

NO-UTE-SI-0001-06

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

VIGENCIA: 20/02/2020

Revisado por:	Aprobado por:
Comité de Seguridad de Información	Directorio
FECHA: 20/02/2020	FECHA: 20/02/2020

ÍNDICE

TRÁMITE Y REVISIONES	4
0.1.- TRÁMITE	4
0.2.- REVISIONES.....	4
1.- OBJETO Y CAMPO DE APLICACIÓN	4
1.1.- VIGENCIA.....	4
1.2.- INVOLUCRADAS/OS Y PARTES INTERESADAS.....	4
2.- REFERENCIAS NORMATIVAS.....	5
2.1.- MARCOS LEGALES QUE APLICAN A ESTA POLÍTICA.....	5
2.2.- ESTÁNDARES EXTERNOS	5
2.3.- RESOLUCIONES	5
3.- DEFINICIONES / ABREVIATURAS / SÍMBOLOS.....	5
3.1.- DEFINICIONES	5
3.2.- ABREVIATURAS.....	9
3.3.- SÍMBOLOS	10
4.- DESARROLLO.....	10
4.1.- POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	10
4.1.1.- OBJETIVO	10
4.1.2.- ALCANCE.....	10
4.1.3.- RESPONSABILIDADES.....	10
4.1.4.- DESCRIPCIÓN.....	11
4.2.- POLÍTICA DE DISPOSITIVOS MÓVILES, TELETRABAJO Y BYOD	11
4.2.1.- OBJETIVO	11
4.2.2.- ALCANCE.....	11
4.2.3.- RESPONSABILIDADES.....	11
4.2.4.- DESCRIPCIÓN.....	12
4.3.- POLÍTICA DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.....	13
4.3.1.- OBJETIVO	13
4.3.2.- ALCANCE.....	13
4.3.3.- RESPONSABILIDADES.....	13
4.3.4.- DESCRIPCIÓN.....	14
4.4.- POLÍTICA DE GESTION DE ACTIVOS DE INFORMACIÓN	14
4.4.1.- OBJETIVO	14
4.4.2.- ALCANCE.....	14
4.4.3.- RESPONSABILIDADES.....	14
4.4.4.- DESCRIPCIÓN.....	15
4.5.- POLÍTICA CONTROL DE ACCESO	17
4.5.1.- OBJETIVO	17
4.5.2.- ALCANCE.....	17
4.5.3.- RESPONSABILIDADES.....	17
4.5.4.- DESCRIPCIÓN.....	18
4.6.- POLÍTICA CRIPTOGRAFÍA	19
4.6.1.- OBJETIVO	19
4.6.2.- ALCANCE.....	19
4.6.3.- RESPONSABILIDADES.....	19
4.6.4.- DESCRIPCIÓN.....	20
4.7.- POLÍTICA SEGURIDAD FISICA Y DEL ENTORNO.....	20

4.7.1.-	OBJETIVO	20
4.7.2.-	ALCANCE	20
4.7.3.-	RESPONSABILIDADES	20
4.7.4.-	DESCRIPCIÓN	21
4.8.-	POLÍTICA SEGURIDAD DE LAS OPERACIONES	22
4.8.1.-	OBJETIVO	22
4.8.2.-	ALCANCE	22
4.8.3.-	RESPONSABILIDADES	22
4.8.4.-	DESCRIPCIÓN	22
4.9.-	POLÍTICA SEGURIDAD DE LAS COMUNICACIONES	23
4.9.1.-	OBJETIVO	23
4.9.2.-	ALCANCE	23
4.9.3.-	RESPONSABILIDADES	24
4.9.4.-	DESCRIPCIÓN	24
4.10.-	POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	24
4.10.1.-	OBJETIVO	24
4.10.2.-	ALCANCE	24
4.10.3.-	RESPONSABILIDADES	25
4.10.4.-	DESCRIPCIÓN	25
4.11.-	POLÍTICA DE RELACIONES CON LOS PROVEEDORES Y TERCERAS PARTES	26
4.11.1.-	OBJETIVO	26
4.11.2.-	ALCANCE	26
4.11.3.-	RESPONSABILIDADES	26
4.11.4.-	DESCRIPCIÓN	26
4.12.-	POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	27
4.12.1.-	OBJETIVO	27
4.12.2.-	RESPONSABILIDADES	27
4.12.3.-	ALCANCE	27
4.12.4.-	DESCRIPCIÓN	27
4.13.-	POLÍTICA DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	28
4.13.1.-	OBJETIVO	28
4.13.2.-	ALCANCE	28
4.13.3.-	RESPONSABILIDADES	28
4.13.4.-	DESCRIPCIÓN	28
4.14.-	POLÍTICA DE CUMPLIMIENTO	29
4.14.1.-	OBJETIVO	29
4.14.2.-	ALCANCE	29
4.14.3.-	RESPONSABILIDADES	29
4.14.4.-	DESCRIPCIÓN	29
5.-	REGISTROS	30
6.-	INDICADORES	30
7.-	ANEXOS	30

TRÁMITE Y REVISIONES

0.1.- TRÁMITE

El documento “Política de Seguridad de la Información” es elaborado por el Comité de Seguridad de la Información y aprobado por Directorio.

0.2.- REVISIONES

Fecha	N° de versión	Elaborado por	Aprobado por	Párrafos modificados	Surge de:
2019-01-31	06	Comité de Seguridad de la Información	Directorio	Se re estructura todo el documento	Revisión trianual de las políticas de seguridad de la información

1.- OBJETO Y CAMPO DE APLICACIÓN

El objeto de la presente política es proteger la información y preservar su integridad, confidencialidad y disponibilidad contra posibles amenazas.

Es de aplicación en todo el ámbito de la Administración Nacional de Usinas y Trasmisiones Eléctricas (UTE). Ataño a todos los usuarios que tengan acceso a activos de información de UTE.

1.1.- VIGENCIA

La presente Norma entra en vigencia a partir de su publicación, establecida en la carátula y pie de página.

Las políticas serán revisadas con una periodicidad no mayor a tres años, con el objetivo de incorporar los cambios derivados de los avances tecnológicos y las modificaciones en la estructura organizativa de UTE, las regulaciones y normas externas.

1.2.- INVOLUCRADAS/OS Y PARTES INTERESADAS

Todos los usuarios y terceras partes deben estar en conocimiento, cumplir y hacer cumplir la presente Política de Seguridad de la Información publicada y comunicada por el equipo de Seguridad de la información de TIC (SEG).

Para todo apartamiento, excepción o salvedad a estas políticas es necesario:

- Documentar, justificar y autorizar según corresponda.
- Realizar un análisis y gestión de riesgos.
- En caso que aplique, realizar análisis de vulnerabilidades.
- Establecer controles compensatorios.

2.- REFERENCIAS NORMATIVAS

2.1.- MARCOS LEGALES QUE APLICAN A ESTA POLÍTICA

- Ley N° 18.331 – Protección de Datos Personales y Acción de “HABEAS DATA”
- Ley N° 18.381 – Ley Sobre el derecho de acceso a la información pública
- Ley N° 18.600 – Documento electrónico y firma electrónica
- Ley N° 18.627 – Mercados de Valores
- Ley N° 19.061 – Transito y seguridad vial en el territorio nacional

2.2.- ESTÁNDARES EXTERNOS

- ISO/IEC 27000: Tecnología de la Información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Visión general y vocabulario.
- ISO/IEC 27001: Tecnología de la Información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Requisitos

2.3.- RESOLUCIONES

- R 97.-1554, 6 de agosto de 1997 (Compromisos u obligaciones a nombre de UTE)
- R 18.-687, 22 de marzo de 2018 (Tabla de Clasificación de Datos de UTE)
- R 13.-1964, 5 de diciembre de 2013 (Definición de Información Privilegiada de UTE)

3.- DEFINICIONES / ABREVIATURAS / SÍMBOLOS

3.1.- DEFINICIONES

Activo de información: Cualquier información o elemento relacionado con el tratamiento de la misma que tenga valor para la organización. La información puede ser almacenada en muchas formas, incluyendo: formato digital (por ejemplo, archivos de datos almacenados en medios ópticos o electrónicos), medio material (por ejemplo, en papel), así como información no representada, en forma de conocimiento de los empleados.

