes al área de recursos humanos los cuales son dirigidos por Telikó y aplicables a todos los empleados de la organización sin excepción, relacionados más no limitados a temas como investigación de antecedentes, proceso disciplinario, reglamento interno de trabajo, cese o cambio de puesto de trabajo, seguridad en las relaciones con proveedores, requisitos de seguridad en contratos con terceros, cumplimiento de los requisitos legales y contractuales, legislación aplicable (ver documento del mecanismo de antisoborno), derechos de propiedad intelectual (DPI), protección de los registros de la organización, protección y privacidad de la información de carácter personal, entrevistas, examen de competencias, pruebas psicométricas, pruebas de confianza proceso de reclutamiento.

Para las bajas del personal o colaboradores, se deberá considerar llevar a cabo la trasferencia de conocimiento por un periodo determinado, con el objeto de que el personal que reemplaza al anterior cuente con los conocimientos mínimos necesarios para la ejecución de las tareas.

Referencias de la ISO 27001:2013

A.7.1.1

A.7.2.2
A.7.2.3
A.7.3.1
A.8.1.2
A.8.1.3
A.8.1.4
A.15.1
A.15.1.1
A.15.1.2
A.15.1.3
A.18.1
A.18.1.1
A.18.1.3
A.18.1.4

3.8 Uso aceptable de activos

Se debe de aplicar esta política a todos los sistemas, personas y procesos que constituyen los sistemas de información de la organización, incluidos los miembros de la junta directiva, directores, empleados, proveedores y otros terceros que tengan acceso a los sistemas de Telikó Solutions.

a. Todos los activos de información en formato digital u otros formatos soportados (papel, trípticos comerciales, flyer), podrán ser desde ficheros de todo tipo (texto, imagen, multimedia, bases de datos, etc.), pasando por los programas y aplicativos que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios; deben ser clasificados dependiendo del impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración, deben ser aplicando criterios de confidencialidad, integridad y disponibilidad para la correcta clasificación.

b. Se debe establecer un inventario de los activos de información disponibles propiedad de Telikó, considerando registrar aspectos tales como su tamaño, ubicación, servicios o departamentos a los que pertenecen y quiénes son sus responsables, el cual debe ser actualizado cada que se de alta, baja o cambio de un activo.

c. Se deben establecer funciones y responsabilidades para el adecuado manejo de los activos en lo que respecta a las actividades relacionadas a: recepción, asignación, salvaguarda, mantenimiento y control de los mismos, tanto en el procedimiento de gestión de activos, como en el formato o carta de asignación de activos. En el caso de los mantenimientos, estos deben ser planificados como mantenimientos preventivos y en su caso documentados cuando se apliquen de manera correctiva.

d. Se debe concientizar el uso adecuado, distribución, uso y conservación del activo. Para la administración de activos. Se debe contar con un responsable para la administración de una base de datos de la gestión de configuración (CMDB, por sus siglas en inglés).

e. Se deben aplicar los siguientes lineamientos de prohibición para cualquier persona que haga uso de los activos de la Organización Telikó:

- Prestar o transferir el activo a cualquier persona distinta a quien fue asignado.
- Enajenar el bien por cuenta propia
- Dañar o alterar sus características físicas o técnicas
- Poner en riesgo los recursos.
- Utilizar el activo a resguardo para tareas NO designadas por Telikó.
- Dejar el equipo desatendido o sin protección.

- Instalación, descarga y modificación de software no autorizado en activos de la empresa.
- El uso de las herramientas de trabajo como equipo de cómputo, internet, cuentas de correo, etc., asignados al colaborador son estrictamente para funciones de interés de Telikó y de ninguna manera para asuntos personales por lo que deben:
- Asumir toda responsabilidad en el uso de dispositivos de almacenamiento externo, así como la información que maneja dentro de ellos.
- Informar a su líder inmediato el acceso de equipo de cómputo personal al corporativo. En caso de requerir acceso a la red inalámbrica, solicitar vía correo electrónico autorización al líder inmediato con la justificación pertinente de la solicitud.
- Respetar la capacidad de almacenamiento del buzón, depurándola constantemente.
- Evitar compartir sus contraseñas y prestar su cuenta.
- Evitar realizar cualquiera de las siguientes actividades:
- 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).
- Enviar información secreta o confidencial 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 Director de Área.
- Difamar, abusar, acosar, hostigar y amenazar a personas por este medio.
- 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 o 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.
- 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.
- Falsificar o eliminar alguna atribución de autor, aviso legal 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, no es posible su exclusión.

Referencias de la ISO 27001:2013

A.8.1.1
A.8.1.2
A.8.1.3
A.8.1.4
A.12.5.1
A.12.6.2

3.9 Clasificación de la información

Se debe entender que la información es un activo crítico para Telikó y sus clientes. Todos debemos estar comprometidos en asegurar el cumplimiento de los estándares de la industria y las mejoras prácticas

Todos los documentos y registros deben estar clasificados en términos de seguridad de la información de acuerdo con el tipo de información que estos contengan. Los criterios de clasificación se basan en el nivel de impacto que puede tener Telikó por incidentes que afecten la confidencialidad, integridad y disponibilidad de los documentos y registros; dichos criterios se describen a continuación:

Criterios de Confidencialidad.

