NO-UTE-SI-0001/05

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Versión 2015 -

Septiembre de 2015

Elaborado por:	**Aprobado por:**
Comité de Seguridad de Información	**RE 15.-2777** **Directorio de UTE**
FECHA: 09/09/2015	**FECHA: 10/12/2015**

0.- TRÁMITE Y REVISIONES

0.1 TRÁMITE

El documento "Política de Seguridad de la Información" en su versión 2015 fue elaborado por el Comité de Seguridad de la Información.
La presente normativa fue aprobada por R 15.-2777 de 10 de diciembre de 2015.

0.2 REVISIONES Y COMPATIBILIDAD TÉCNICA

0.2.1.- Revisiones de la Política de Seguridad de la Información

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 la Empresa, las regulaciones y normas externas.

0.2.2.- Detalle de revisiones

Fecha	N° de revisión	Párrafos modificados
22/7/2015	05	• Se modifican los nombres de las unidades que forman parte del Comité de Seguridad según la nueva estructura organizativa (BAMBU): - Sistemas de Información y Telecomunicaciones por Tecnologías de la Información y Comunicaciones. - Despacho Nacional de Cargas (DNC) por Despacho de Cargas. - Planificación de la Explotación y Estudios por Despacho de Cargas. • Se unifican las unidades de SIS (Sistemas de Información) y TEL (Telecomunicaciones) por TIC (Tecnologías de la Información y Comunicaciones). • Se modifica el nombre de la unidad Auditoria Interna y Seguimiento de la Gestión por Auditoria Interna. • Se normalizan todas las referencias a "UARIs" como "U-TIC y las UARIs". • Se unifican los nombres y las responsabilidades de las UARIs SIS y U-TEL por U-TIC. • Se unifican los nombres y las responsabilidades de las UARIs U-EDPyT y U-PRO-TRA por U-TRA. • Se modifica el nombre de la UARI U-TEL-DIS por U-DIS-ACD. • Se modifica la denominación de la unidad "Sector Despacho Nacional de Cargas" de la UARI U-DNC por "División Despacho de Cargas". • Se modifica la denominación de la unidad "Sector Planificación de la Explotación y Estudios" de la UARI U-PEE por "División Despacho de Cargas". • Se modifica la denominación de las UARIs U-

		HID, U-EOL y U-TER por U-GEN-HID, U-GEN-EOL y U-GEN-TER respectivamente. • Se agrega la definición de la unidad de Tecnologías de la Información y Comunicaciones (TIC). • Se modifica la denominación de la unidad "Relaciones Públicas" por "Comunicación Corporativa y Responsabilidad Social". • Se modifica la denominación de la unidad "Recursos Humanos" por "Gestión Humana".
5/03/2014	04	• Se corrige el ámbito de aplicación de las presentes políticas cuyo cumplimiento atañe a todos los funcionarios y contratados de cualquier tipo. • Se incorpora la clasificación de la información privilegiada para considerar impacto de nuevas leyes. • Se agrega la responsabilidad de ABA en la incorporación del Compromiso de Confidencialidad Corporativo en los pliegos. • Se sustituye la Política de uso de dispositivos portátiles por una nueva política de uso de dispositivos móviles. • Se agrega una política sobre manejo de medios de almacenamiento. • Se agrega una política sobre redes sociales. • Se actualizan las responsabilidades de la UARI U-PEE. • Se incorpora la definición de Instalaciones de infraestructura tecnológica de UTE. • Se adecua la definición de Comité de Seguridad de la Información: creado Por R 07.-456 de fecha 19 de abril de 2007.
2010	03	• Se pasa a considerar la Seguridad de la Información a nivel general poniendo foco en la Seguridad Informática. • Se pasa a revisar con una periodicidad no mayor a tres años. • Se modifica la clasificación de la información para considerar impacto de nuevas leyes. • En base a las recomendaciones de distintas auditorías internas y externas, se incorporan múltiples ajustes a la última versión de las PSI.
01-08-2006	02	• Se cambia el formato de la política de acuerdo a las recomendaciones y mejores prácticas de la norma ISO 27001. • Se incorpora política sobre redes inalámbricas. • Se contemplan los diferentes roles que hacen a la seguridad informática de la empresa. introduciéndose el papel del Comité de Seguridad de la Información y las UARIs.

5-08-2004	01	• En “Gestión de la seguridad” se agrega un apartado sobre los “Atributos de la información” Se establece que los responsables funcionales deben clasificar la información según su nivel de sensibilidad, y se especifican los cuidados a tener en cuenta en lo que toca al tratamiento de la información de la empresa. • Se reforzó la política de Controles sobre Internet. Cortafuegos y revisiones periódicas de bitácoras. • Se modificó la política de Controles sobre el Correo electrónico. Se agrega que se puede revocar un usuario de correo por irregularidades en el uso del mismo, que no se permite el uso por terceras personas y que SIS puede establecer restricciones al uso de esta herramienta con fines de optimización. • Se incorpora una política específica de “Controles sobre los computadores portátiles” • En “Controles sobre Operaciones” se agrega un apartado sobre “Bitácoras”. • En “Administración de cambios” se agrega un apartado sobre “Cambios a programas relacionados con la seguridad informática. • En “Desarrollo de sistemas” se agrega un apartado sobre: “Desarrollo de programas relacionados con la seguridad informática”. • Se agrega una política sobre “Controles sobre virus”. • Se agrega una política para considerar “Otros aspectos” que hacen a la Adquisición de software y hardware, propiedad intelectual, venta de software, servicio de procesamiento a terceros y cumplimiento de normas externas.
27-12-2001	00	• Versión inicial del documento.

1.- MARCO GENERAL

1.1 ÁMBITO DE APLICACIÓN

Es de aplicación en todo el ámbito de la Administración Nacional de Usinas y Trasmisiones Eléctricas (UTE). Atañe a todos los funcionarios (en cualquier carácter), consultores y personal contratado que hacen uso de la información provista por UTE. Atañe a todos los funcionarios y contratados de cualquier tipo.

1.2 VIGENCIA

La política aquí definida entra en vigencia a partir de su aprobación.

1.3 ALCANCE

La Política se expresa como “deber ser” y se toma como un marco de referencia para las áreas.

2.- DEFINICIONES

Amenaza: Una causa potencial de un incidente indeseado, que puede dar lugar a daños a un sistema o una organización.

Área: Unidad funcional definida como tal en el organigrama de UTE, incluyendo aquellas que, si bien por su jerarquía no lo son, lo sean por su relación de dependencia.

BYOD – en castellano "trae tu propio dispositivo".

Canales de medios sociales: blogs, micro-blogs, wikis, redes sociales, servicios de marcadores sociales, los servicios de calificación de usuario y cualquier otra colaboración en línea, plataformas para compartir o publicar tanto si se accede a través de la web, un dispositivo móvil, mensajería de texto, correo electrónico o cualquier otra plataforma de comunicaciones existente.

Cuenta en un Medio Social: Una presencia personalizada en un canal de redes sociales iniciado voluntariamente por un individuo. Las redes sociales permiten a los usuarios crear cuentas propias en los medios sociales, las cuales se pueden utilizar para colaborar, interactuar y compartir contenido y actualizaciones de estado. Cuando un usuario se comunica a través de una cuenta de medios de comunicación social, las publicaciones hechas se atribuyen a su perfil de usuario.

Comité de Seguridad de la Información: Grupo interdisciplinario liderado por la Gerencia de Tecnologías de la Información y Comunicaciones (TIC) creado por R 07.-456 de fecha 19 de abril de 2007, cuya principal responsabilidad será 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, Trasmisión, Distribución, Comercial, Planificación, Secretaría Técnica, Despacho de Cargas, Asesoría Técnico Jurídica, Secretaría General, y Tecnologías de la Información y Comunicaciones (TIC).

Contenido Oficial: contenido en línea disponible públicamente, creado y hecho público por UTE, verificado en virtud de que es accesible a través de nuestra página web corporativa.

Control: Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos de la empresa serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.