Ejemplos de activos de información:

- a) Información: bases de datos, archivos de datos, documentación, contratos, acuerdos.
- b) Software: sistemas de información (propios o subcontratados), software de base (sistemas operativos, manejadores de base de datos, etc.), herramientas de desarrollo, y utilitarios.
- c) Físicos: equipamiento de computación, equipamiento de comunicaciones, medios de almacenamiento de información removibles y otros equipamientos.
- d) Instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua y gas, etc.
- e) Servicios: servicios de cómputo y de comunicaciones, servicios generales (calefacción, iluminación, energía, y aire acondicionado, etc.).
- f) Intangibles personales: conocimientos, calificaciones, habilidades y experiencia del usuario.

Amenaza: Causa potencial de un incidente de seguridad de la información, que puede dar lugar a daños en un sistema de información.

Área Segura: Instalaciones que:

- Contienen información no pública.
- Procesan información.

Asegurar: Acciones para el mejor cumplimiento de objetivos o controles establecidos.

BYOD: Dispositivos portátiles personales para llevar a cabo tareas del trabajo y/o conectarse a la red y/o recursos de UTE.

Certificado Digital: Archivo electrónico cuyo objetivo es identificar inequívocamente a su poseedor (usuario o sitio web), emitido por Proveedores de Servicios de Certificación.

Ciclo de Vida de Certificados: Etapas de un certificado digital desde su creación hasta su eliminación (emisión, renovación y revocación).

Cifrado: Conversión de datos de un formato legible a un formato codificado, donde solo se pueden leer o procesar después de haberlos descifrado.

Clasificación de la Información:

La información en UTE se clasifica como:

- **Dato Personal:** Información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. Según Ley 18.331 art 4 numeral D.
- **Dato Sensible:** Datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual sensible Ley 18.331 art. 4 numeral E.
- **Información Pública:** Es toda la información que emana, produce, esté en posesión de, o bajo el control de UTE, con independencia del soporte en el que esté contenida, salvo las excepciones o secretos establecidos por Ley, así como la información reservada o confidencial.
- **Información Reservada:** Aquella cuya difusión pueda:
 - Comprometer la seguridad pública o la defensa nacional.
 - Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de reservado al Estado uruguayo.
 - Dañar la estabilidad financiera, económica o monetaria del país.
 - Poner en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona.
 - Suponer una pérdida de ventajas competitivas para el sujeto obligado o pueda dañar su proceso de producción.
 - Desproteger descubrimientos científicos, tecnológicos o culturales desarrollados o en poder de los sujetos obligados.
- **Información Confidencial:** Se considera información confidencial:
 - Aquella entregada en tal carácter a los sujetos obligados siempre que:
 1. Refiera al patrimonio de la persona.
 2. Comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica que pudiera ser útil para un competidor.
 3. Esté amparada por una cláusula contractual de confidencialidad.
 - Los datos personales que requieran previo consentimiento informado (Ley Nº 18.381, arts. 9 y 10).
- **Información Privilegiada:** Se considera información privilegiada (de acuerdo al Art. 6 de la Ley Nº 18.627).
 - La información de un emisor – o de los valores que emita – obtenida en razón del cargo o posición, inclusive la transmitida por un cliente en relación a sus propias

órdenes pendientes, que no se ha hecho pública y que, de hacerse pública, podría influir sensiblemente sobre la cotización de los valores emitidos o sus derivados.

- Asimismo, se considera información privilegiada la que se tiene de las operaciones de transmisión de la titularidad a realizar por un inversionista en el mercado de valores a fin de obtener ventaja con la negociación de valores.

La información reservada, confidencial y/o privilegiada:

- Será protegida contra la divulgación no autorizada a través de cualquier medio físico o electrónico.
- Si fuera transportada o transmitida por un medio de comunicación inseguro (Internet, intranet, cartuchos, medios, etc.) contará con protecciones adicionales (cifrado, contratos, precintos, etc.).
- Será explícitamente identificada como tal y será destruida al final de su vida útil (considerando los plazos precaucionales definidos por UTE).
- En caso de ser necesario imprimirse se realizará de acuerdo a un procedimiento que se ajuste a la normativa vigente.

Constituyen uso indebido de la información privilegiada (Art. 6 de Ley Nº 18.627) las acciones que se definen a continuación:

- Revelar o confiar información privilegiada antes de que se divulgue al mercado.
- Recomendar la realización de operaciones con valores sobre los que se tiene información privilegiada.
- Adquirir o enajenar – para sí o para terceros, directa o indirectamente – valores sobre los cuales posea información privilegiada.
- En general, valerse de información privilegiada directa o indirectamente, en beneficio propio o de terceros.

Por R 13.-1964 de fecha 5 de diciembre de 2013 toda la información clasificada como privilegiada será tratada como reservada hasta su desclasificación.

Comité de Seguridad de la Información: Grupo interdisciplinario liderado por la Gerencia de Tecnologías de la Información y Comunicaciones creado por R 07.- 456 de fecha 19 de abril de 2007, cuya principal responsabilidad es velar por el cumplimiento de las Políticas de Seguridad y en el futuro elaborar las nuevas versiones de las mismas. Por R 11.-462 de fecha 14 de abril de 2011 se modifica el nombre del Comité de Seguridad Informática a Comité de Seguridad de la Información.

El Comité de Seguridad de la Información está conformado por representantes de las Gerencias Generación (Hidráulica, Térmica y Eólica), Transmisión, Distribución, Comercial, Planificación, Secretaría Técnica, Despacho de Cargas, Asesoría Técnico Jurídica, Secretaría General y Tecnologías de la Información y Comunicaciones.

El mismo es responsable de:

- Identificar y analizar las normas relativas a la seguridad de la información incluidas en Leyes, Decretos y Reglamentaciones de organismos nacionales e internacionales que sean de aplicación obligatoria a los efectos de asesorar en su cumplimiento a las unidades según corresponda.
- Elaborar las nuevas versiones de las Políticas de Seguridad de la Información.
- Velar por el cumplimiento de las Políticas de Seguridad de la Información.
- Difundir el Compromiso de Confidencialidad Corporativo a todas las áreas y la obligatoriedad de su utilización.

Compromiso de Confidencialidad Corporativo: Contrato o acuerdo de confidencialidad que se firma cuando se va a tener conocimiento de información que requiere discreción y se trata de evitar que las partes implicadas puedan divulgar o utilizar dicha información para fines diferentes a los establecidos en el contrato.

Confidencialidad: Propiedad que determina que la información esté disponible y sea revelada únicamente a individuos, entidades o procesos autorizados.

Criptografía: Método de cifrado para lograr que un mensaje no pueda ser leído por un tercero sin autorización, es decir, asegurar la confidencialidad de la información.

Disponibilidad: Propiedad de la información de ser accesible y utilizable por solicitud de individuos, entidades o procesos autorizados.

Dispositivos Móviles – Dispositivos Transportables: Todo equipo que proporcione portabilidad y posea capacidad de almacenamiento y/o procesamiento de información, con conexión permanente o intermitente a la red. Por ejemplo: Notebooks, Laptop o PDA, Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Cintas, Pendrive o similar, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

Evento de Seguridad de la Información: Ocurrencia identificada de un estado de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de controles, o una situación previamente desconocida que pueda ser relevante para la seguridad.