Se refiere al impacto generado en Telikó, por la divulgación no autorizada de información del SGI y se relaciona directamente con los derechos de acceso de “lectura”. Para esta categoría se definen los siguientes niveles:

- **Público**. La divulgación no autorizada de este tipo de información no representa impacto alguno para la organización. Cualquier persona interna o externa puede conocerla.
- **Uso Interno**. La divulgación no autorizada de este tipo de información puede representar impactos bajos sobre la imagen de la organización, sin incurrir en incumplimiento de leyes o regulaciones nacionales y/o extranjeras. Sólo personal interno se puede conocerla.
- **Confidencial**. La divulgación no autorizada de este tipo de información puede representar multas importantes por incumplimiento de leyes o regulaciones nacionales y/o extranjeras, imagen adversa de la organización manejable de cara a clientes, proveedores y competidores, pérdida de ventaja competitiva. Sólo personal explícitamente autorizado puede conocerla.
- **Secreto**. La divulgación no autorizada de este tipo de información puede representar multas severas por incumplimiento de leyes o regulaciones nacionales y/o extranjeras, imagen adversa de la organización no manejable de cara a clientes, proveedores y competidores, o pérdida de ventaja competitiva a gran escala. Sólo personal de Alta Dirección y personal explícitamente autorizado por esta última puede conocerla.

Criterios de Integridad.

Se refiere al impacto para Telikó por la modificación no autorizada de información del SGI y se relaciona directamente con los derechos de acceso de “escritura”. Para esta categoría se definen los siguientes niveles:

- **Tolerable.** La modificación no autorizada (intencional o accidental) de este tipo de información no afecta lo suficiente como para evitar que esta pueda seguir siendo utilizada sin producir errores en el o los procesos involucrados.
- **Indispensable**. La modificación no autorizada (intencional o accidental) de este tipo de información afecta lo suficiente como para evitar que esta pueda seguir siendo utilizada ya que puede producir errores y afectar el resultado por su uso.

Criterios de Disponibilidad.

Se refiere a los impactos por no tener acceso a la información en el momento en que esta sea requerida y se relaciona directamente con los derechos de acceso de “borrado”. Para esta categoría se definen los siguientes niveles:

- **No Crítica**. La no disponibilidad de este tipo de información no representa impacto alguno para la organización al no ser un registro vital o recurso mínimo necesario para un proceso de negocio. Sólo personal autorizado puede tener acceso a ella.

- **Crítica.** La no disponibilidad de este tipo de información sí representa impactos para la organización por ser un registro vital o recurso mínimo necesario para un proceso crítico del negocio. Sólo personal explícitamente autorizado puede tener acceso a ella. Para esta clasificación es importante tomar en cuenta que independientemente del formato en el que se encuentre (físico o electrónico) se debe conservar una copia en físico del mismo, esto como medida de control en caso de un desastre.

3.10 Etiquetado de la información.

Se debe de confirmar por la alta dirección, y los encargados del sistema de gestión toda la información clasificada. Se debe contener la leyenda de “clasificación” de conformidad con las disposiciones aplicables.

La información deberá ser etiquetada para los casos en que ésta sea secreta o confidencial.

3.11 Protección y manejo de la información.

Deben ser promovidos mecanismos de protección de información, la cual dicha responsabilidad recae en la alta dirección, el oficial de seguridad, el gerente de entrega de servicio, el director de operaciones y cualquier responsable de personal.

Se debe contar con un control de acceso para todo activo de información protegido según su clasificación, debe contar con un control de acceso, donde se establezca qué personas son las autorizadas para el manejo de la información en el activo asignado.

Todo el personal de Telikó debe estar obligado a no revelar a terceras personas la información que conozcan por el ejercicio de sus funciones, por lo que están obligados a mantenerla confidencial y privada para evitar su divulgación.

Se debe establecer que los usuarios de acuerdo con sus funciones podrán trabajar y hacer uso de la información de Telikó en los activos de información asignados y resguardar la versión final.

Deben implementarse clausulas en la relación con proveedores y clientes que sean adecuadas para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales en los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado.

Referencias de la ISO 27001:2013

A.8.2.1
A.8.2.2
A.8.2.3
A.18.1.2

3.12 Política de Control de Acceso

Se debe establecer el acceso a las instalaciones de Telikó de acuerdo con los siguientes lineamientos:

a. Contar con huella biométrica registrad y autorizada para poder acceder a las instalaciones de Telikó, o en su caso con tarjeta asignada previamente registrada y autorizada o tocar de manera mecánica para que la recepcionista valide s se permite o no el acceso al vestíbulo.

b. En caso de ser visitante y acceder previo a que la puerta sea abierta de manera mecánica por la recepcionista, se deberá registrar en la bitácora manual el registro, con al menos fecha, nombre completo, a quién visita y con qué propósito y el visitante será acompañad por la recepcionista o alguna otra persona de Telikó. En caso de no ser visitante, el empleado accederá por la segunda perta con la misma huella o tarjeta previamente registrada y autorizada.

c. Se debe administrar el ingreso a las instalaciones con base en las siguientes definiciones:

   Empleados SOC: aquellos que laboren dentro de las instalaciones de Telikó; deberán portar identificación de forma visible, contar con registro biométrico para acceder a través de las puertas de ingreso y para abrir la puerta de entrada al centro de operaciones de seguridad. De igual manera, las instalaciones de Telikó cuentan con un SITE, al cual solo podrá acceder quien cuente con el debido registro biométrico de huella dactilar para poder acceder a este sitio en particular.

   Empleados Staff Telikó: aquellos que laboren dentro de las instalaciones, realizando actividades dentro de las oficinas de Telikó; deberán de contar con registro biométrico para poder entrar y salir de las instalaciones.

   Contratistas y Proveedores: son todos aquellos que acuden a las instalaciones de forma temporal para realizar actividades previamente programadas. Estos deberán registrarse con alguna identificación oficial a la entrada del edificio donde se encuentran las oficinas de Telikó, al momento de ingresar a las instalaciones de Telikó deberán de nuevo registrarse como segundo filtro de entrada; estos deberán ser escoltados dentro de las instalaciones al entrar y salir de las mismas.