Derechos de autor: protegen el derecho que tiene el autor para controlar la reproducción y el uso de cualquier expresión creativa que se ha fijado en forma tangible, tales como obras literarias, gráficas, fotográficas, audiovisuales, electrónicas y musicales. Es ilegal reproducir y usar el material con derechos de autor a través de los canales de medios sociales, sin el permiso del propietario del mismo.

Equipamiento informático: Hardware utilizado en el procesamiento de la información, se consideran incluidos en este concepto también los equipos de comunicaciones y telecontrol.

Equipamiento informático crítico: Equipamiento identificado como crítico o con una categoría superior de criticidad en el análisis de riesgos de las UARIs.

Incidente de Seguridad Informática: Una interrupción no planeada de un servicio de TI o la reducción en la calidad del servicio. Se puede entender que un evento que amenace la calidad, seguridad o fiabilidad del servicio, aunque todavía no haya impactado, también se considera incidente.

Incidente de Seguridad de Información: Una serie de eventos indeseados o inesperados que tiene una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la integridad, disponibilidad o confidencialidad de la información.

Instalaciones de infraestructura tecnológica de UTE: incluye Centros de Procesamiento de Datos, Centros de Impresión y ensobrado, Salas de Comunicaciones, Centros de Maniobras de Distribución y bóvedas de almacenamiento de respaldos.

Medios de almacenamiento externo: dispositivo de almacenamiento extraíble que se conecta a un equipo para intercambiar información. Por ejemplo, los pendrives, discos externos, u otros dispositivos como smartphones, tabletas y PDA´s.

Notebook: Equipo portátil con iguales prestaciones a un computador personal (PC).

Netbook: Equipo similar a un Notebook con menor tamaño y recursos limitados.

Objetivo de control: Una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad particular.

Perfil de usuario - El titular de una cuenta de medios sociales puede personalizar sus perfiles de usuario dentro de un canal de medios sociales, con información específica acerca de sí mismo. Esa información se puede poner a disposición de otros usuarios.

Sistemas de Gestión: Se trata de los Sistemas Integrados de la Empresa que cubren los procesos de las Áreas de Negocio y Funcionales. Son de aplicación extendida a múltiples sectores y usuarios.

Tableta: Es similar a un teléfono inteligente pero con una pantalla de mayor tamaño generalmente de 7 pulgadas o superior.

Teléfono inteligente (Smartphone): Es un equipo celular con prestaciones avanzadas, con pantalla táctil o multitáctil, que incorpora funcionalidades como por ejemplo, acceso a red de datos, wifi, bluetooth, cámara de fotos y/o filmación, incluye sistema operativo, administrador de archivos y también herramientas de ofimática.

Unidad: unidad organizativa definida en SAP.

TIC: Gerencia de Tecnologías de la Información y Comunicaciones. Surge de la fusión de las áreas de Tecnología (anteriormente denominada Sistemas de Información) y Telecomunicaciones.

Unidad administradora de recursos de información (UARI): Unidad responsable de administrar equipos o sistemas que manejan información relevante para la Empresa, ya sean sistemas informáticos, redes de datos o equipos para aplicaciones industriales o administrativas. Estas UARIs están definidas explícitamente en el anexo A, cada una tiene un ámbito de actuación definido, al cual están referidas las responsabilidades que se les asigna en el presente documento. U-TIC es una UARI cuyo ámbito de actuación es corporativo y horizontal a nivel de toda la empresa, por lo que muchas veces se la citará a lo largo del documento en forma explícita.

Sistemas de Información: Conjunto de recursos informáticos utilizados para el tratamiento y administración de datos e 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.

Separación de funciones: Principio de seguridad de la información que establece la segregación de tareas para reducir el riesgo de que una persona pueda cometer errores o fraudes. Una persona o equipo de trabajo no puede ser también quien audite o controle las tareas suyas o de su propio equipo.

PDA (del inglés: personal digital assistant) es una computadora de mano, organizador personal o una agenda electrónica de bolsillo. Actualmente estos dispositivos están siendo sustituidos por los smartphone.

3.- INTRODUCCIÓN

UTE ha desarrollado sistemas de información que apoyan muchas de las actividades diarias de la mayoría de las unidades de la Empresa. Estos sistemas no sólo se han transformado en herramientas imprescindibles para gran parte de los procesos de los niveles operativos, sino que constituyen una importante fuente de datos para la toma de decisiones operativas, tácticas y estratégicas. La base de la eficacia y eficiencia de estos sistemas de información es su credibilidad, que está dada por la confiabilidad y seguridad de la información que mantienen.
Con tal motivo se ha definido la Política de Seguridad de la Información, que comprende un conjunto de normas y controles aplicables a la información utilizada en la Empresa, a los procesos de administración de la misma y a toda la infraestructura y tecnología asociada, utilizada por UTE para sí o para terceros.

3.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La información y los procesos que la apoyan, los sistemas y las redes son importantes activos de la Empresa. Definir, alcanzar, mantener y mejorar la seguridad de la información es esencial para lograr sus objetivos.
Cualquiera sea la forma que tome la información o los medios (soportes) por los que se comparta o almacene, la misma debe estar siempre protegida adecuadamente.

La información manejada y producida por los sistemas de información debe ser relevante y pertinente para los procesos del negocio, debe ser entregada de manera oportuna, correcta, consistente y utilizable (principio de efectividad), procurando ser provista a través de la óptima utilización de los recursos (principio de eficiencia). Debe además ser apropiada para que cada Gerencia pueda cumplir con sus responsabilidades relacionadas con la operación de la Empresa (principio de confiabilidad) y con el cumplimiento de leyes, regulaciones y acuerdos contractuales (principio de cumplimiento).
La seguridad de la información se preserva a través de los siguientes principios:

- **confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
- **integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

3.2. OBJETIVO DE LA SEGURIDAD DE LA INFORMACIÓN

El objetivo principal es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad de las operaciones de la Empresa, reducir al mínimo los daños causados por una contingencia y maximizar el retorno de las inversiones y las oportunidades de negocio.

4.- MARCO DE REFERENCIA

La seguridad de la información se consigue implementando un conjunto adecuado de controles como ser: políticas, procesos, procedimientos y funciones (informatizadas o no), y asignando los recursos necesarios. Estos controles deben ser establecidos, implementados, revisados y mejorados cuando fuere necesario para asegurar que se cumplen los objetivos específicos de seguridad de información de la Empresa.
Los planes de seguridad para cumplir esta política serán elaborados por cada área y tendrán los plazos y metas definidos por la misma.
Sobre la base de la familia de normas ISO/IEC relativas a la seguridad de la información y provisión de servicios, mejores prácticas como ITIL y recomendaciones de organismos de reconocido prestigio tales como el Colegio de Contadores, Economistas y Administradores del Uruguay, Information Systems Audit & Control Association, Information Systems Audit & Control Foundation, Instituto Uruguayo de Auditoría Interna, Institute of Internal Auditors, UNIT, etc., la Empresa identificará los requisitos de seguridad y control, considerando la evaluación de los riesgos, los requisitos externos (legales, normativos y contractuales) y los requisitos internos (políticas, lineamientos, principios y objetivos que forman parte del procesamiento de la información).

5.- POLÍTICAS GENERALES

5.1 CUMPLIMIENTO DE REQUISITOS LEGALES, REGULADORES Y CONTRACTUALES

El Comité de Seguridad debe 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 en UTE a los efectos de asesorar en su cumplimiento a las unidades de la Empresa según corresponda.

La utilización de cualquier tipo de información y/o productos tecnológicos debe ceñirse a las especificaciones de uso de su autor y a las normas jurídicas vigentes.

5.2 ORGANIZACIÓN DE LA SEGURIDAD

5.2.1.- Gestión de la Seguridad de la Información

Es responsabilidad de cada área de UTE contar con un Plan de Seguridad de información conforme a los requisitos de la norma ISO/IEC 27001 con revisión anual. Cada Plan de Seguridad de información debe incluir al menos:

- Un análisis y gestión de riesgos
- Análisis de vulnerabilidades
- Plan de continuidad operativa

Los resultados del análisis de riesgos ayudarán a orientar y determinar una adecuada acción gerencial y las prioridades para implementar los controles seleccionados.