Firma Digital: Es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

- Identificar al firmante de manera inequívoca.
- Asegurar la integridad del documento firmado.
- Asegurar que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación.
- Asegurar el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento.

Incidente de Seguridad de la Información: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de UTE y amenazar la seguridad de la información.

Integridad: Propiedad de exactitud y completitud de la información, manteniendo los datos libres de modificaciones no autorizadas

Medio: Refiere a medios de almacenamiento lógico, físico, o cualquier otro medio tangible que oficie de contenedor de información.

Necesidad de Saber, Necesidad de Hacer: Principio de seguridad de la información que indica el otorgamiento de permisos de acceso a recursos e información con los mínimos privilegios necesarios para cumplir con las tareas asignadas.

Normativa Vigente Incidente: Disposiciones (jurídica, contractual, etc) que aplican al caso concreto.

Oposición de Intereses: Operación realizada con la intervención de varios actores con diferentes funciones de control.

Procesos Críticos: Aquellos que en caso de falla afectan la satisfacción del cliente y exponen a UTE a pérdidas económicas, de imagen y demandas legales.

Responsable de Activo de Información: Usuario responsable de asegurar que el activo de información bajo su responsabilidad está protegido y seguro.

Riesgo: El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a UTE.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Separación de Funciones: Principio que establece la segregación de tareas para reducir el riesgo de que un usuario y/o terceras partes puedan cometer errores o fraudes.

Sistema de Información: Infraestructura de tecnología, procesos, aplicaciones de negocios y software, disponibles a los usuarios para el desarrollo de las tareas.

Técnico Representante de la Unidad Usaria de los Servicios o de la Compra: Es el encargado de informar sobre la admisibilidad técnica de las ofertas.

Terceras Partes: Personas que brindan o reciben servicios de UTE, proveedores, socios de negocio y clientes de servicios de consultoría.

UARI: Unidad Administradora de Recursos de Información: Unidad responsable de administrar equipos o sistemas que manejan información relevante para la Empresa, ya sean sistemas informáticos, redes de datos, equipos para aplicaciones industriales y/o administrativas.

Unidad: Unidad organizativa definida en SAP.

Usuarios: Funcionarios (en cualquier carácter), personas físicas o jurídicas (consultores, personal contratado, proveedores y terceras partes) que hacen uso de información y/o activos de información de UTE.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

3.2.- ABREVIATURAS

AYS: División Abastecimientos y Servicios

AUD: División Auditoría Interna

BYOD: Bring Your Own Device - Trae Tu Propio Dispositivo

CAU: Centro de Atención de Usuarios

CERTuy: Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay

GER: Gerencia General

HUM: División Gestión Humana

LET: Área Asesoría Técnica Jurídica

PDA: Asistente Personal Digital

PSI: Políticas de Seguridad de la Información de UTE

SAP: Systems, Applications, Products in Data Processing: Sistema informático que le permite a las empresas administrar sus recursos humanos, financieros-contables, productivos, logísticos y más.

SEG: Seguridad de la Información de TIC

SGSI: Sistema de Gestión de la Seguridad de la Información

SUSI: Sistema de Usuarios. Sistema que permite gestionar los permisos de los usuarios en los diferentes sistemas de información corporativos de UTE.

TIC: División Tecnología de la información y Telecomunicaciones

UTE: Administración Nacional De Usinas y Trasmisiones Eléctricas

UARI: Unidad administradora de recursos de información

- **U-DIS-ACD:** UARI Automatización y Control de Distribución
- **U-DNC:** UARI Despacho Nacional de Cargas
- **U-GEN-EOL:** UARI Generación Eólica
- **U-GEN-HID:** UARI Generación Hidráulica
- **U-GEN-TER:** UARI Generación Térmica
- **U-PEE:** UARI Planificación de la Explotación y Estudio
- **U-SEC:** UARI Secretaría General
- **U-TIC:** UARI Tecnologías de la Información y Telecomunicaciones
- **U-TRA:** UARI Transmisión

3.3.- SÍMBOLOS

No aplica.

4.- DESARROLLO

4.1.- POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1.1.- OBJETIVO

Organización interna.

Establecer un marco de referencia de gestión de la implementación y operación de la seguridad de la información, para la distribución de funciones y responsabilidades como parte fundamental de los objetivos y actividades de UTE.

4.1.2.- ALCANCE

Todos los usuarios de UTE.

4.1.3.- RESPONSABILIDADES

SEG

Evaluar periódicamente la arquitectura de seguridad, de forma de proveer el marco para proteger los recursos de tecnología y la información accesible a través de estos.

Implementar los estándares, normas y procedimientos de control necesarios para asegurar el cumplimiento de las políticas de seguridad de la información definidas.

Establecer los mecanismos para notificar la Política de Seguridad de la Información y sus modificaciones a todos los usuarios de UTE.

Actuar como coordinador en temas de seguridad de la información entre todas las unidades de UTE.

Monitorear e inspeccionar todo uso de sus recursos de tecnología de información y ante situaciones irregulares iniciar investigaciones administrativas.

Ante la detección de una conducta por parte de un usuario que interfiera con la normal operación de los sistemas de información o no cumpla con las presentes Políticas de Seguridad, SEG se reserva el derecho de bloquear preventivamente los permisos de acceso del mismo.

Responsable de Activo de Información:

Asegurar que los usuarios, cuya actividad afecte directa o indirectamente a los activos de información bajo su responsabilidad:

- Cumplan con las Políticas de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.
- Firmen el Compromiso de Confidencialidad Corporativo si corresponde, previo a:
 - Ejecución de contratos relacionados con empresas proveedoras de personal y/o de bienes y servicios a UTE.
 - Tramitar permisos de acceso a activos de información.

Resguardar los registros de Compromiso de Confidencialidad Corporativo firmados por terceras partes.

UARI

Controlar la gestión técnica de roles y separación de funciones sobre los activos de información.

4.1.4.- DESCRIPCIÓN

Roles y Responsabilidades para la Seguridad de la Información: Definir y asignar las responsabilidades sobre los activos de información.

Separación de funciones: Restringir las funciones y áreas de responsabilidad en conflicto, sobre la base de los principios: “necesidad de hacer”, “necesidad de saber”, “separación de funciones” y “oposición de intereses” para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

Contacto con las Autoridades: Mantener contactos apropiados con las autoridades pertinentes.

Contacto con Grupos de Interés Especial: Mantener contactos apropiados con grupos de interés y asociaciones profesionales especializadas en seguridad.

Seguridad de la Información en la Gestión de Proyectos: Abordar la seguridad de la información en la gestión de proyectos, independientemente del tipo de proyecto.

4.2.- POLÍTICA DE DISPOSITIVOS MÓVILES, TELETRABAJO Y BYOD

4.2.1.- OBJETIVO

Proteger la información de UTE almacenada o accesible desde dispositivos móviles provistos por UTE, BYOD y conexiones por teletrabajo.

Evitar la infección y distribución de código malicioso.

Prevenir accesos no autorizados a recursos de UTE.

4.2.2.- ALCANCE

Todos los dispositivos móviles provistos por UTE y BYOD que contengan o accedan a información de UTE.

Conexiones remotas a recursos de UTE.

4.2.3.- RESPONSABILIDADES

SEG

Definir buenas prácticas y controles que mitiguen los riesgos asociados sobre los dispositivos móviles, BYOD y conexiones remotas.

UARI

En su ámbito de acción cada UARI es responsable de:

- Implementar y monitorear controles para proteger la información de UTE presente en los dispositivos móviles, BYOD y las conexiones remotas.
- Gestionar respaldos, administración de archivos, sincronización y la seguridad sobre dispositivos móviles administrados por TIC.
- Gestionar la instalación, configuración y seguridad de los dispositivos móviles.