3.13 Visitantes generales al SOC

Se debe considerar visitante todo aquel personal que no labore dentro de las instalaciones de Telikó, siendo estos proveedores, contratistas, representativos de otras empresas, entre otros.

Se debe realizar el registro en el primer filtro de entrada, donde anotarán sus datos:

- Nombre
- Razón de la visita: actividad a la que acude
- Fecha y hora
- Firma

Después de completar los formatos de acceso, se dará acceso a las instalaciones y se les dirigirá un espacio designado.

Se debe acompañar a los visitantes durante su estancia al interior de las oficinas.

3.14 Salida de activos fuera de las instalaciones de Telikó.

Se deberá registrar cualquier activo que salga de las instalaciones de Telikó en el formato correspondiente,

Se deberá anotar al menos en el formato la siguiente información:

- Nombre y tipo de activo
- Número de serie (de tenerlo)
- Fecha de salda
- Nombre y firma de quien autoriza la salida del activo
- Nombre y firma de quien solicita la salida del activo
- Motivo de la salida
- Destino del activo

3.15 Control y revisión de la provisión de servicios

Se debe contar con algún formato o registro para verificar que la entrega del servicio sea correcta en tiempo y forma conforme a lo definido y requerido formalmente, ya sea en acuerdo interno o en contratos.

Se debe garantizar en todos los requerimientos de servicios, se incluyan las especificaciones de la entrega, características de bienes o servicios requeridos, entregables, fechas de entrega, responsable de la recepción y de la entrega, condiciones de pago y entrega, niveles de servicio, revisiones y validaciones, así como el plan y calendario de trabajo y actividades. Asimismo, en caso de que requiere tener acceso a la red, sistemas o aplicaciones de Telikó, se deben obtener las autorizaciones correspondientes.

De lo anterior, en cada una de las entregas, se debe generar la documentación que soporte la entrega de los bienes y servicios, la cual debe ser revisada y validada por los responsables de la recepción por parte de Telikó, debiendo firmar de recibido y visto bueno, previo a efectuar los pagos correspondientes, en caso de tratarse de bienes y servicios adquiridos, y para los casos de servicios internos, antes de declarar una entrega y liberación, se deberá contar con la documentación de las entregas conforme a lo planeado con las aprobaciones de que fueron realizadas en tiempo y forma.

Se debe evaluar y validar el cumplimiento de los niveles de servicio acordados, a fin de garantizarlos, y generar la documentación que lo acredite, y en su caso, se identifiquen desviaciones o incidencias, para poder determinar las penalizaciones correspondientes en caso de aplicar.

Asimismo, se deben definir mecanismos por medio de los cuales se considere la planificación de la evaluación de la entrega de bienes y servicios.

3.16 Seguridad física.

Se deberán seguir las siguientes reglas:

a. Utilizar perímetros de seguridad (barreras tales como muros, accesos controlados por guardias de seguridad o personal encargado de registrar a los visitantes con el fin de proteger las áreas que contienen información y medios de procesamiento de información.
b. Definir claramente los perímetros de seguridad y los controles de cada uno de ellos dependiendo de los requerimientos de seguridad de los activos dentro del mismo.
c. Contar con un área de recepción, una persona dedicada para la aplicación de controles de acceso físico a las oficinas de Telikó.
d. Contar con un sistema de monitoreo en puntos estratégicos de las instalaciones para registrar la actividad desarrollada, así como el monitoreo de zonas.
e. Establecer una zona segura para las operaciones del SOC o resguardo de los activos críticos de Telikó. Un área segura puede ser una oficina que puede ser cerrada con llave, o algún sistema de seguridad como control de acceso biométrico. Debe contar con registros del personal al que se otorgue acceso a las áreas definidas como seguras y registrar entrada y salida de visitantes.
f. Se deben requerir a todos los proveedores, usuarios de tercero y todos los visitantes llevar alguna forma de identificación visible e inmediatamente se debe notificar al oficial de seguridad si se encuentran algunos visitantes no acompañados o si alguno no lleve una identificación visible.
g. Contar con protección contra amenazas externas y ambientales también contra la protección física, el daño del fuego, terremoto, siniestro y otras formas de desastre natural.
h. Dentro de las instalaciones de Telikó se establece que queda prohibido el fumar y consumir bebidas alcohólicas o cualquier sustancia psicotrópica.
i. Se debe definir espacios específicos para consumir alimentos y estos deben ser distintos a las áreas destinadas para realizar labores de trabajo.
j. El equipo de cómputo y dispositivos móviles que se utilicen para trabajar, no deben retirarse sin autorización previa del usuario o custodio del activo.

k. Se pueden realizar revisiones no planeadas para detectar el retiro de propiedad, dispositivos de grabación no-autorizados, armas, etc., y evitar su ingreso al local. Toda revisión no planeada debe ser llevadas a cabo en concordancia con la legislación y regulaciones relevantes. Solo el oficial de seguridad puede llevar a cabo revisiones no planeadas con autorización de la alta dirección.
l. Se deben identificar y designarse un área de carga y descarga en el área cercana a la puerta de emergencia de las oficinas, donde personal externo puede tener acceso y debe encontrarse aislado de activos críticos, en las cuales el acceso debe ser controlado, y se debe contar con un registro de quienes acceden a ella, así como de los materiales, equipos, activos entre otros, que salen y entran de éstas. En caso de que el área designada no se encuentre disponible, la recepción principal de las oficinas, se utilizará como área de carga o descarga.