Para los equipos y sistemas de información que no cuenten con niveles de riesgo aceptables y los recursos que no cumplan con la presente política, se deben implementar controles compensatorios adecuados siendo debidamente justificados y documentados.

Siempre que se apliquen las excepciones o salvedades establecidas en estas políticas, se deberán documentar adecuadamente las solicitudes, justificaciones y autorizaciones correspondientes. Todo apartamiento, excepción o salvedad a estas políticas deberá ser considerado cuando se realice el análisis de riesgo mencionado en el primer párrafo de este punto.

Todas las áreas deben realizar anualmente evaluaciones del cumplimiento de las Políticas y gestionar el análisis de vulnerabilidades realizado por un tercero independiente, sobre los sistemas de información en su ámbito de acción. Los resultados de las mismas deben ser comunicados al Comité de Seguridad de la Información.

5.3 REQUISITOS DE FORMACIÓN, ENTRENAMIENTO Y CONOCIMIENTO EN SEGURIDAD

Los funcionarios de UTE, ya sea personal permanente o contratado, deben participar de las actividades de capacitación necesarias para proteger adecuadamente los recursos de información de la empresa. Estas actividades deben estar incluidas en un plan de formación continua que abarque los diferentes aspectos de la presente Política.

Todas las personas, tanto físicas como jurídicas que brinden sus servicios a UTE, independientemente de la forma de relacionamiento con la Empresa, deben estar en conocimiento y cumplir con la Política de Seguridad de la Información. Esta obligación estará debidamente especificada en los acuerdos contractuales que tengan con UTE dependiendo de la naturaleza del servicio.

5.4 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.
- **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.
- **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. 18.331, Arts. 9 y 10).

- **Información privilegiada**: Se considera información privilegiada (de acuerdo al Art 246.1 de la Ley 18627)
  - La información de un emisor – o de los valores que emita – obtenida en razón del cargo o posición, inclusive la trasmitida 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 trasmisión 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:

- Debe ser protegida contra la divulgación no autorizada a través de cualquier medio físico o electrónico.
- Si fuera trasportada o trasmitida por un medio de comunicación inseguro (Internet, intranet, cartuchos, medios, etc.) deberá contar con protecciones adicionales (encriptación, contratos, precintos, etc.).
- Debe ser explícitamente identificada como tal y debe ser destruida al final de su vida útil (considerando los plazos precaucionales definidos por la empresa).
- En caso de ser necesario imprimirse debe hacerse de acuerdo a un procedimiento que se ajuste a la normativa vigente.

Constituyen uso indebido de la información privilegiada (art. 246.2 de Ley 18627) 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.-1964de fecha 5 de diciembre de 2013 toda la información clasificada como privilegiada será tratada como reservada hasta su desclasificación.

5.5 DISPONIBILIDAD DE LA INFORMACIÓN

La información debe estar disponible cuando ésta sea requerida por los procesos de la Empresa, o para dar cumplimiento a las leyes vigentes en materia de Protección de Datos Personales y Acceso a la Información Pública.
Se deben adoptar las medidas necesarias para salvaguardar la información así como los recursos necesarios para asegurar su disponibilidad.

5.6 INCIDENTES DE SEGURIDAD

Un usuario, ante cualquier sospecha o evidencia de violación de seguridad de la información o incumplimiento de la presente política, debe reportarlo a su línea jerárquica. Si se trata de un incidente de TI debe reportarlo además a U-TIC y/o a la UARI involucrada.
Ante un incidente de seguridad la línea jerárquica debe tomar las medidas pertinentes para minimizar el impacto en la continuidad del negocio.

6.- POLÍTICAS ESPECÍFICAS DE TECNOLOGÍAS DE INFORMACIÓN

6.1 POLÍTICA SOBRE PROPIEDAD INTELECTUAL DE SOFTWARE

Todo software de terceros que se utilice en la Empresa debe tener un acuerdo de licencia debidamente documentado cuando así corresponda. Este acuerdo deberá indicar si existe alguna limitación en su utilización.
Se deben realizar revisiones periódicas del software instalado en los equipos informáticos de la Empresa a efectos de verificar el cumplimiento de los acuerdos de licencia vigentes. La periodicidad estará establecida en el Plan de Seguridad de Información de cada área.
Todo software desarrollado en la Empresa por personal propio o ajeno es propiedad intelectual de UTE, sin perjuicio del reconociendo moral a las personas involucradas en el desarrollo de dicho software, debiendo analizarse la conveniencia de su inscripción en el Registro de Derechos de Autor.

6.2 POLÍTICA SOBRE CONTROLES DE INTERNET

6.2.1.- Controles sobre el uso de Internet

Internet es una herramienta de trabajo suministrada por la Empresa y el acceso a la misma por razones de servicio deberá ser autorizado por un superior jerárquico con nivel gerencial, quien tendrá 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, U-TIC controlará el acceso a Internet y ante su comprobación dará aviso a la línea jerárquica correspondiente, pudiendo suspender los permisos de navegación.

Toda la información que UTE presenta en páginas de Internet que en caso de ser alterada pueda provocar perjuicios en el negocio debe ser revisada sistemáticamente por el área funcional dueña de la información.
Toda aplicación a ser utilizada en ambiente de Internet debe estar sujeta a pruebas de vulnerabilidad antes de ser puesta en producción.
UTE se reserva el derecho de auditar el registro de accesos a Internet identificando los sitios WEB a los que accede cada usuario. Para ello U-TIC debe registrar los accesos a Internet en una bitácora, la que estará disponible para control de las líneas correspondientes, siempre y cuando exista una presunción de violación a las políticas de uso, o a las políticas de seguridad, o se haya identificado un acceso no autorizado, y siempre y cuando la Jefatura respectiva así lo disponga mediante decreto fundado. Dicho acceso deberá guardar la debida razonabilidad con los derechos de los usuarios, y deberá ser comunicado al Gerente de Sector correspondiente quedando registro de la comunicación.

6.2.2.- Controles sobre conexiones a Internet

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 U-TIC, quien monitorizará que no se utilicen otras formas de conexión no autorizadas.
Toda conexión entre la red de comunicaciones de UTE e Internet debe mantener un cortafuegos (firewall) para proteger la información y los sistemas contra accesos no autorizados. Cada modificación en la configuración de los cortafuegos deberá ser probada en un entorno aislado. U-TIC verificará que la configuración sea adecuada y periódicamente efectuará revisiones a efectos de comprobar que los mismos se mantienen configurados de acuerdo a las condiciones aprobadas. La periodicidad será definida en el Plan de Seguridad. La documentación de los cortafuegos es reservada y debe actualizarse siempre que se haga una modificación a la configuración.
La asignación de un dispositivo móvil de UTE para acceder a las aplicaciones habilitadas a través de Internet, requiere autorización previa de un funcionario con nivel Gerencial.
El acceso a internet para invitados se realizará a través de redes wifi instaladas con tal propósito en los distintos locales de UTE mediante un usuario y contraseña de uso temporal.

6.3 POLÍTICA SOBRE EL USO DEL CORREO ELECTRÓNICO

Esta política es de aplicación también sobre la mensajería instantánea corporativa.
El correo electrónico es una herramienta de trabajo suministrada por la Empresa y el acceso a la misma por razones de servicio deberá ser autorizado por un superior jerárquico.
La administración de la herramienta debe garantizar el carácter privado que tiene la información que en él se almacena de manera que el contenido sea accesible sólo por el dueño del buzón.
La cuenta de correo es para uso personal e intransferible siendo la utilización de la misma de total responsabilidad del usuario asociado.
El mismo debe utilizarse exclusivamente para comunicaciones de carácter laboral de UTE. 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.