4.2.4.- DESCRIPCIÓN

Dispositivos Móviles: Utilizar los dispositivos móviles provistos por UTE con fines laborales y tomar las siguientes precauciones de seguridad:

- a. **Condiciones de Uso:** El uso particular está permitido siempre y cuando se cumpla con la política de Gestión de Activos de Información (4.4) y el consumo de recursos o el contenido no comprometan la seguridad de los sistemas de información.

Cumplir con la legislación vigente que prohíbe a los conductores de cualquier tipo o categoría de vehículos, cuando circulen, el uso de dispositivos de telefonía móvil o cualquier otro medio o sistema de comunicación, salvo cuando el desarrollo de la comunicación tenga lugar sin emplear cualquiera de las manos, según Ley N° 19.061 – Transito y seguridad vial en el territorio nacional.

- b. **Pérdida o Robo:** Tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo
- c. **Funcionalidades:** No está permitido realizar el desbloqueo de las limitaciones del fabricante y/o proveedor, alterar las configuraciones realizadas por UTE o cualquier otro método de cambio de las protecciones.

Entregar el dispositivo al CAU cuando sea solicitado por U-TIC, ya sea por razones de auditoría, administración o configuración.

- d. **Privacidad de los Datos:** Tomar las apropiadas precauciones para prevenir que otras personas externas a la organización (familia, amigos, etc.) tengan acceso a los dispositivos móviles de UTE y los recursos asociados a los mismos.

En caso que el dispositivo almacene información de UTE, el usuario firmará un acuerdo de derechos y obligaciones, permitiendo la eliminación remota de los mismos por parte de UTE en caso de robo o pérdida del dispositivo o cuando ya no se encuentran autorizados a utilizar el servicio.

Teletrabajo: Utilizar los mecanismos de seguridad establecidos para acceder a recursos de UTE mediante conexiones remotas.

Contar con un proceso formal para la administración de las solicitudes de alta, baja y modificación para estas autorizaciones. Estos registros quedarán accesibles con motivos de auditoría durante 5 años.

BYOD: Contar con mecanismos de seguridad aplicada a la información de UTE para:

- Separar la información personal de la laboral.
- Asegurar el almacenamiento, tratamiento y acceso de dicha información.

4.3.- POLÍTICA DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

4.3.1.- OBJETIVO

Previo al empleo

Asegurar que los usuarios entiendan sus responsabilidades y sean aptos para los roles para los cuales están siendo considerados.

Durante el empleo

Asegurar que los usuarios sean conscientes y cumplan con las responsabilidades de seguridad de la información.

Finalización y cambio de la relación laboral o empleo

Proteger los intereses de UTE como parte del proceso de cambiar o finalizar la relación laboral.

4.3.2.- ALCANCE

Todos los usuarios de UTE.

4.3.3.- RESPONSABILIDADES

Dirección, Gerencias y Jefaturas

Velar por el cumplimiento de la Política de Seguridad de la Información, así como proveer los recursos necesarios para garantizar la seguridad de la información de UTE.

HUM

Incorporar en el contexto de los descriptivos de los puestos de trabajo, la obligatoriedad de la notificación y el cumplimiento de las Políticas de Seguridad de la Información vigente.

AYS

Incorporar en todos los pliegos la obligación de firmar el Compromiso de Confidencialidad Corporativo a las empresas proveedoras de personal y/o de bienes y servicios a UTE.

LET

Participar en la confección y revisión del Compromiso de Confidencialidad Corporativo a firmar por los usuarios no funcionarios de UTE que utilicen activos de información y en la definición de sus consecuencias en caso de incumplimiento del mismo.

SEG

Informar a los usuarios de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.

Realizar actividades de capacitación y sensibilización respecto del cumplimiento de la Política de Seguridad de la Información.

Jefe Unidad

Controlar el cumplimiento de las Políticas de Seguridad de la información por parte de su personal a cargo. Ante un incumplimiento aplicar el procedimiento disciplinario vigente en UTE.

Eliminar acceso a los activos de información a todo funcionario que cambie de unidad o tarea.

Cuando un usuario a su cargo termina su relación laboral con UTE:

- Comunicar las responsabilidades y las obligaciones de seguridad de la información que permanecen válidas después de la terminación de su vínculo laboral.
- Solicitar todos los elementos que fueron suministrados para desarrollar sus tareas.
- Solicitar la baja del usuario o tercera parte que se desvincula de UTE.

4.3.4.- DESCRIPCIÓN

Selección: Evaluar que los candidatos cumplan las condiciones y requisitos para desempeñar tareas en UTE de conformidad con la normativa vigente incidente, considerando las necesidades y particularidades de UTE.

Términos y Condiciones del Empleo: Establecer en los acuerdos contractuales con usuarios y terceras partes sus responsabilidades y las de UTE en cuanto a la seguridad de la información.

Toma de Conciencia, Educación y Formación en la Seguridad de la información: Los usuarios participarán regularmente de las actividades de capacitación necesarias para proteger adecuadamente los recursos de información de UTE. Estas actividades estarán incluidas en un plan de formación continua que abarque los diferentes aspectos de la presente Política.

Finalización o Cambio De Responsabilidades Laborales: Los usuarios son responsables de cumplir sus obligaciones después de la terminación de su vínculo laboral con UTE o ante un cambio de tareas.

4.4.- POLÍTICA DE GESTION DE ACTIVOS DE INFORMACIÓN

4.4.1.- OBJETIVO

Responsabilidad por los activos

Identificar los activos de información de UTE y definir las responsabilidades de protección adecuadas.

Clasificación de la información

Asegurar que la información reciba un adecuado nivel de tratamiento de acuerdo a su clasificación.

Manejo de medios

Prevenir la divulgación o acceso no autorizados, la modificación, eliminación o la destrucción de la información almacenada en los medios.

4.4.2.- ALCANCE

Todos los usuarios de UTE.

4.4.3.- RESPONSABILIDADES

Gerencias

Clasificar la información y mantener la Tabla de Clasificación de Información de UTE, en base a la legislación nacional vigente.

Aplicar medidas de etiquetado y protección necesarias.

Designar los responsables de los activos.

Responsable de Activo de Información

Revisar sistemáticamente la información que UTE publica en diferentes medios de comunicación (internet, redes sociales, etc), que en caso de ser alterada pueda provocar perjuicios en el negocio.

SEG

Definir procedimientos para la clasificación, etiquetado y tratamiento de información de UTE.

Definir procedimientos para eliminar medios de forma segura.

Definir requisitos y buenas prácticas para la utilización de servicios en la nube.

Evaluar los acuerdos de confidencialidad y de servicio en la nube.

Controlar los servicios de infraestructura utilizados en la nube y evaluar la seguridad de los mismos.

Técnico Representante de la Unidad Usaria de los Servicios o de la Compra:

Controlar previo al inicio de los contratos o compras directas (con o sin pliegos), la presentación del Compromiso de Confidencialidad Corporativo firmado por parte del responsable de las empresas contratistas.

Comprobar que el proveedor de la nube posea una política de seguridad que se alinee a las Políticas de Seguridad de la Información.

UARI

Identificar, documentar e implementar reglas para establecer el uso aceptable de los activos de información, las cuales están alineadas a su clasificación.

Definir los niveles y perfiles de autorización para acceso, modificación y eliminación de los mismos.

AUD

Auditar las actividades que involucren el manejo de información confidencial y reservada.

4.4.4.- DESCRIPCIÓN

Inventario de Activos: Identificar los activos asociados con la información y los recursos de procesamiento de información y elaborar y mantener un inventario de los mismos.

Responsable de los Activos: Todos los activos del inventario deben contar con un responsable designado.