3.17 Protección contra amenazas externas y del medio ambiente

La política de protección del medio ambiente debe cumplir los siguientes puntos:

a. Existir disposiciones adecuadas para la detección y el control de incendios, entre las que se incluyen extintores de incendios deben instalarse en lugares fácilmente visibles y accesibles.
b. Existir personal capacitado en el uso de extintores de incendios.
c. Limpiar periódicamente el suelo, las paredes, los armarios de almacenamiento y los equipos informáticos.
d. Contar con un sistema de alimentación ininterrumpida para todas las instalaciones críticas que procesan datos que son críticos para el funcionamiento de Telikó.
e. Los reguladores de voltaje instalados para protegerse de las fluctuaciones de potencia.

f. Instalar disyuntores de capacidad apropiada para proteger el hardware contra el aumento del voltaje de alimentación.

Referencias de la ISO 27001:2013

A.9.1.1
A.9.1.2
A.11.1.1
A.11.1.2
A.11.1.3
A.11.1.4
A.11.1.5
A.11.1.6

3.18 Gestión de acceso a usuario.

Registros y baja de usuarios.

Se debe tener un registro de todas las altas, bajas y cambios a los aplicativos y servicios de Telikó.

Se debe eliminar o deshabilitar todas las cuentas de acceso tan pronto como la necesidad de la misma haya terminado. Esto puede incluir lo siguiente:

a. Usuario que abandona la organización - El acceso se inhabilitará dentro de las 24 horas laborables siguientes a la notificación de salida del empleado por parte de Recursos Humanos o en caso de así requerirlo debe ser realizado de manera inmediata una vez autorizado por la alta dirección.
b. Proveedor que completa una tarea - El acceso se inhabilitará tan pronto como se reciba la notificación del equipo en cuestión al término de la tarea.

c. Acceso por pruebas - El acceso se inhabilitará y eliminará tan pronto como finalice la actividad de prueba.

Provisión de acceso a usuarios.

a. Todas las altas, bajas y cambios de usuarios deben ser previamente aprobadas por el jefe inmediato, y en el caso de cuentas privilegiadas se debe contar con la aprobación del encarga de seguridad de la información.
b. Las cuentas de usuario o ID deben ser únicas y utilizarse de manera individual sin ser compartidas, así como utilizar una contraseña robusta que cumple con lo definido en la política.
c. Debe estar restringido el acceso a las utilidades del sistema sólo a los administradores o usuarios autorizados.
d. Se deben permitir el acceso a todos los usuarios conectados al dominio de Telikó solo desde una puerta de enlace central
e. Se debe obtener la aprobación por escrito con el visto bueno del dueño del servicio o información y el responsable del área delimitando correctamente el alcance de acceso a la red de Telikó para proveedores
f. Se debe controlar el acceso remoto a las redes de Telikó mediante un mecanismo de autenticación adecuado; proporcionar acceso VPN o HTTPS para los usuarios autorizados.
g. Todo acceso mediante conexión remota (VPN) debe contar con el visto bueno del departamento de TI y el responsable del SOC o la alta dirección.

Gestión de privilegios de acceso y gestión de información.

a. Se deben mantener limitados los privilegios de usuario solamente a los servicios necesarios para el desempeño de las tareas asignadas y este se debe de controlar por el departamento de TI de Telikó.
b. La información secreta de autenticación es controlada por el departamento de TI de Telikó.
c. Se debe revisar por el departamento de TI de Telikó los derechos de acceso de usuario en intervalos de tiempo definidos, los cuales deben corresponder con las matrices de perfiles.
d. Se debe contar con registros de accesos y actividades ejecutadas en los sistemas y aplicativos, los cuales deben mantenerse en un lugar seguro y con acceso restringido únicamente al personal facultado.
e. Se debe considerar que los registros no deben ser modificados ni eliminados bajo ninguna circunstancia.
f. Se debe llevar a cabo la recertificación de usuarios y privilegios asignados, al menos anualmente, a fin de validar y actualizar la información.

Referencias de la ISO 27001:2013

A.9.2.1
A.9.2.2
A.9.2.3
A.9.2.4
A.9.2.5
A.9.2.6

3.19 Responsabilidades del usuario.

Se debe establecer términos y condiciones para el acceso a información confidencial tales como que:

a. Cada usuario debe contar con un user id.
b. Todo el personal de Telikó es responsable del uso de contraseñas, las cuales son confidenciales e intransferibles.

c. Para hacer uso de la infraestructura tecnológica, el usuario debe aceptar los términos y condiciones de la Política de Uso Aceptable de Aplicativos/servicios.
d. Cambiar por el usuario la contraseña inicial inmediatamente después de que le fue asignada al sistema o aplicativo.
e. Tener acceso a los aplicativos solo a los usuarios autorizados, con la cuenta asignada para tal efecto; en ningún caso deben acceder usando una cuenta diferente.

Referencias de la ISO 27001:2013

A.9.3.1

3.20 Control de acceso a sistemas y aplicaciones y herramientas de gestión

Todo el personal de Telikó es responsable de su contraseña, la cual es confidencial y debe mantenerse secreta. Para hacer uso de la infraestructura tecnológica, los usuarios deben aceptar los términos y condiciones de la Política de Uso Aceptable de Aplicativos.

El usuario debe cambiar la contraseña inicial, después de que le fue asignada al sistema o aplicativo, mismo que debe estar configurado para que esto sea de forma automática.

La contraseña no debe mostrarse al inicio de sesión ni ser transmitida en texto claro.

Deben registrarse los intentos de acceso exitosos y fallidos.

Se deben tener acceso a los aplicativos los usuarios autorizados, con la cuenta asignada para tal efecto; en ningún caso deben acceder usando una cuenta diferente.

Referencias de la ISO 27001:2013

A.9.4.1
A.9.4.2
A.9.4.3
A.9.4.4

3.21 Cifrado

Se debe asegurar el uso adecuado del cifrado para proteger la autenticidad e integridad de la información.