Está prohibido el uso del correo electrónico para enviar mensajes de tipo "cadena". La difusión de información corporativa a todos los usuarios, se deberá canalizar por Intranet, o el correo electrónico, para lo cual será necesaria una autorización con nivel gerencial.
Está prohibido distribuir información que contravenga las leyes de derecho de autor (piratería), o contraria a las buenas costumbres, o que contenga agravios o amenazas, o que instiguen a la violencia, al desprecio u odio racial, étnico, sexual, religioso, o a contravenir normas jurídicas o sirvan para acosar en cualquier forma a cualquier funcionario o tercero ajeno a la organización.
La información clasificada en UTE como confidencial, reservada, sensible y/o privilegiada, no puede ser enviada por medio del correo electrónico ni almacenada fuera de UTE sin agregar medidas de protección adicionales que garanticen un nivel de seguridad adecuado.
Los administradores de la herramienta deberán proveer métodos de transmisión seguros para la información que así lo requiera.
No se deben ejecutar programas, que vengan adjuntos con mensajes de una fuente no reconocida, ya que los mismos pueden contener virus que afecten a los recursos de UTE.
Ante un incidente de seguridad informática o investigaciones administrativas, la unidad de Seguridad de la Información podrá bloquear una cuenta de correo de un usuario de UTE. 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.
UTE no puede garantizar que las comunicaciones a través del correo electrónico fuera de la Empresa sean privadas. Las comunicaciones electrónicas dependiendo de la tecnología usada pueden ser interceptadas por otras personas.

6.4 POLÍTICA SOBRE EL USO DE REDES SOCIALES

Los medios sociales como blogs, wikis, redes sociales (por ejemplo, Facebook, twitter, YouTube, LinkdIn, etc.), o sitios web personalizados están cambiando la forma en que nos comunicamos con los usuarios, clientes y otras partes interesadas fuera y dentro de la red de UTE. A pesar que las nuevas plataformas emergentes parecen cambiantes todo el tiempo, su aspecto básico permanece constante y es similar a las formas tradicionales de la comunicación: entablar un diálogo, proporcionar e intercambiar información y fomentar el entendimiento.
Todas las comunicaciones oficiales de UTE deben ser autorizadas por una autoridad competente por R 97.- 1554 de 6 de agosto de 1997. Esto también es aplicable a medios sociales, contribuciones en los foros o en las bases de datos de conocimiento como Wikipedia.

6.4.1.- Comunicaciones en nombre de UTE

Las áreas funcionales deben controlar los canales de medios sociales relevantes y deben establecer reglas para actuar frente a potenciales informes de eventos adversos o posibles contenidos inapropiados o ilegales que aparecen en su esfera de responsabilidad. Siempre se debe tener presente las obligaciones de preservar datos que pueden estar sujetos a una retención legal.

Las cuentas oficiales de UTE en medios sociales a través de las cuales se comunica deben estar publicadas en el sitio institucional de UTE en internet.

La comunicación sobre los ingresos, tarifas, planes futuros, así como declaraciones sobre productos de UTE ("información promocional") debe ser realizada por los expertos en el tema de las áreas autorizadas.

UTE tiene obligaciones reglamentarias y legales para retener cierta información como registros por lo tanto, toda la información pertinente que se interprete como una posición de UTE en el espacio de medios sociales, debe ser capturada y mantenida como registro de manera confiable y admisible por el área funcional responsable. Recordar que los informes de la empresa están sujetos a los mismos estándares legales que los medios de comunicación tradicionales.

Se debe respetar el compromiso con la transparencia, la información equilibrada y la igualdad de trato de todas las partes y los derechos de autor dando crédito a los autores originales de cualquier contenido de terceras partes que se vaya a publicar (textos, imágenes, marcas comerciales, vídeo, etc.) y que UTE tenga los derechos de autor o de aprobación por escrito para el uso de dicho material.

6.4.2.- Comunicaciones personales referidas a UTE o de sus productos

Es importante que el usuario siempre recuerde a quien representa y cuál es su papel en la comunidad de los medios sociales. Al igual que con los medios tradicionales, los usuarios tienen la oportunidad y la responsabilidad de gestionar eficazmente la reputación de la compañía y participar selectivamente en las conversaciones en línea en que UTE sea mencionada.

Los usuarios deben ser conscientes que en las redes sociales no hay separación entre un perfil personal y el de negocio por lo que se debe recordar que los colegas, clientes y competidores pueden tener acceso al contenido que publique.

Todo usuario es responsable de sus acciones y las opiniones expresadas. Cuando un usuario se está expresando en público su contribución puede permanecer en línea durante mucho tiempo y llegar a un público más amplio - tanto interna como externamente. Cualquier cosa que dañe el negocio y reputación de UTE en última instancia, será su responsabilidad.

Ser respetuoso de todos los individuos, razas, religiones y culturas.

Sólo se puede compartir la información pública. No está permitido hablar de información clasificada como confidencial, reservada y/o sensible.

Si realiza comentarios sobre cualquier persona de UTE o de sus productos o iniciativas en un foro público o en un sitio web o blog personal de nuestros competidores, asegúrese de revelar plenamente su afiliación con UTE y que sus opiniones son personales y no atribuibles a UTE. (Ejemplo: ". Yo trabajo para UTE, todas las opiniones expresadas son mías y no representan necesariamente la posición y/o opiniones de mi empleador")

Si usted no es un portavoz oficial de UTE y se encuentra con comentarios positivos o negativos acerca de UTE o de sus productos en línea que usted cree que es importante, considere remitírselas a la unidad de Comunicación Corporativa y Responsabilidad Social.

6.5 POLÍTICA SOBRE CONTROLES DE SEGURIDAD LÓGICA

U-TIC y las UARI´s, deben:

- Especificar y justificar los apartamientos de la Política de Seguridad de la información, motivados por limitaciones técnicas, recursos o como consecuencia del análisis de riesgo realizado, los cuales deben ser aprobados por la línea jerárquica correspondiente.
- Intercambiar información sobre cualquier incidente de seguridad que pueda afectar alguno de los recursos que dichas unidades administran.
- En sus respectivos planes anuales de seguridad establecerán las revisiones de seguridad de los sistemas operacionales, las pruebas de vulnerabilidad y auditorías independientes que serán realizados por personal competente.

Como criterio general, en caso de existir razones de servicio que desaconsejen el uso de los mecanismos previstos en este Punto, deberán establecerse controles compensatorios suficientes que minimicen los riesgos cubiertos por dichos mecanismos.
Siempre que se apliquen las excepciones o salvedades establecidas en estas políticas, se deberán documentar adecuadamente las solicitudes, justificaciones y autorizaciones correspondientes. Todo apartamiento, excepción o salvedad a estas políticas deberá ser considerado cuando se realice el análisis de riesgo mencionado en el primer párrafo de este punto.

6.5.1.- Administración

Se debe definir y documentar la responsabilidad y los procedimientos para la gestión de controles de seguridad de los sistemas de información así como los procedimientos para la asignación de los permisos de administración.
Los cambios a los controles de seguridad del sistema deben ser autorizados y documentados de acuerdo con procedimientos de administración definidos que sean monitoreados y verificados en forma independiente.
Debe controlarse el acceso a los sistemas de información a través de identificadores únicos (usuario y contraseña), los que no habrán de ser compartidos.
Se permite el uso de usuarios genéricos para ejecutar tareas específicas y/o desatendidas justificándose su carácter excepcional y manteniendo la responsabilidad funcional sobre dichas tareas.
La administración de los usuarios predefinidos en el software adquirido a terceros, debe ser 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".

6.5.2.- Autenticación de los usuarios

Como mínimo los usuarios deben identificarse y autenticarse mediante dos identificadores únicos (usuario y contraseña) al inicio de cada sesión.
Las contraseñas de los usuarios deben estar sujetas a reglas definidas por la unidad Seguridad de la Información, validadas por el Comité de Seguridad, que minimicen los riesgos de violación de la seguridad lógica.
El software de administración de la seguridad lógica debe obligar a los usuarios a cambiar la contraseña una vez transcurrido el período de cambio obligatorio y la primera vez que el usuario ingresa al sistema después del alta o de un cambio de contraseña.
Dicho período será definido por U-TIC o las UARI’s en el ámbito de su competencia.