Uso aceptable de los activos:

- **Activos de Información**

Utilizar la información disponible en UTE independiente del soporte contenedor, únicamente para el desempeño de sus funciones.

- **Aplicaciones e Infraestructura en la Nube:**

Proteger la información transmitida y almacenada en la nube, acorde a su clasificación y cumpliendo la legislación vigente.

Gestionar una copia adicional en los servidores de UTE de toda información almacenada en la nube, para garantizar la disponibilidad de la misma en caso de contingencia de los servicios de la nube.

Gestionar un acuerdo de nivel de servicio con el proveedor de servicios e infraestructura contratada por UTE.

Los usuarios de UTE autorizados deben poder recuperar y eliminar en forma segura información publicada en la nube, acorde a su rol.

UTE deberá poder eliminar los datos personales que queden en los servidores del proveedor de la nube, una vez finalizada la relación comercial o en casos excepcionales.

Cada una de las partes (UTE y el proveedor de la nube) es responsable de cumplir con la legislación vigente.

- **Internet**

Internet es una herramienta de trabajo suministrada por UTE y el acceso a la misma por razones de servicio será autorizado por un superior jerárquico con nivel gerencial, quien tiene derecho a revocarlo o limitarlo ante un uso indebido o cuando el usuario pase a realizar tareas que no requieran su utilización.

Está prohibido navegar por páginas con contenido contrario a la moral y las buenas costumbres, páginas de apuestas o que instiguen a la violencia, al desprecio u odio racial, étnico, sexual, religioso o a contravenir normas jurídicas.

Ante indicios de amenazas a la seguridad de información y/o a la incorrecta utilización del servicio, TIC controlará el acceso a Internet y ante su comprobación dará aviso a la línea jerárquica correspondiente, pudiendo suspender los permisos de navegación. UTE se reserva el derecho de auditar el registro de accesos a Internet identificando los sitios a los que accede cada usuario.

Los únicos accesos permitidos a Internet desde cualquier equipo conectado a las redes de UTE, son los realizados a través de conexiones establecidas con la autorización de TIC.

- **Correo Electrónico y Mensajería Instantánea**

Correo con salida a Internet, es una herramienta de trabajo suministrada por UTE para comunicaciones de carácter laboral. Todos los funcionarios tendrán acceso a la misma. El acceso para personal contratado o buzones genéricos será autorizado por un superior jerárquico.

Es de uso personal e intransferible y la utilización de la misma es de total responsabilidad del usuario asociado.

Por excepción se permite ocasionalmente el uso particular siempre y cuando el consumo de recursos o el contenido no comprometan la seguridad de los sistemas de información.

Ante un incidente de seguridad de información o investigación administrativa, SEG tiene la potestad de bloquear una cuenta de correo de un usuario. Sin embargo, no se podrá acceder a la información en ella contenida sin un debido proceso que asegure la objetividad, autenticidad, conservación e inalterabilidad de la misma, debiendo documentarse lo actuado mediante acta notarial y previa autorización del Directorio o de GER y el contralor de la persona involucrada o un representante por él designado o, cuando esto no sea posible, un representante del personal.

- **Redes Sociales**

Todas las comunicaciones oficiales de UTE deben ser autorizadas por una autoridad competente según la reglamentación vigente.

Esto también es aplicable a medios sociales (como blogs, wikis, redes sociales como por ejemplo, Facebook, Twitter, YouTube, LinkedIn.), contribuciones en los foros o en las bases de datos de conocimiento como Wikipedia.

Todo usuario es responsable de sus acciones y de las opiniones expresadas en las redes sociales referentes a UTE.

No está permitido compartir información clasificada como confidencial o reservada por UTE.

Devolución de Activos

Devolver todos los activos de información físicos que le fueron suministrados para desarrollar sus tareas como por ejemplo computadoras portátiles, documentación, llaves, tarjetas magnéticas, etc. cuando un usuario termina su relación laboral con UTE.

Eliminación de Activos

Destruir la información confidencial independientemente del medio que la soporte al término de su vida útil.

Clasificación de Activos

Gestionar y etiquetar los activos de información según su criticidad, su susceptibilidad a divulgación o modificación no autorizada y su clasificación en la Tabla de Clasificación de Información de UTE vigente.

4.5.- POLÍTICA CONTROL DE ACCESO

4.5.1.- OBJETIVO

Requisitos del negocio

Limitar el acceso a información y a instalaciones de procesamiento de información.

Gestión de acceso del usuario

Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

Responsabilidad del usuario

Hacer que los usuarios sean responsables de salvaguardar su información de autenticación.

Control de acceso a los sistemas y las aplicaciones

Prevenir el acceso no autorizado a los sistemas y las aplicaciones.

4.5.2.- ALCANCE

Todos los usuarios.

4.5.3.- RESPONSABILIDADES

UARI

Definir procedimientos en su ámbito de acción para:

- La gestión del control de acceso del usuario a los activos de información.
- Bloquear automáticamente los usuarios no utilizados por un período determinado.
- Eliminar en forma periódica los usuarios bloqueados con determinada antigüedad.

- Eliminar los permisos de acceso otorgados a los usuarios que cesan su relación laboral con UTE, una vez registrada la baja en el sistema por HUM.

SEG

Controlar los permisos de acceso asignados a los administradores de recursos de TIC y las tareas de administración realizadas con dichos permisos.

Responsable de Activo de Información

Revisar periódicamente los permisos de acceso de los usuarios.

Jefe Unidad

Autorizar los accesos a los activos de información para los usuarios y terceras partes, dejando constancia de la solicitud realizada.

Retirar los derechos de acceso a los activos de información a los usuarios que se desvinculan de UTE y a los usuarios que no los requieran para desempeñar sus tareas.

Revisar los permisos de acceso cuando se alteran las tareas de un usuario.

Administración funcional

Revisión periódica de los permisos de acceso de usuarios:

- A intervalos planificados.
- Cuando se alteran las tareas de un usuario, por ejemplo, como resultado de una transferencia a otra unidad.

Verificar periódicamente que los permisos de acceso:

- Implantados en el sistema se corresponden con los definidos.
- De los usuarios del sistema se corresponden con los autorizados por los jefes.

4.5.4.- DESCRIPCIÓN

Control de Acceso: Establecer una política de control de acceso, documentada y revisada en base a los requisitos del negocio y de la seguridad de la información, basada en los siguientes principios: "mínimo acceso necesario", "necesidad de hacer", "necesidad de saber", "separación de funciones" y "oposición de intereses".

La administración de los usuarios predefinidos en el software adquirido a terceros, será realizada como si fueran usuarios reales, siempre que sea técnicamente posible.

El acceso a las contraseñas de los usuarios genéricos y/o predefinidos estará fuertemente restringido sobre la base de los principios "necesidad de saber" y "necesidad de hacer".

Acceso a Redes y a Servicios en Red: Los usuarios deben disponer únicamente de acceso a las redes y a los servicios de red a los que han sido autorizados.

Registro y Baja de Usuarios: Seguir un proceso formal para la administración de las solicitudes de alta, baja y modificación de usuarios, sus permisos de acceso y contraseñas. Este proceso incluirá un mecanismo que permita registrar dichas solicitudes. Los registros quedarán accesibles con fines de auditoría durante cinco años.

Provisión de Acceso a los Usuarios: Utilizar un procedimiento para asignar o revocar los derechos de acceso que contemple todos los tipos de usuario para todos los activos de información.

Gestión de Derechos de Acceso Privilegiado: Restringir y controlar la asignación y la utilización de los derechos de acceso privilegiados, sobre la base de los principios "necesidad de saber" y "necesidad de hacer".

Gestión de Información de Autenticación Secreta de Usuarios: Utilizar un procedimiento que garantice la entrega efectiva de la información de autenticación a la persona que corresponda.