Las claves criptográficas creadas para los diferentes servicios en los casos que apliquen deben ser resguardadas y almacenadas de manera segura.

No deben revelarse a consultores, contratistas, o terceros, las claves de cifrado a menos que se haya obtenido autorización del Gerente de Sistemas y Director de Administración.

Nunca deben emplear programas utilitarios de cifrado que soliciten que el usuario ingrese una contraseña o clave de cifrado.

3.22 Controles criptográficos.

Se debe asegurar mecanismos que permitan cifrar información, gestionar claves y certificados, desde su generación, almacenamiento, archivo, recuperación, distribución retiro y destrucción.

Se debe asignar a un encargado o encargados el resguardo de certificados, quienes son del área de Tecnologías.

Se debe asegurar el cifrado de los equipos portátiles como laptops que pertenezcan a Telikó.

Para el servicio de correo electrónico se debe garantizar la seguridad y privacidad a los usuarios a través de una conexión web (HTTPS) seguras o transferencia segura de datos (canal cifrado) para el tráfico de información sensible.

Los datos corporativos confidenciales en redes no protegidas se deben asegurar mediante la autenticación y la confidencialidad mutuas 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 (en inglés Virtual Private Network) con algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) o SEAL.

Referencias de la ISO 27001:2013

A.10.1.1
A.10.1.2
A.18.1.5

3.23 Políticas de seguridad en operaciones.

Se debe documentar los procedimientos de operación y los procesos de todas las áreas de Telikó en manuales de operación de acuerdo con lo establecido en los objetivos y lineamientos del Telikó.

Se debe responsabilizar al dueño de sistema de gestión y cada responsable para documentar procedimientos y de contar con memorias técnicas para la administración

Par la administración de cambios, debe existir un ticket en el sistema de administración y se debe contar con el visto bueno del responsable del aplicativo o responsable funcional con nivel jerárquico inferior inmediato.

Se debe considerar la evaluación de los aspectos de seguridad cuando se presente un cambio de alto impacto o significativo

Referencias de la ISO 27001:2013

A.12.1.1
A.12.1.2
A.12.1.3

3.24 Procedimientos Seguros de Inicio de Sesión

Para asegurar que los inicios de sesión de los usuarios a los sistemas y aplicaciones son seguros, se debe restringir y controlar los accesos, vigilando lo siguiente:

- Se deberá identificar y verificar la identidad de los colaboradores a través de su usuario y contraseña.
- Solo los usuarios autorizados por el área de Sistemas podrán acceder a los equipos o servidores.
- Se deberá 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.

- Se debe 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 5 minutos y al volver a utilizarse deberá solicitar de nuevo la contraseña de ingreso al usuario.
- Deben generarse los registros de auditoría que contengan excepciones y eventos relativos a la seguridad.
- Deben mantenerse durante un periodo de tiempo definido para poder acceder a futuras investigaciones o monitoreo de control de accesos.
- Se debe 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.
- Debe existir un método de sincronización de relojes.
- 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 utilizar un protocolo de Internet para sincronizar los relojes de los sistemas informáticos (NTP).
- El acceso a servicios de red, aplicaciones y sistemas de información, debe ser a través de usuarios y contraseñas.

3.25 Protección contra código malicioso

Se debe asegurar que todos los equipos de escritorio, móviles (laptops) y servidores utilizados en la red de la Institución, tengan instalado software antivirus mantenerlo actualizado, tanto en versión como en definición de firmas.

Se debe cumplir con una configuración base de parches de seguridad de cada sistema operativo y realizar por parte del equipo de TI una revisión periódica para la gestión de vulnerabilidades detectadas, la definición de planes de acción y su seguimiento.

Referencias de la ISO 27001:2013

A.12.2.1
A.12.4.4
A.12.6.1

3.26 Respaldo y borrado de información

Se debe responsabilizar a todos los mandos medios y superiores identificar la información que sea sensible para la operación de su área de acuerdo con su criticidad y deben dar aviso a la Dirección.

Se debe respaldar periódicamente toda la información (configuraciones, logs, file systems, bases de datos, etc.) que resida en los sistemas.

Se debe revisar y validar periódicamente la información respaldada, se deben almacenar los respaldos generados en un sitio seguro.

Se debe responsabilizar a cada usuario por el respaldo de su información y datos dentro del activo asignado.

Se debe ejecutar el procedimiento de borrado seguro para los equipos que sean eliminados, desechados o reasignados, asimismo, la información contenida en estos medios, debe ser respalda y resguardarse en un medio alterno de manera segura, es decir en un sitio seguro, a fin de asegurar su disponibilidad y preferentemente estos se mantendrán protegidos con mecanismos de cifrado.

Se debe proteger, registrar y revisar de manera periódica las actividades de los usuarios y administradores de cada sistema y debe ser reportado cualquier irregularidad a la alta dirección.

Referencias de la ISO 27001:2013

A.12.3.1
A.12.4.1
A.12.4.2
A.12.4.3

3.27 Seguridad de las comunicaciones.

Se debe responsabilizar al área de TI o responsable de sistemas el diseño, implementación, establecimiento, contratación, administración, mantenimiento y soporte de las redes de voz y datos y de toda la infraestructura de comunicaciones que las soportan.

Telikó debe contar con la infraestructura necesaria para la protección de la información y sus activos tecnológicos, así como, para el monitoreo y detección oportuna de incidentes de seguridad.

Se deben implementar mecanismos para el uso del servicio de internet en la empresa, la cual debe contar con herramientas de seguridad y de filtrado de contenido, que permitan la segmentación de navegación conforme a la operación de las áreas.