Debe existir un proceso formal para la administración de las solicitudes de alta, baja y modificación de usuarios y cambio de contraseña para los sistemas de información. Este proceso debe incluir un mecanismo que permita registrar dichas solicitudes. Estos registros deben quedar accesibles con motivos de auditoria durante 5 años.
La entrega de la contraseña deberá realizarse bajo recibo y por medio de un procedimiento que garantice la entrega efectiva a la persona que corresponde y la obligación de su cambio luego del primer ingreso.
Las excepciones a este punto deberán estar documentadas y justificadas.
Los privilegios de acceso de los usuarios, sistemas y programas, deben estar restringidos sobre la base de los principios: “necesidad de hacer”, “necesidad de saber”, “separación de funciones” y “oposición de intereses”.

6.5.3.- Controles para accesos remotos

Cuando se deba acceder a algún recurso desde fuera de las redes de UTE se deberán utilizar los mecanismos de seguridad definidos por la unidad de Seguridad de la Información a tales efectos.
Debe existir un proceso formal para la administración de las solicitudes de alta, baja y modificación para estas autorizaciones. Estos registros deben quedar accesibles con motivos de auditoría durante 5 años.

6.5.4.- Revocación de derechos de acceso

Debe hacerse una revisión de los derechos individuales de acceso cuando se alteran las tareas de un usuario, por ejemplo, como resultado de una transferencia a otra unidad.
Debe existir un procedimiento donde se indique que si un usuario no es utilizado por un período determinado, será bloqueado automáticamente. Adicionalmente se eliminarán en forma periódica los usuarios bloqueados con determinada antigüedad la cual será establecida en el procedimiento. A las personas que cesan su relación laboral con UTE, una vez registrada la baja en el sistema por Gestión Humana, se les debe eliminar los usuarios y permisos de acceso.

6.5.5.- Controles de seguridad

Las sesiones de estaciones de trabajo sin actividad luego de un período determinado deben desconectarse automáticamente o bloquearse, en caso de ser posible.
Debe llevarse un registro automático de los accesos a datos de alto riesgo y deben generarse rastros de auditoria que permitan ser revisados en forma independiente.
Todas las aplicaciones deberán contar con una funcionalidad de control de accesos.
Las UARIs en sus respectivos ámbitos de acción, deberán identificar los procesos y parámetros de seguridad críticos que definen el alcance de los sistemas de control de acceso siendo responsables de controlar en sus respectivos ámbitos que los mismos se estén realizando de acuerdo a lo definido. Los cambios a estos procesos y parámetros deben ser autorizados por la Gerencia de División o superior respectiva.
Salvo por razones debidamente justificadas, la cantidad de usuarios con permisos de administración sobre los sistemas de control de accesos debe estar restringida al mínimo indispensable para realizar eficientemente las tareas del cargo, debiendo existir “oposición de intereses” y “separación de funciones” entre los administradores de los sistemas de control de accesos (usuarios y permisos) y los administradores de recursos.
Los administradores deben contar con los conocimientos necesarios para realizar sus tareas, acompasando las actualizaciones tecnológicas que así lo ameriten.

Los administradores, para desarrollar sus tareas, deberán utilizar herramientas que permitan una adecuada separación de funciones y que registren en bitácoras adecuadamente protegidas de accesos no autorizados las actividades realizadas. Las bitácoras deberán mantenerse durante el periodo definido por el responsable de la información para permitir su utilización con fines de control y auditoria.
Se deben supervisar anualmente los perfiles de acceso asignados a los administradores de recursos y las tareas por ellos realizadas. En caso de no ser posible se deberán documentar y justificar las excepciones.
Los administradores de TI no deben acceder a los equipos de los usuarios sin el consentimiento de los mismos, incluyendo la asistencia remota, salvo por incidentes de seguridad y riesgos en la disponibilidad de los servicios informáticos. Cuando se haga uso de esta excepción, deberá comunicarse el hecho y su justificación al usuario y/o al superior inmediato del mismo, en forma inmediata y por un medio de comunicación fehaciente.
Ante una investigación administrativa, no se podrá acceder a la información 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 de la línea jerárquica con un nivel no inferior a Gerente de División, y el contralor de la persona involucrada o un representante por él designado o, cuando esto no sea posible, un representante del personal.

6.6 POLÍTICA SOBRE CONTROLES DE SEGURIDAD FÍSICA

La implementación de una adecuada seguridad física en todas Instalaciones de infraestructura tecnológica de UTE es necesaria a los efectos de:

- Evitar la utilización no autorizada de los recursos.
- Garantizar que los recursos están protegidos contra peligros naturales, hurto y daño.

6.6.1.- Acceso físico

El acceso físico al equipamiento informático, fuentes de energía eléctrica, cableado, aire acondicionado, provisión de agua, sector de conexiones de telecomunicaciones y periféricos, debe limitarse al personal que lo necesita para el desempeño de sus tareas habituales.
El acceso físico a las instalaciones y al equipamiento informático será autorizado por el responsable de la instalación de acuerdo a un procedimiento establecido para ello.
Debe registrarse en un sistema de control de visitas, cualquier acceso por parte de terceros y funcionarios a los locales con equipamiento informático crítico, cualquiera sea el motivo de la visita. Al acceder al local, la persona deberá estar debidamente identificada, bien presentando su cédula de identidad o su tarjeta de identificación de funcionario.

6.6.2.- Controles y servicios auxiliares

Las instalaciones deben contar con rutas de escape y salidas de emergencia adecuadamente señalizadas, para facilitar la evacuación del personal en forma rápida y segura en caso de siniestro.

El equipamiento informático crítico debe albergarse en un ambiente equipado con dispositivos para la detección y extinción de incendios. Los dispositivos mencionados deberán ser probados de acuerdo a las especificaciones del fabricante. Deben contar con fuentes de energía ininterrumpible (UPS, bancos de baterías, inversores y grupos generadores si corresponde) para garantizar la disponibilidad del servicio en caso de falla del suministro de energía eléctrica, de acuerdo a los niveles de servicio requeridos.
Deben tomarse las precauciones necesarias para asegurar un ambiente con los niveles de temperatura y humedad requeridos por los fabricantes del equipamiento informático.
Las Instalaciones de infraestructura tecnológica de UTE deben tener un sistema de control que permita monitorizar todos los servicios auxiliares (detectores de humo, temperatura y humedad) y que permita visualizar la actividad en cada una de las salas.
Los controles de acceso físico y lógico para las copias de respaldo (back-up) de registros y datos esenciales que se conservan en bóvedas de almacenamiento deben tener como mínimo el mismo nivel de protección que se da para los originales.
Los soportes que se utilizan para mantener datos fuera de línea deben tener el mismo nivel de protección que se brinda para los datos en línea.
Todo el equipamiento informático debe estar identificado e inventariado mediante un código único que además se pueda visualizar en el equipo y cualquier modificación al inventario debe ser autorizada por U-TIC o por la UARI si corresponde a equipamiento dentro de su ámbito de acción.
Anualmente las UARIs en sus respectivos ámbitos de acción deben realizar una revisión general de las Instalaciones de infraestructura tecnológica de UTE: y de su equipamiento informático, que incluya la verificación de los contratos de seguros sobre la base de un análisis costo-beneficio y a las directrices impartidas por la Empresa.

6.7 POLÍTICA DE USO DE DISPOSITIVOS MOVILES

A los efectos de la presente política se consideran dispositivos móviles los teléfonos celulares inteligentes, tabletas, lectores tipo PDA y computadores portátiles (laptops, netbooks, etc.).

6.7.1.- Condiciones de uso

Los servicios publicados en internet podrán ser accedidos desde cualquier dispositivo móvil. Los restantes servicios y recursos sólo podrán ser accedidos desde los dispositivos provistos por UTE.

Los dispositivos móviles provistos por UTE deben utilizarse para actividades de carácter laboral.
Cuando exista una solicitud de entrega del dispositivo móvil de UTE, por parte de U-TIC lo cual puede ser por razones de auditoría, administración o configuración, los usuarios son responsables de entregarlos al Centro de Atención de Usuarios.
El usuario debe tener el debido cuidado de la integridad física del dispositivo.
Los usuarios no tienen permitido realizar ni autorizar ningún arreglo o servicio para el dispositivo que tenga asignado.

6.7.2.- Pérdida o robo de dispositivos de UTE

Es responsabilidad del usuario tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo.