Bloqueo Automático y Baja Definitiva: Utilizar un procedimiento para bloqueo y baja automático de usuarios no utilizados.

Uso de Información de Autenticación Secreta: La contraseña es secreta para cada usuario. Las únicas excepciones admitidas serán cuando se solicita la creación del usuario y cuando se solicita el cambio por olvido de la misma. Queda prohibida la práctica de registrar o anotar la contraseña en cualquier medio que no esté adecuadamente protegido.

Restricción de Acceso a la Información: Restringir en base a las necesidades del negocio y a la política de control de acceso a la información y a las funcionalidades de los sistemas de información.

El equipo de desarrolladores no tendrá acceso a la información que se encuentra en producción, con excepción de la información estrictamente necesaria para el trabajo que realice, siempre que técnicamente sea posible.

Procedimiento de Ingreso Seguro: Utilizar un procedimiento seguro de inicio de sesión para controlar el acceso a los activos de información.

Gestión de contraseñas: Asegurar el uso de contraseñas robustas y la obligación de su cambio luego del primer ingreso.

Restringir y controlar el uso de programas utilitarios capaz de anular los controles del sistema.

Control de Acceso a Códigos Fuente de Programas: Restringir el acceso al código fuente de los programas en los entornos de producción.

Antes de pasar el código correspondiente al sistema de información en desarrollo al entorno de producción, eliminar todos los permisos especiales a los equipos de desarrollo y pruebas, de modo que los permisos de acceso requeridos sólo puedan ser solicitados por los medios habituales.

4.6.- POLÍTICA CRIPTOGRAFÍA

4.6.1.- OBJETIVO

Controles criptográficos

Definir un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.

4.6.2.- ALCANCE

Toda la información más allá de su clasificación, que requiera ser protegida para mantener la confidencialidad, autenticidad e integridad.

4.6.3.- RESPONSABILIDADES

SEG

Definir buenas prácticas sobre criptografía.

Controlar la gestión técnica de los controles criptográficos y definir procedimientos e instructivos para la adecuada implementación de la firma digital.

Gestionar los certificados digitales.

UARI

En su ámbito de acción:

- Utilizar buenas prácticas sobre técnicas criptográficas donde sea requerido.
- Método de Cifrado: Identificar el nivel requerido de protección, definiendo el tipo y la calidad del algoritmo de cifrado y la longitud de las claves criptográficas a utilizar.

4.6.4.- DESCRIPCIÓN

Gestión de los Certificados Digitales: Utilizar un procedimiento para la gestión de los certificados digitales.

Proteger y utilizar, según lo establecido por SEG, las claves y dispositivos utilizados para la firma digital y el cifrado de la información según Ley N° 18.600 – Documento electrónico y firma electrónica.

Uso de Controles Criptográficos: Desarrollar e implantar una política sobre el uso de los controles criptográficos para proteger la información.

Gestión de Claves: Desarrollar e implantar una política sobre el uso, protección y duración de las claves criptográficas a través de todo su ciclo de vida.

Firma Digital: Utilizar firma digital en aquellos procesos que requieran la autenticidad, integridad y el no repudio de los documentos electrónicos y/o firmas electrónicas y transacciones realizadas.

4.7.- POLÍTICA SEGURIDAD FISICA Y DEL ENTORNO**4.7.1.- OBJETIVO**Áreas seguras

Evitar el acceso físico no autorizado, daño e interferencia contra las instalaciones de procesamiento de información y la información.

Equipamiento

Prevenir pérdidas, daños, hurtos o comprometer los activos de información, así como la interrupción de las operaciones relacionadas con dichos activos.

4.7.2.- ALCANCE

Los activos de información.

4.7.3.- RESPONSABILIDADES**SEG**

Asesorar en buenas prácticas sobre controles de acceso físico y del entorno.

UARI

Gestionar el control de acceso en áreas seguras.

Definir las buenas prácticas sobre los controles de acceso físico y del entorno en su ámbito de acción.

Responsable de Activo de Información

Autorizar el acceso a los activos de información y las áreas seguras.

4.7.4.- DESCRIPCIÓN

Perímetro de Seguridad Física: Definir los perímetros de seguridad para proteger las áreas seguras que contienen información de UTE.

Proteger adecuadamente los equipos que queden desatendidos de acuerdo a las buenas prácticas definidas.

Controles de Acceso Físico: Implementar controles de ingreso apropiados que aseguren únicamente el acceso del personal autorizado.

Seguridad de Oficinas, Recintos e Instalaciones: Diseñar y aplicar seguridad física a oficinas, despachos e instalaciones.

Protección Contra Amenazas Externas y Ambientales: Diseñar y aplicar protección física contra desastres naturales, ataques malintencionados o accidentales.

Trabajo en Áreas Seguras: Diseñar y aplicar procedimientos para trabajar en áreas seguras.

Áreas de Carga, Despacho y Acceso Público: Controlar y aislar los puntos de ingreso a las instalaciones de procesamiento de información para evitar ingresos no autorizados.

Ubicación y Protección de los Equipos: Ubicar y proteger el equipamiento para reducir la exposición a los riesgos ocasionados por amenazas, peligros ambientales y acceso no autorizado.

Servicios de Apoyo: Proteger el equipamiento de infraestructura y comunicaciones contra interrupciones causadas por fallas en los servicios de apoyo (por ejemplo, la electricidad, las telecomunicaciones, el agua potable, el gas, el alcantarillado, la ventilación y el aire acondicionado).

Seguridad en el Cableado: Proteger de interceptación, interrupción, interferencia o daños al cableado de energía, de telecomunicaciones que transporta datos y de los servicios de información auxiliares.

Mantenimiento de los Equipos de Apoyo: Realizar el correcto mantenimiento al equipamiento de los servicios de apoyo para asegurar su mayor disponibilidad e integridad.

Retiro de Activos de Información: Los activos de información no se podrán retirar de las instalaciones de UTE sin autorización previa por parte del responsable del mismo.

Seguridad de los Activos de Información Fuera de las Instalaciones de UTE: Proteger los activos de información fuera de los locales de UTE, teniendo en cuenta los diferentes riesgos a que se encuentran expuestos.

Seguridad en la Reutilización o Eliminación de los Equipos: Asegurar que todos los datos no públicos y software licenciado sea eliminado de forma segura en cualquier medio de almacenamiento antes de ser reutilizado o dispuesto para su eliminación.

Activos de Información Físico Desatendido: Proteger adecuadamente los activos de información físicos, cuando el responsable del activo se ausente de su puesto de trabajo.

Escritorio y Pantalla Limpia: Adoptar una política de escritorios y pantallas limpias para proteger la información.

4.8.- POLÍTICA SEGURIDAD DE LAS OPERACIONES

4.8.1.- OBJETIVO

Procedimientos y responsabilidades operacionales

Asegurar el funcionamiento correcto y seguro de los activos de información necesarios para el procesamiento de la información.

Protección contra el software malicioso

Asegurar que los activos de información estén protegidos contra el software malicioso.

Respaldo

Protección contra la pérdida de información.

Registro y seguimiento

Registrar los eventos y generar evidencia.

Control de los sistemas de información en producción

Asegurar la integridad de los sistemas de información que está en producción.

Gestión de la vulnerabilidad técnica

Evitar la explotación de vulnerabilidades técnicas.

Consideraciones de la auditoría de sistemas de información

Minimizar el impacto de las actividades de auditoría en los sistemas de información que están en producción.

4.8.2.- ALCANCE

Todos los sistemas de información y los activos de información asociados.

4.8.3.- RESPONSABILIDADES

UARI, SEG y AUD

En su ámbito de acción:

- Realizar pruebas de controles, análisis de vulnerabilidades y/o pruebas de penetración, previa autorización y coordinación con la gerencia correspondiente. La planificación de estas pruebas (incluyendo el análisis de riesgos realizado) así como los resultados de las mismas serán documentadas e informadas a la gerencia correspondiente. Esta documentación se conservará durante cinco años.