Debe estar clasificada la zona de seguridad en caso de existir, basadas en funciones, tipo de datos y requerimientos de acceso a los espacios de almacenamiento.

Se deben utilizar mecanismos de autenticación y cifrado para la protección de la comunicación inalámbrica.

Se debe asegurar que los segmentos de red que transmitan información confidencial utilicen una cifrado robusto.

Se debe cuidar el cumplimiento de los requerimientos de seguridad mínimos para cada elemento de la red.

Referencias de la ISO 27001:2013

A.13.1.1
A.13.1.2
A.13.1.3

3.28 Manejo de medios.

Los medios extraíbles como son discos duros externos y memorias, deben ser asignados previa autorización del jefe inmediato, y deben ser protegidos por medio de mecanismos que salvaguarden la información contenida en estos, y en caso de que sean reasignados o eliminados, deben pasar por un procedimiento de borrado seguro. La información contenida en estos medios, debe resguardarse en un medio alterno a fin de asegurar su disponibilidad y preferentemente estos se mantendrán protegidos con mecanismos de cifrado.

Se mantendrá un registro de la asignación de los medios extraíbles para mantener su control, el cual será responsabilidad del encargado de seguridad de la información.

En el caso de requerir la transferencia de medios físicos, estos deben ser transportados de manera segura, y deben ser asignados a un responsable custodio de su transporte procurando las especificaciones del fabricante, quien debe vigilar que la protección del empaque sea segura y lo mantenga protegido.

Referencias de la ISO 27001:2013

A.8.3.1
A.8.3.2
A.8.3.3

3.29 Política de escritorio limpio y seguridad de los equipos

Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles (memorias USB, SD, micro SD, Discos duros externos, CD, DVD), y una política de pantalla limpia en las instalaciones de Telikó.

Es responsabilidad de cada usuario la protección de los sistemas de información a su cargo; con el fin de minimizar la exposición de la información sensible; los sistemas de información y elementos de procesamiento deben asegurar tomar las medidas pertinentes para proteger la información, los datos (en físico y digital) y los sistemas de información. Estas medidas se nombran a continuación:

1. Guardar documentos críticos, tabletas, celulares, portátiles (laptops) en los cajones bajo llave, cuando no los estén utilizando o en un área segura.
2. No publicar o dejar a la vista, documentos o datos críticos como: nombres de usuario, contraseñas, direcciones IP, contratos, números de cuentas, nombre de clientes, archivos de propiedad intelectual, datos personales y/o cualquier información importante.
3. De haber ausencias de su lugar de trabajo, por tiempo prolongado, se debe asegurar que la información usada quede fuera del alcance de terceras personas.
4. Está prohibido tener sustancias o líquidos en el escritorio, ya que estos pueden dañar los equipos, así como la documentación.
5. No dejar dispositivos de respaldo de información, como USB, discos duros externos, CD, DVD, etc., para el fácil acceso de cualquier persona.
6. No escribir contraseñas ni otros datos sensibles en papeles o documentos que queden a la vista.
7. El usuario es responsable de cerrar su sesión de trabajo y dejar el equipo bloqueado, cuando no esté en uso.
8. Proteger los equipos contra fallos de alimentación y alteraciones causadas por fallos en los suministros, Se debe asegurar una corriente regulada para minimizar riesgo en caso de ser posible.
9. Solo retirar equipos de la empresa con previa autorización del jefe directo del colaborador y debe asegurarse el correcto cuidado del activo fuera de las instalaciones.
10. Se debe proporcionar el activo cuando sea requerido por el área de TI, jefe directo o encargado de seguridad de la información, mantenimientos programados con el fin de asegurar la disponibilidad e integridad del activo.
11. Los equipos deben colocarse en lugares seguros para protegerlos de robos o daños.
12. Todos los equipos deben someterse a un mantenimiento cuando sea requerido.
13. Deben existir controles para proteger el equipo de los campos electromagnéticos, altas temperaturas, humedad, fluctuaciones de potencia, etc.
14. El mantenimiento realizado en los equipos por parte de terceros debe contar con controles adecuados para proteger los datos que contienen de robos o fugas.
15. Asegúrese de que tiene un acuerdo de nivel de servicio y un contrato con el proveedor para el mantenimiento preventivo
16. Se debe seguir el proceso de reutilización o eliminación de equipo y/o proceso de destrucción de información impresa. para confirmar la correcta eliminación de información.
17. Nunca deje documentación impresa en la impresora ni deseche información confidencial en la basura sin antes asegurarte que pueda ser ilegible.

18. La impresora debe mantener un método de autenticación para su uso restringiendo el acceso a los documentos impresos.
19. Los cables de las líneas y redes de telecomunicaciones para las instalaciones de procesamiento de información deben protegerse de la interceptación no autorizada y de los daños.
20. Los cables deben tenderse en los espacios del edificio. Todo el cableado debe realizarse con cables plano o cruzado de una categoría mayor a 5.
21. Los cables de alimentación estarán separados de los cables de comunicaciones para evitar interferencias.
22. Toda la documentación física que contenga datos e información relevante, deben mantenerse bajo resguardo en cajones o gavetas con llave, lejos del daño por fuego, húmedas, robo, destrucción accidental, entre otros. Asimismo, no debe mantenerse al alcance del acceso de personal no autorizado.
23. Cualquier documento físico debe apegarse a las políticas descritas en este documento, siendo responsabilidad del usuario el correcto resguardo e información cuidando la CIA de seguridad de la información