Si el dispositivo está perdido, robado o se sospecha que está comprometido en cualquier sentido, el usuario debe notificar inmediatamente al Centro de Atención a Usuarios de la situación y realizar la denuncia policial correspondiente. Esta notificación y la denuncia deben tener lugar para poder cancelar cualquier servicio móvil asociado al dispositivo, así como también borrar remotamente la información contenida en la memoria del mismo en la medida de lo posible.

6.7.3.- Aplicaciones y descargas en dispositivos de UTE

Todo el software para el dispositivo debe ser provisto e instalado o aprobado por U-TIC o la UARI correspondiente.

6.7.4.- Respaldo, administración de archivos, sincronización y antivirus

El software necesario para realizar respaldos, sincronización de datos y de contactos será proporcionado y/o autorizado por U-TIC.
Es responsabilidad del usuario:

- Realizar los respaldos de la información contenida en el dispositivo.
- Notificar a U-TIC cuando detecte un incorrecto funcionamiento del antivirus o ante sospecha de desactivación u otra anomalía.

6.7.5.- Funcionalidades y características de manejo

El Hardware, sistema operativo y utilitarios que vienen instalado de fábrica y forman parte del dispositivo no deben sufrir cambios a menos que hayan sido requeridos y autorizados por U-TIC o las UARI´s según corresponda. No está permitido que el usuario realice el desbloqueo de las limitaciones del fabricante y/o proveedor (root/jailbreak), o que realice cualquier otro método de cambio de las protecciones.

6.7.6.- Seguridad del Usuario

Ley Nº 19.061 artículo 13: “Se 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, excepto cuando el desarrollo de la comunicación tenga lugar sin emplear cualquiera de las manos”.

6.7.7.- Obligaciones de Seguridad y Privacidad para los datos de la empresa

Los usuarios deben 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. Los usuarios no deben:

- Compartir el dispositivo.
- Compartir usuario, contraseña, PIN u otro tipo de credencial.
- Compartir medios de comunicación.

6.7.8.- Buenas prácticas para la protección de los datos

Los usuarios de dispositivos móviles deben cumplir con las políticas de seguridad tanto cuando los usen en el puesto de trabajo como cuando estén fuera de la empresa.
Las instalaciones no gestionadas o no aprobadas comprometen el ambiente operativo y también constituyen un riesgo de seguridad, incluyendo el esparcimiento de virus o software malicioso tanto con o sin intención.
Los usuarios deben respetar las siguientes medidas preventivas de seguridad para proteger la información y las aplicaciones instaladas en el dispositivo:

- Los dispositivos no deben quedar a la vista en un vehículo desatendido aunque sea por un período corto de tiempo.
- Los dispositivos no deben ser dejados en un vehículo durante toda la noche.
- Los dispositivos deben estar posicionados de manera que no queden visibles desde una ventana de la planta baja.
- Si en la pantalla de un dispositivo móvil se está mostrando información sensible en un lugar público se debe posicionar de tal manera que la información no pueda ser vista por otros.
- En situaciones vulnerables (aeropuertos, hoteles, centro de conferencias, etc.) el dispositivo no debe quedar desatendido bajo ninguna circunstancia.
- Los dispositivos deberán ser cargados como equipaje de mano cuando se viaja
- No se debe mover información desde un dispositivo a otro usando bluetooth.
- Solo está permitido copiar información sensible o confidencial al dispositivo móvil o de almacenamiento extraíble cuando sea requerida para trabajar en modo desconectado. En caso de realizarlo la información debe estar encriptada con los mecanismos que provea U-TIC.
- Para asegurar un almacenamiento adecuado se debe mantener la copia de datos al mínimo, sólo los datos o contenido que sea necesario para propósitos laborales.

6.7.9.- Responsabilidades

El responsable de autorizar el uso de dispositivos móviles de UTE a sus colaboradores, debe ser un superior de nivel gerencial.
U-TIC es responsable de:

- La identificación e inventario de los dispositivos móviles como propiedad de UTE en forma visible. Dicha identificación deberá ser resistente a su remoción.
- Establecer las condiciones de uso de los dispositivos móviles y comunicar las mismas a los responsables identificados en el inventario.
- Proveer el software necesario para realizar respaldos, sincronización de datos y de contactos, así como también el antivirus necesario para la protección de los dispositivos.
- Garantizar que las tecnologías, aplicaciones y medios de comunicación utilizados sean seguros y confiables.
- Asegurar que las aplicaciones para dispositivos móviles estén disponibles y optimizadas.
- Determinar las medidas de seguridad mínimas que deben tener los equipos a adquirir.

La unidad que realice el proceso de adquisición y recepción dispositivos móviles de uso operativo específico deberá coordinar con U-TIC para inventariarlo. En caso de ser posible los equipos contarán con al menos las siguientes medidas de seguridad:

- Bloqueo de operación mediante contraseña.
- Encriptación de archivos con información confidencial o reservada.
- Antivirus habilitado y actualizado.

No es responsabilidad de U-TIC recuperar ningún tipo de información en caso de que el dispositivo se haya perdido, haya sido robado o dañado.
Es responsabilidad de los usuarios de dispositivos móviles de UTE:

- El cumplimiento de las condiciones de uso establecidas por U-TIC en lo relativo al hardware y al software en él instalado, tanto cuando estos sean utilizados dentro como fuera de la Empresa.

- Llevar el dispositivo al Centro de Atención de Usuarios cuando sea solicitado por U-TIC ya sea por razones de auditoría, administración o configuración.
- Tener el debido cuidado de la integridad física del dispositivo.
- tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo.
- En caso de pérdida, robo, el usuario deberá notificar inmediatamente al Centro de Atención a Usuarios de la situación y realizar la denuncia policial correspondiente.
- Realizar los respaldos y verificar que el antivirus se encuentre activo y actualizado.
- Evitar el bloqueo de las limitaciones del fabricante y/o proveedor (root/jailbreak), o realizar cualquier otro método de cambio de las protecciones con las que se entregó el dispositivo.
- El cumplimiento de la Ley Nº 19.061 artículo 13 el cual 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.

6.8 POLÍTICA DE MANEJO DE MEDIOS DE ALMACENAMIENTO

Se deben implementar procedimientos adecuados para la gestión de los medios de almacenamiento:

- Deben eliminarse en forma segura y sin peligro cuando no se necesiten más, de acuerdo a los procedimientos definidos por las UARIs.
- Debe establecerse procedimientos de utilización y almacenamiento de la información para protegerla de su mal uso o divulgación no autorizada.
- Antes de su disposición deben revisarse los medios de almacenamiento para asegurar que los datos confidenciales y/o sensibles y software licenciado se haya removido o sobre escrito con seguridad.

6.9 GESTIÓN DE CONTINUIDAD DE LOS SISTEMAS DE INFORMACIÓN

La información, las instalaciones y componentes críticos de tecnología de información deben contar con alternativas adecuadas que permitan asegurar la continuidad de las operaciones de la Empresa y reducir al mínimo los daños causados por una contingencia. Deben estar vigentes procedimientos que permitan que la organización restablezca los servicios del negocio ante esta eventualidad.

6.9.1.- Plan de Continuidad

Debe proveerse a los sistemas de información de procedimientos de recuperación en caso de contingencia, que incluyan los niveles de criticidad acordados y documentados para realizar la recuperación en el caso de desastres o fallas de los sistemas. Esto permitirá recuperar los recursos más críticos en primer lugar. Los niveles de criticidad deberán surgir de un proceso formal de evaluación de riesgos en el cual participen activamente los responsables funcionales de los sistemas de información, U-TIC y/o las UARIs según el ámbito de aplicación. Los niveles de criticidad así acordados deberán quedar debidamente documentados.
La elaboración, mantenimiento y pruebas periódicas de los planes y procedimientos de continuidad debidamente documentados, serán responsabilidad de cada uno de los responsables funcionales. Los mismos contarán con el apoyo de las UARIs y las Administraciones de cada sistema.

Las UARIs, en sus respectivos ámbitos de acción, deben acordar con los proveedores (internos o externos) de servicios críticos, tiempos de repuesta que permitan garantizar el restablecimiento del servicio en ocasión de una contingencia.
Deben almacenarse copias del Plan de Continuidad en lugares físicamente independientes con los niveles de seguridad y control adecuados.