4.8.4.- DESCRIPCIÓN

Procedimientos Documentados de Operación: Documentar, mantener y poner a disposición de todos los usuarios que lo necesiten, los procedimientos relacionados con el procesamiento de información.

Gestión de Cambios: Definir e implementar controles en base a un análisis de riesgos, cuando se realicen cambios en las instalaciones de procesamiento de información y en los sistemas de información.

Gestión de la Capacidad: Supervisar y adaptar el uso de recursos, así como proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido de los sistemas de procesamiento de información.

Separación de los Recursos Para Desarrollo, Prueba y Ambientes de Producción: Separar los ambientes de desarrollo, prueba y producción para reducir los riesgos de acceso o cambios no autorizados a los recursos de producción.

Controles Contra Software Malicioso: Implementar controles de detección, prevención, y recuperación para proteger la información contra software malicioso. Adicionalmente realizar campañas de formación y comunicación al usuario.

No instalar software sin la previa autorización de la UARI según corresponda. En caso de instalar software tomar todas las medidas para cumplir con la presente Política.

Respaldo de la Información: Realizar regularmente respaldos, pruebas periódicas de su correcto almacenamiento y recuperación, de la información y de los sistemas de información.

Registro de Eventos (Bitácora): Revisar regularmente los registros de eventos que documentan las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Protección de la Información de Registros de Eventos: Proteger contra alteración y acceso no autorizado, a la información de registro de eventos y los medios contenedores de la misma.

Registros del Administrador y del Operador: Registrar, proteger y revisar regularmente las actividades de los administradores y operadores de sistemas.

Sincronización de Relojes: Configurar correctamente los relojes de los dispositivos de información pertinentes, para asegurar la exactitud de los registros de auditoría, que pueden requerirse para investigaciones o como pruebas en casos legales o disciplinarios.

Instalación de los Sistemas de Información en Producción: Implantar procedimientos para controlar la instalación de los sistemas de información en producción.

Gestión de Vulnerabilidades Técnicas: Obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información, evaluar la exposición de UTE a estas vulnerabilidades, y tomar las medidas apropiadas para abordar el riesgo asociado.

Restricciones a la Instalación de Software: Establecer e implantar reglas relativas a la instalación de software por los usuarios.

Controles de Auditoría de Sistemas de Información: Los requisitos y las actividades de auditoría que implican la verificación de los sistemas de información que están en producción se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio.

4.9.- POLÍTICA SEGURIDAD DE LAS COMUNICACIONES

4.9.1.- OBJETIVO

Gestión de seguridad de la red

Asegurar la protección de la información en las redes y en sus recursos de procesamiento de información.

Transferencia de información

Mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa.

4.9.2.- ALCANCE

Todos los usuarios.

4.9.3.- RESPONSABILIDADES

TIC

Implementar y gestionar las infraestructuras de comunicaciones de acuerdo a la presente política.

UARI

Proteger con mecanismos de control de acceso físico y/o lógico a los componentes de la red de comunicaciones de UTE.

Dotar a los sistemas de comunicaciones niveles definidos y coherentes de integridad de datos, confidencialidad y disponibilidad.

Establecer los mecanismos de transferencia segura de información entre UTE y terceras partes.

4.9.4.- DESCRIPCIÓN

Controles de Redes: Gestionar y controlar las redes para proteger la información en los sistemas de información.

Seguridad de los Servicios de red: Incluir en los acuerdos de servicio los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.

Segregación de las Redes: Separar en las redes los usuarios y los sistemas de información, en base a: niveles de confianza, unidades de UTE o una combinación de ambas.

Transferencia de Información: Implementar políticas, procedimientos y controles para proteger la información durante su intercambio independientemente del medio de comunicación a utilizar.

Mensajería Electrónica: Proteger apropiadamente de acuerdo a la legislación nacional vigente la información involucrada en la mensajería electrónica de UTE.

4.10.- POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

4.10.1.- OBJETIVO

Requisitos de seguridad de los sistemas de información

Asegurar que la seguridad de la información es una parte integral de los sistemas de información, a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

Seguridad en los procesos de desarrollo y soporte

Considerar la seguridad de la información en el ciclo de vida del desarrollo de los sistemas de información.

Datos de prueba

Proteger los datos utilizados para las pruebas de acuerdo con su clasificación.

4.10.2.- ALCANCE

Todos los sistemas de información utilizados en UTE.

4.10.3.- RESPONSABILIDADES

UARI

Establecer y aplicar buenas prácticas para el desarrollo seguro de los sistemas de información de UTE.

4.10.4.- DESCRIPCIÓN

Análisis y Especificación de los Requisitos de Seguridad de la Información: Incluir en los requisitos para los nuevos sistemas de información o para las mejoras en los ya existentes, requisitos relacionados con la seguridad de la información.

Servicios de Aplicación de Seguridad en las Redes Públicas: Proteger la información contra la actividad fraudulenta, la divulgación y modificación no autorizada, en los sistemas de información que hacen uso de redes públicas.

Protección en las Transacciones de los Sistemas de Información: Proteger las transacciones de los sistemas de información para prevenir la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.

El grado de los controles adoptados será proporcional al nivel del riesgo asociado a cada tipo de transacción.

Procedimientos de Control de Cambios del Sistema: Implementar un procedimiento de control de cambios que aplique durante el ciclo de vida del desarrollo de un sistema de información.

Revisión técnica de las Aplicaciones Después de Cambios en la Plataforma Operativa: Asegurar que los cambios en las plataformas operativas y los sistemas de información no afecten las operaciones o la seguridad de UTE.

Restricciones en los Cambios al Software Subcontratado: Desalentar la realización de modificaciones al software subcontratado, limitándose a los cambios necesarios y controlar estrictamente los cambios que se realicen.

Principios de la Ingeniería de Sistemas Seguros: Establecer, documentar, mantener y aplicar mecanismos de seguridad (análisis de riesgos, análisis de vulnerabilidades, implementación de controles, etc) en el diseño de los sistemas de información.

Entorno de Desarrollo Seguro: Establecer y proteger adecuadamente los entornos de desarrollo.

Desarrollo Subcontratado: Supervisar y realizar el seguimiento de las actividades de desarrollo de sistemas subcontratadas.

Pruebas de Seguridad de Sistemas: Realizar pruebas de las funcionalidades de seguridad, durante el desarrollo y mantenimiento del sistema.

Pruebas de Aceptación de Sistemas: Establecer criterios de aceptación de los requisitos de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones.

Protección de los Datos de Prueba: Seleccionar, proteger y controlar los datos de prueba de acuerdo a la clasificación de la información.

4.11.- POLÍTICA DE RELACIONES CON LOS PROVEEDORES Y TERCERAS PARTES

4.11.1.- OBJETIVO

Seguridad de la información en las relaciones con los proveedores y terceras partes

Asegurar la protección de los activos de información de UTE, accesibles por los proveedores y terceras partes.

Gestión de la prestación de servicios del proveedor

Mantener la seguridad de la información y la entrega del servicio, acorde con los acuerdos de nivel de servicio establecidos con los proveedores.

4.11.2.- ALCANCE

Activos de información accedidos por proveedores y terceras partes.

4.11.3.- RESPONSABILIDADES

Responsable del Activo de Información

Evaluar, autorizar o denegar y documentar las solicitudes de acceso a los activos de información que se encuentren bajo su responsabilidad.

UARI

Gestionar los accesos sobre activos de información que hayan sido previamente autorizados por el responsable del activo de información a proveedores y terceras partes.