Referencias de la ISO 27001:2013

A.11.2.1
A.11.2.2
A.11.2.3
A.11.2.4
A.11.2.5
A.11.2.6
A.11.2.7
A.11.2.8
A.11.2.9

3.30 Desarrollo Seguro

Los siguientes lineamientos se deben de aplicar a todos los sistemas desarrollados o cuyo código fuente sea adquirido por TELIKÓ S.A.P.I. de C.V:

a) Debe realizarse una evaluación de riesgo como parte del ciclo de desarrollo de software para asegurar que todas las partes comprendan plenamente las implicaciones que este pudiera llegar a tener.

b) Se deben definir mecanismos por medio de los cuales se determinen las reglas y lineamientos para el desarrollo de software, en caso de llevar a cabo esta actividad.

c) Para el desarrollo de software se deben utilizan procedimientos formales de control de cambios, así como definir la participación del responsable de seguridad y los requerimientos específicos de seguridad.

d) Toda la información, aplicación o software creado o implementado por el personal es propiedad de la empresa.

e) Se deben implementar controles de seguridad apropiados para las aplicaciones utilizadas.

f) Se debe asignar un responsable involucrado en la revisión del correcto funcionamiento de los nuevos desarrollos y los cambios a los ya existente, en particular de los relacionados a las aplicaciones consideradas como críticas. Así mismo los cambios debe ser registrados, evaluados, priorizados, categorizados, conforme a un proceso establecido para el control de cambios, que debe

considerar los diferentes tipos de cambios, especificando las particularidades para los cambios de emergencia.

g) Se debe restringir y controlar el acceso al código fuente de las aplicaciones informáticas o programas que busquen violar la seguridad de la información.

h) El ambiente de pruebas deberá estar separado al menos lógicamente de los demás ambientes y se deberán ejecutar pruebas integrales y pruebas de seguridad para asegurar los impactos hacia otros sistemas con interface. Se deberá restringir el uso de datos e información de los ambientes productivos en los de pruebas a menos que se tenga la debida autorización por personal facultado dueño de dicha información. El control de acceso para las cuentas de usuario y administración de los ambientes de pruebas deben restringir que dichas cuentas tengan acceso a los ambientes productivos.

i) En caso de requerir desarrollo subcontratado (outsourcing) se debe designar un responsable para la gestión, supervisión, monitoreo y control de las actividades del personal externo.

j) Solo personal autorizado debe tener acceso a los ambientes de prueba/desarrollo según su rol, siempre y cuando se mantenga una segregación entre éstos.

k) En la fase de prueba o posterior a un cambio crítico se deben ejecutar pruebas por medio de la cuales se determine y evalúe el impacto a las operaciones o funcionalidad.

l) Se deben ejecutar y documentar pruebas de aceptación, así como definir criterios relacionados para los nuevos sistemas, actualizaciones y nuevas versiones.

Referencias de la ISO 27001:2013

A.9.4.5
A.12.1.4
A.14.2.1
A.14.2.2
A.14.2.3
A.14.2.4
A.14.2.5
A.14.2.6
A.14.2.7
A.14.2.8
A.14.2.9
A.14.3.1

3.31 Intercambio de información

Cuando se intercambie información utilizando cualquier medio de comunicación para transferir información se debe tener en cuenta los siguientes elementos:

1. Cuando utilice un teléfono móvil en un lugar público, asegúrese de que ninguna persona no autorizada escuche información confidencial, así como de utilizar canales de comunicación no seguros.
2. Seguir los controles sobre el intercambio de información o software mediante el uso de correo electrónico e Internet descritos en este documento.
3. Se deben configurar reglas de acceso y navegación en el firewall.
4. Los usuarios se asegurarán de que ninguna información interna o confidencial sea compartida

5. Los datos sensibles al cliente y de identificación personal se intercambiarán utilizando procedimientos seguros como el cifrado SSL y el túnel VPN seguro.
6. Todos los correos electrónicos que salgan de TELIKÓ a cualquier otra entidad deben tener responsivas de correo ("Este mensaje de correo electrónico puede contener información confidencial, privada o legalmente privilegiada").
7. Las cuentas de correo electrónico que se almacenen en el equipo del usuario deben estar protegidos con una contraseña.
8. Los usuarios deben informar inmediatamente al equipo de TI de cualquier actividad sospechosa o problema que observen con el sistema de correo electrónico.
9. La información confidencial enviada por correo debe estar encriptada o protegida por contraseña.
10. Los usuarios de correo electrónico deben asegurarse de que se utilicen protocolos de comunicación seguros para acceder al servidor de correo electrónico.
11. Toda la información identificada en la categoría de “confidencial” o “secreto” debe garantizarse la protección y divulgación de esta información de manera responsable y dentro de los límites autorizados.
12. Se debe cumplir con los elementos adicionales que sean incluidos en un acuerdo de confidencialidad o no divulgación celebradas con clientes, proveedores o asociados.

Referencias de la ISO 27001:2013

A.13.2.1
A.13.2.2
A.13.2.3
A.13.2.4

3 Roles y responsabilidades.

El rol de oficial de seguridad, como único rol de seguridad de la información tiene a su cargo al menos las siguientes responsabilidades.

1. Participar en la definición y verificar la implementación y continuo cumplimiento de las políticas y procedimientos de seguridad.

2. Elaborar el Plan de Seguridad, el cual deberá contener, por cada proyecto que se defina, nombre del proyecto, objetivo, alcance, fechas de inicio y fin, áreas involucradas. Asimismo, todos los proyectos deberán incluir la definición de especificaciones de seguridad de la información, las cuales deben ser validadas por el oficial de seguridad.

3. Mantenerse informado sobre noticias, actualizaciones y aspectos en materia de seguridad de la información, así como, recibir información oportuna y tener contactos especializados en seguridad, así como enriquecer la información y genera un mejor contexto de tendencias, noticias de los sectores, a nivel geográficos, empresariales, a través de las notificaciones de ISACA, de la herramienta MDR, el SANS Storm, entre otros.