6.9.2.- Respaldos

Los soportes conteniendo los respaldos (backups) deben protegerse adecuadamente durante el transporte desde y hasta su lugar de almacenamiento externo.
Debe definirse y documentarse la frecuencia con que se hacen copias de respaldo (back-up) y el período de conservación de los mismos
Ante cambios de gran impacto debe estar previsto un procedimiento para retornar a la situación anterior.
La información almacenada debe ser probada periódicamente para asegurar que sea recuperable.
Debe garantizarse para la información de respaldo como mínimo la misma confidencialidad que para la de origen. La recuperación de un respaldo debe estar autorizada por un usuario con permiso de acceso a dicha información.
La solución integral de respaldo debe asegurar la confiabilidad y calidad requerida.

6.9.3.- Servicios a terceros en situación de contingencia

En los acuerdos de nivel de servicio brindados a terceros se deberán incorporar cláusulas en las cuales se indique que frente a situaciones de contingencia en UTE el servicio brindado podrá verse afectado.

6.10 POLÍTICA DE CONTROLES SOBRE ADMINISTRACIÓN DE EQUIPOS INFORMATICOS

Es esencial un control efectivo de las operaciones realizadas en el equipamiento informático, para asegurarse que los sistemas de información funcionan en un ambiente seguro.

6.10.1.- Administración del hardware y software

Las tareas de administración de hardware y software corresponden a U-TIC y las UARIs en sus respectivos ámbitos de acción (ver anexo A). Las mismas podrán ser delegadas en otras unidades de la Empresa siempre que existan las razones de servicio que así lo justifiquen. Deberá documentarse por escrito las tareas que sean delegadas.
El hardware y software debe ser instalado, administrado y mantenido de acuerdo a normas definidas y documentadas.
Los sistemas críticos deben ser soportados por instalaciones y equipamiento que garanticen los niveles de disponibilidad definidos y acordados.
Deben registrarse los resultados de la ejecución de los procesos “no atendidos” en el ambiente de producción.
El personal de operaciones del centro de cómputos no debe tener acceso a programas, utilitarios o comandos que les permita modificar datos de producción en forma no autorizada.
Todo software (incluyendo el software de libre distribución o en demostración) que se instale en los equipos informáticos debe contar con el visto bueno de U-TIC o la UARI en su ámbito de acción, a efectos de asegurar la continuidad de la operación, el cumplimiento de los estándares de seguridad, y requisitos legales vigentes.

U-TIC y las UARIs en sus respectivos ámbitos de acción, deberán remover, en el momento de detectarlo, cualquier software instalado en un equipo informático que no cumpla con cualquiera de los puntos de la presente política.

6.10.2.- Bitácoras relevantes para la seguridad de la información

Todo sistema deberá guardar en la bitácora la información necesaria y suficiente para identificar quién, cuándo y cómo accedió y/o modificó, qué información crítica y/o confidencial.
Las UARIs mantendrán un inventario actualizado de las bitácoras relevantes para garantizar la continuidad del negocio y las que registren acceso a información crítica y/o confidencial. Por ejemplo el inventario deberá incluir las bitácoras correspondientes a:

- Sistemas en producción,
- Acceso a bases de datos,
- Correo electrónico,
- Accesos a Internet,
- Accesos a través de VPN
- Accesos a los servidores de archivos y aplicaciones críticas,
- actividades realizadas por usuarios de tipo administrador,
- Operaciones realizadas en cualquier equipo crítico (por ej. cortafuegos, detectores de intrusos, etc.).

El registro de las bitácoras debe mantenerse por el periodo establecido en los acuerdos de nivel de servicio. En caso que no esté establecido deberá mantenerse durante un año.
En situaciones excepcionales se permitirá la desactivación de acuerdo al procedimiento establecido por U-TIC o la UARI en su ámbito de acción, debiendo darse aviso a la administración funcional o a la unidad Seguridad de la Información según corresponda. Este procedimiento debe incluir:

- Documentación sobre los motivos de las excepciones y autorizaciones otorgadas
- Medidas para limitar los accesos al mínimo imprescindible.
- Criterios para guardar los documentos.
- Medidas compensatorias a aplicar cuando se desactiven bitácoras de seguridad y las que registran el acceso a información crítica y/o confidencial.

La unidad Seguridad de la Información o la línea jerárquica de la UARI en su ámbito de acción, realizará un seguimiento de las desactivaciones y podrá investigar las mismas a efectos de adoptar las medidas preventivas y correctivas necesarias.
Queda prohibido borrar y/o alterar, total o parcialmente, el contenido de una bitácora sin que previamente se haya realizado una copia de respaldo de la misma.

6.11 POLÍTICA DE ADMINISTRACIÓN DE CAMBIOS QUE AFECTEN LA SEGURIDAD DE INFORMACIÓN.

Los procedimientos de cambios deben proveer un enfoque formal, permitiendo que los cambios individuales se apliquen en forma controlada y coherente ya que existe un riesgo de que ocurran errores no intencionales o alteraciones indebidas tras la aplicación de los mismos.

6.11.1.- Gestión de cambios

Debe existir un procedimiento de control de cambios que brindará el método con el cual se mantendrá toda la información sobre un cambio determinado.

Deben evaluarse los riesgos (incluyendo el impacto sobre la seguridad) de cambios al sistema informático de manera que se pueda notificar con tiempo a todos los usuarios y deben existir procedimientos de recuperación para restablecer las operaciones en caso de ocurrir una falla.
Deben probarse todos los cambios antes de que se apliquen al ambiente de producción, para reducir el riesgo de una falla.
Los cambios deben ser autorizados por el responsable del equipo de soporte del sistema que realizará el cambio y los responsables funcionales de la aplicación.
Una misma persona no debe iniciar, aprobar e implementar los cambios.

6.11.2.- Cambios de emergencia

Se acepta que en ocasiones se requiera realizar cambios de emergencia. Tales cambios pueden llegar a ser implementados antes de su aprobación, pero deben ser documentados exhaustivamente, sujetos a aprobación posterior e informados al responsable funcional.
La unidad Seguridad de la Información y las UARIS en su ámbito de acción, realizarán un seguimiento de los cambios de emergencia realizados y podrán revisar periódicamente los mismos e informar al responsable funcional que corresponda.

6.11.3.- Cambios a programas relacionados con la seguridad de la información

Los cambios a programas relacionados con la seguridad de la información deberán ser aprobados por la unidad Seguridad de la Información o por la UARI antes de su puesta en producción.

6.12 POLÍTICA SOBRE DESARROLLO DE SISTEMAS

Los controles sobre el desarrollo de los sistemas de aplicación son esenciales para asegurar que los sistemas:

- Cumplen los requerimientos de la Organización.
- Incluyen un nivel adecuado de seguridad y control.
- Son probados y documentados antes de ser puestos en producción.

Los recursos deben ser probados y documentados antes de ser puestos en entorno de producción.
U-TIC tiene el rol de coordinación e integración para la definición de las políticas y estándares de seguridad para el desarrollo de aplicaciones en UTE.
Las unidades de negocio son responsables de los servicios que prestan de acuerdo a los objetivos de la empresa. En este marco funcional, deciden y aprueban los servicios informáticos que necesitan siguiendo las estrategias corporativas en seguridad y tecnologías de información de UTE.
Las aplicaciones pueden ser desarrolladas por U-TIC o por las UARIs en su ámbito de especialización.
Los desarrollos de aplicaciones que van a utilizar las redes de datos obligatoriamente deben tomar en consideración la afectación de los anchos de banda disponibles en UTE.
Deberán acordarse con U-TIC los anchos de banda requeridos por las aplicaciones que utilicen significativamente este recurso.