4.11.4.- DESCRIPCIÓN

Seguridad de la Información para las Relaciones con Proveedores y Terceras Partes:

Acordar con proveedores y terceras partes los requisitos de seguridad de información para la mitigación de los riesgos asociados con el acceso a los activos de información de UTE.

Tratamiento de la Seguridad Dentro de los Acuerdos con Proveedores: Establecer y acordar con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de la infraestructura de TIC, los requisitos pertinentes de seguridad de la información.

Cadena de Suministro de Tecnologías de la Información y las Comunicaciones con Proveedores: Incluir requisitos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de información, productos y servicios de tecnologías de la información y las comunicaciones, en los acuerdos con proveedores.

Seguimiento y Revisión de los Servicios de los Proveedores: Realizar periódicamente seguimiento, revisiones y auditorías de la prestación de servicios de los proveedores, manteniendo la documentación pertinente.

Gestión del Cambio en los Servicios de los Proveedores: Gestionar teniendo en cuenta la clasificación de los activos de información y la evaluación de los riesgos asociados, los cambios en la prestación de servicios de los proveedores.

4.12.- POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

4.12.1.- OBJETIVO

Asegurar un enfoque coherente y eficaz a la gestión de incidentes, eventos y vulnerabilidades de seguridad de la información, incluyendo la comunicación a todas las partes interesadas.

4.12.2.- RESPONSABILIDADES

SEG

Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información, incluida la comunicación a las partes interesadas sobre eventos de seguridad y debilidades con el fin de prevenir y mitigar el impacto de los mismos.

Dar seguimiento, documentar y analizar los incidentes de seguridad reportados.

Conservar bajo custodia, la información relativa a violaciones, problemas o investigaciones relacionadas con la seguridad de la información durante al menos cinco años. Se aplica a las bitácoras de los sistemas, y toda la documentación generada durante las investigaciones realizadas.

Mantener contactos apropiados con las autoridades pertinentes y en caso de incidentes de seguridad de la información reportar a CERTuy.

TIC

Gestionar los incidentes de seguridad en su ámbito de acción y tomar las medidas para minimizar el impacto en la continuidad del negocio.

UARI

Gestionar los incidentes de seguridad en su ámbito de acción y tomar las medidas para minimizar el impacto en la continuidad del negocio y reportar a SEG en caso que corresponda.

Informar a SEG las violaciones y problemas reportados en su ámbito de forma de contar con un único repositorio de incidentes.

4.12.3.- ALCANCE

Todos los usuarios.

4.12.4.- DESCRIPCIÓN

Responsabilidades y Procedimientos: Establecer procedimientos y responsabilidades para la gestión de incidentes de seguridad, de forma de asegurar una respuesta rápida, eficaz, ordenada y metódica.

Reporte de Eventos de Seguridad de la Información: Reportar tan pronto como sea posible a su línea jerárquica, al CAU o a SEG, los eventos de seguridad de la información, incidente asociado a los sistemas de información y toda sospecha o evidencia de violación de seguridad.

Reporte de Debilidades de Seguridad de la Información: Reportar según los procedimientos definidos la sospecha o evidencia de una debilidad de seguridad de la información.

Evaluación y Decisión Sobre los Eventos de Seguridad de la Información: Evaluar los eventos de seguridad de la información y clasificarlos como eventos o incidentes de seguridad de la información.

Respuesta a Incidentes de Seguridad de la Información: Gestionar los incidentes de seguridad de la información según procedimientos definidos.

Aprendizaje Obtenido de los Incidentes de Seguridad de la Información: Utilizar para reducir la posibilidad o el impacto de incidentes futuros, el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información.

Recolección de Evidencia: Definir y aplicar procedimientos para la identificación, recopilación, adquisición y conservación de información, que puede servir como evidencia forense.

4.13.- POLÍTICA DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

4.13.1.- OBJETIVO

Continuidad de la seguridad de la información

Incluir la seguridad de la información en los sistemas de gestión de continuidad del negocio de UTE.

Disponibilidad

Asegurar la disponibilidad de las instalaciones de procesamiento de información.

4.13.2.- ALCANCE

Todos los procesos de UTE.

4.13.3.- RESPONSABILIDADES

Gerencias

Definir los requisitos de seguridad para la continuidad del negocio, en su ámbito de acción.

SEG y UARI

En su ámbito de acción:

Coordinar y dar soporte a las actividades de planificación de continuidad de la seguridad de la información del negocio.

4.13.4.- DESCRIPCIÓN

Planificación de la Continuidad de la Seguridad de la Información del Negocio: Determinar los requisitos de seguridad de la información al planificar la continuidad del negocio y la recuperación ante situaciones adversas.

Implementación de la Continuidad de la Seguridad de la Información del Negocio: Establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de seguridad de la información durante una situación adversa.

Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información del Negocio: Verificar a intervalos regulares los controles de seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

Disponibilidad de las Instalaciones de Procesamiento de Información: Las instalaciones de procesamiento de información deben contar con los recursos necesarios para cumplir con los requisitos de disponibilidad.

4.14.- POLÍTICA DE CUMPLIMIENTO

4.14.1.- OBJETIVO

Cumplimiento con los requisitos legales y contractuales

Asegurar el cumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con los requisitos de seguridad.

Revisiones de seguridad de la información

Evaluar a intervalos regulares el cumplimiento de las políticas y procedimientos de seguridad de la información de UTE.

4.14.2.- ALCANCE

Todos los requisitos normativos de aplicación en UTE.

4.14.3.- RESPONSABILIDADES

Gerencias

Definir y documentar todos los requisitos normativos y contractuales aplicables a UTE relacionados a la seguridad de la información.

Revisar regularmente en su ámbito de acción, que los procedimientos asociados al uso de información cumplen con normas, buenas prácticas de seguridad de la información y legislación vigente.

UARI

Implementar procedimientos para asegurar el cumplimiento de los requisitos legales aplicables.

4.14.4.- DESCRIPCIÓN

Identificación de la Legislación Aplicable: Identificar, documentar y actualizar para cada sistema de información, todos los requisitos legales, reglamentarios, contractuales y el enfoque de la organización para su cumplimiento.

Derechos Propiedad Intelectual: Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

Protección de Registros de Información: Proteger contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada los registros de información, de acuerdo con los requisitos legales, reglamentarios, contractuales y de negocios.

Privacidad y Protección de Información de Datos Personales: Asegurar la privacidad y la protección de los datos personales, como se exige en la legislación vigente y en las reglamentaciones pertinentes, según corresponda.

Regulación de Controles Criptográficos: Usar controles criptográficos que cumplan con todos los acuerdos, leyes y reglamentaciones pertinentes.

Revisión Independiente de la Seguridad de la Información: El enfoque de UTE para la gestión de la seguridad de la información y su implementación (es decir los objetivos de

control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), deben ser revisados independientemente a intervalos planificados o cuando ocurran cambios significativos.

Revisión de Conformidad Técnica: Revisar regularmente los sistemas de información para asegurar su conformidad con las políticas y las normas de seguridad de la información de UTE.

5.- REGISTROS

Código / Nombre	Cuándo	Responsable de registrar	Responsable de archivo	Lugar / Soporte	Período de archivo
Notificación	Cada vez que se modifica la Política	SEG	SEG	Base de datos de sistema SUSI	5 años

6.- INDICADORES

(SEG-20): Seguimiento de notificaciones de última versión de política de S.I. Indicador mensual. Refleja el porcentaje de usuarios notificados de la última versión de la Política de Seguridad de Información aprobada por Directorio.

(SEG-24): Estado de vigencia y aprobación de la política actual. Indicador anual. Refleja años de aprobación de las políticas. Tiene como meta tres años, debido que las políticas son revisadas o ajustadas como máximo cada tres años.

7.- ANEXOS

No aplica