4. Informar en su caso, los incidentes de seguridad graves, a los terceros interesados, clientes, y entidades regulatorias como la policía cibernética.

5. Autorizar y vigilar la asignación de los accesos a la Infraestructura Tecnológica, incluyendo aquellos de Usuarios de la Infraestructura Tecnológica con mayores privilegios, utilizados para ingresar a la información recibida, generada, almacenada, procesada o transmitida conforme a lo definido en las

políticas y procedimientos de seguridad de la información. La autorización y ejecución no podrán realizarse por la misma persona.

6. Para el caso de los accesos por excepción, tales como usuarios de ambientes de desarrollo con acceso a ambientes de producción y con accesos por eventos de contingencia, contar con un registro que contenga la siguiente información: nombre del Usuario de la Infraestructura Tecnológica, aplicación asociada, ambiente, motivo de la excepción y fecha de inicio y fin de la asignación.

7. Verificar que al menos una vez al año o antes en caso de eventos o Incidentes de Seguridad de la Información, se revisen las actividades y asignación de perfiles (matrices de perfiles) y permisos de acceso en los diferentes componentes de la Infraestructura Tecnológica, incluyendo aquellas del personal técnico que cuente con altos privilegios, tales como administración de sistemas operativos y de bases de datos, con el fin de detectar actividades inusuales o no autorizadas.

8. Aprobar y verificar el cumplimiento de las medidas que se hayan adoptado para subsanar deficiencias detectadas con motivo de los hallazgos tanto de auditoría interna como externa relacionada con la Infraestructura Tecnológica y de seguridad de la información.

9. Apoyar al equipo de respuesta a incidentes de seguridad, para la detección y respuesta de Incidentes de Seguridad de la Información, debiendo formar parte de este.

10. Informar a la alta dirección la verificación del Incidente de Seguridad de la Información que se trate, respecto de las acciones tomadas y del seguimiento a las medidas para prevenir o evitar que se presenten nuevamente los mencionados incidentes.

11. Informar del estado de gestión de la seguridad de la información cuando sea necesario.

12. Mantener comunicación con el responsable de riesgos quien podría ocupar el rol de backup del oficial de seguridad.

13. Actualizar la política, procedimientos, estándares de configuración e instrucciones de trabajo cada año.

4 Cumplimiento.

En caso de incumplimiento total o parcial de las políticas descritas en este documento, será responsabilidad del encargado de seguridad de la información en coordinación con la alta dirección, determinar y aplicar las medidas necesarias, considerando la gravedad de la falta, las cuales podrán ir desde un acta administrativa, una amonestación verbal, hasta un tema penal y rescisión de contrato.

Todo el personal sin excepción debe informar al encargado de seguridad, cualquier incumplimiento que identifique, o reportarlo como un incidente de seguridad, indicando al menos, fecha, tipo de incumplimiento y personal involucrado, a fin de que el encargado de seguridad analice la situación y determine acciones.

Asimismo, las excepciones deben documentarse y justificarse, además de ser comunicadas y validadas por el responsable de seguridad.

Anexo 1 Términos y definiciones

Para los efectos del presente documento, se entenderá por:

Término	Definición
Activo de información	Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
Amenaza	Cualquier evento, circunstancia humana, natural o tecnológica que tiene el potencial de causar algún tipo de daño a los activos de información de la Institución.
Confidencialidad	La característica o propiedad de la información, de poder ser conocida únicamente por individuos autorizados.
Disponibilidad	La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.
Impacto	Grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.
Incidente	Es la afectación o interrupción a los activos de TI, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.
Integridad	La acción de mantener la exactitud y corrección de la información.
Riesgo	La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TI, las infraestructuras críticas o los activos de información.
Roles	Conjunto de responsabilidades, actividades y autorizaciones que se otorga a una persona o equipo. Una persona o equipo pueden tener varios roles.
Seguridad de la información	La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
Software libre	Programa de computación cuya licencia garantiza al usuario acceso al código fuente del programa y lo autoriza a ejecutarlo con cualquier propósito, modificarlo y redistribuirlo el programa original como sus modificaciones en las mismas condiciones de licenciamiento acordadas al programa original, sin tener que pagar regalías a los desarrolladores previos.
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, otras propiedades, como la autenticidad, rendición de cuentas, no repudio, y confiabilidad también pueden estar involucradas.
Vulnerabilidades	Debilidades que pueden ser aprovechadas por una amenaza, es decir, a las debilidades de los activos o sus medidas de protección que facilitan el éxito de una amenaza potencial. En el contexto de los riesgos de la seguridad de la información, solamente las consecuencias negativas (pérdidas) son consideradas para transferir el riesgo.

Control de Cambios

Fecha	Alcance del cambio	Descripción del cambio	Versión
20/02/2021	Actualización del contenido del documento	Se ajustan los temas de segregación de ambientes de desarrollo y pruebas. Se ajusta el tema de cambio. Se agregan los activos con datos e información en físico y su manejo. Se agregan cambios de emergencia.	1.2
17/04/2020	Actualización al Contenido del documento	Se Incluyeron controles para el dominio 14 - Desarrollo. Se modifica la sección de generalidades. Se Agregan mecanismos de manera más específica. Se Agregan controles para cableado. Se Incluyen todos los controles criptográficos. Se agregan características para NTP. Se Detallan funciones de seguridad y revisión de la Dirección. Se Detalla la política de uso de impresora e intercambio de información. Se Detalla el uso de redes, correo electrónico seguro y protocolo seguro.	1.1
15/01/2020	Actualización al Contenido del documento	Creación del Documento	1.0