6.12.1.- Metodología de desarrollo de sistemas

La metodología de desarrollo de sistemas debe incluir:

- Requerimientos funcionales

- Requerimientos de seguridad
- Niveles de prueba
- Procedimientos de implementación
- Pruebas de aceptación por los responsables funcionales
- Respaldos periódicos de los programas en desarrollo
- Control de las versiones de un programa

Toda solicitud de desarrollo o mantenimiento de software debe tener una especificación formal escrita (diseño conceptual / diseño funcional) y debidamente aprobada por la unidad dueña de la información.
Deben aplicarse las normas de documentación a todo el ciclo de desarrollo de un sistema e incluirse las especificaciones técnicas de las medidas de seguridad que se hayan implementado, de modo que pueda ser mantenido por personas que no hayan participado en el desarrollo.
Los ambientes de desarrollo y prueba deben mantenerse estrictamente separados del ambiente de producción, siempre que técnicamente sea posible.
Antes de pasar el software de aplicación en desarrollo al entorno de producción, se le deben 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.
El equipo de desarrollo no debe tener 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.
La transferencia de los programas de aplicación y las estructuras de datos del ambiente de desarrollo a producción debe realizarla el jefe de equipo de soporte o las personas autorizadas por él.
Se deben eliminar del software, antes de su puesta en producción, todos los caminos de acceso no autorizados (puertas traseras, atajos, etc.).
Si los requerimientos de seguridad lo ameritan, deberán realizarse pruebas de vulnerabilidad antes de poner en producción una aplicación.

6.12.2.- Desarrollo de programas relacionados con la administración de usuarios y permisos de acceso a recursos

La unidad Seguridad de la Información debe participar activamente en el diseño, desarrollo, prueba y puesta en producción de los programas utilizados para automatizar tareas relacionadas con la administración de usuarios y permisos de acceso a recursos en el ámbito de U-TIC. Ninguno de estos programas podrá ser puesto en producción sin la aprobación previa de la mencionada unidad.

6.13 POLÍTICA SOBRE CONTROLES EN LA COMUNICACIÓN DE DATOS

El aumento de la utilización de sistemas de comunicación de datos ha incrementado la importancia de la seguridad de las redes para proteger los sistemas informáticos. Se requieren controles para asegurarse que los mensajes no se corrompan y evitar accesos no autorizados.
Debe protegerse con mecanismos de control de acceso físico y/o lógico los componentes de la red de comunicaciones de UTE.
U-TIC debe contar con herramientas para verificar que el consumo de las aplicaciones cumpla con los anchos de banda acordados.
U-TIC, y la UARI involucrada deberán actuar en forma coordinada en materia de administración y mantenimiento del hardware y software correspondiente a la red de comunicaciones de UTE.

U-TIC y la UARI involucrada deben mantener actualizada la documentación que describe la red de comunicaciones.
U-TIC es la unidad responsable de ampliar, modificar y administrar la red de telecomunicaciones de la Empresa. Toda modificación o ampliación significativa de la red corporativa de comunicaciones de UTE, deberá ser coordinada con U-TIC.
Se deben cambiar las contraseñas por defecto de todos los componentes de comunicaciones antes de su incorporación a la red de comunicaciones de UTE. Las contraseñas además deben estar sujetas a reglas para "Autenticación de Usuarios" de acuerdo a lo descrito en el punto "Autenticación de los Usuarios" de la presente política.
Los componentes de la red de comunicaciones de UTE deben:

- Utilizar protocolos de comunicación con un adecuado nivel de seguridad.
- Permitir, siempre que sea posible, su gestión remota.

La conexión a las redes de comunicaciones de la Empresa de cualquier equipamiento informático que no sea propiedad de UTE, estará sujeta a autorización gerencial previa basada en razones de servicio
Los equipos informáticos (PC o computadoras portátiles) que requieran conectarse con un dispositivo (medidor, relé, etc.) utilizando la red de UTE, deberán hacerlo de acuerdo a un procedimiento que garantice la seguridad de la misma.
Cualquier conexión de comunicaciones entre locales de UTE no contiguos o con terceros (suministradores de servicios u otras Empresas) debe tramitarse a través de U-TIC.
En lo que respecta a equipamiento inalámbrico:

- Se deben cumplir los estándares y los procedimientos y controles internos para que las implementaciones inalámbricas resulten suficientemente seguras, manteniendo las mismas adecuadas a los cambios tecnológicos.
- No está permitida la conexión en forma simultánea de una máquina a la red de UTE y a cualquier otra red externa a UTE.
- El diseño y administración de estas redes, así como la adquisición del equipamiento se realizará en forma coordinada con U-TIC.
- U-TIC debe realizar controles para detectar dispositivos no autorizados instalados en la Red de UTE y en caso de encontrar equipos en esas condiciones se tomarán las acciones correctivas correspondientes.

6.14 POLÍTICA DE CONTROLES SOBRE SOFTWARE MALICIOSO

Los usuarios no deben intentar erradicar del equipo software malicioso, como ser virus, troyanos, gusanos, spyware, etc. En caso de sospecharse una infección se debe dejar de utilizar el equipo y llamar al Centro de Atención de Usuarios en forma inmediata. Además, deberá suspenderse el uso de cualquier dispositivo de almacenamiento utilizado en la computadora infectada.
Todo software, antes de su instalación o ejecución, deberá ser revisado a efectos de verificar que se encuentra libre de virus. Si el software está encriptado y/o comprimido deberán verificarse, además, los archivos resultantes de su desencriptación y/o descompresión.
Los archivos provenientes de una fuente externa solo podrán ser utilizados después de haber sido controlados con el software antivirus.
U-TIC será responsable de seleccionar e implementar como estándar el software antivirus destinado a la protección de las estaciones de trabajo, dispositivos móviles y servidores de la red. Periódicamente se actualizará el estudio realizado.

Todos los equipos informáticos deberán tener instalado y funcionando en las condiciones establecidas el software antivirus seleccionado como estándar. Se prohíbe al usuario la deshabilitación del mismo y la realización de cambios en la configuración, los cuales podrán ser efectuados exclusivamente por U-TIC o la UARI en su respectivo ámbito de acción.
Cuando por alguna razón no sea posible instalar software antivirus en un equipo, se deberán adoptar las medidas compensatorias necesarias y suficientes para reducir los riesgos derivados del software malicioso.
El software que se distribuya a terceras partes deberá ser sometido, previamente, a pruebas de detección de posibles virus. Deberán documentarse los objetivos, las herramientas utilizadas y los resultados de dichas pruebas.
Deberán instalarse en todos los equipos informáticos, todas las actualizaciones que el proveedor del software antivirus publique y que mejoren las capacidades del producto.
La unidad Seguridad de la Información y cada UARI en su ámbito de acción, verificará periódicamente en todos los servidores y las estaciones de trabajo que el software antivirus está instalado, funciona en las condiciones establecidas y se encuentra actualizado.
La unidad Seguridad de la Información enviará a todos los usuarios, cuando corresponda, información y material de referencia sobre los virus y los productos antivirus así como sobre las obligaciones y políticas establecidas.

6.15 POLÍTICA SOBRE ADQUISICIÓN DE HARDWARE, SOFTWARE y SERVICIOS

Siempre que se adquiera hardware, software y/o servicios para procesar información de la empresa se deberá evaluar los antecedentes del proveedor, la continuidad y certificaciones del proceso, producto y/o servicios.
La seguridad debe ser considerada desde la especificación de los requerimientos hasta su implementación y los requerimientos de seguridad deben estar identificados y documentados.
Todo proveedor debe garantizar que el software y/o hardware no contiene ningún código desarrollado para poner en riesgo la seguridad de la información.
En caso de detectarse tal tipo de código, el proveedor deberá emplear todos los esfuerzos razonables consistentes con las prácticas de desarrollo comunes en la industria para resolverlo tan pronto como sea posible.
Las contraseñas que provee el proveedor deberán ser cambiadas, en forma inmediata una vez terminada su instalación, por otras que cumplan con las reglas definidas en la presente política, excepto que exista una razón técnica que lo haga desaconsejable (lo cual se deberá documentar).
La adquisición de equipamiento informático, dispositivos móviles y/o software de uso corporativo debe ser gestionada a través de U-TIC o por otras unidades en coordinación con U-TIC, salvo excepciones que serán debidamente documentadas.
Todo software que se adquiera deberá contar con una licencia que permita la realización de copias con fines de respaldo.

6.16 POLÍTICA SOBRE VENTA DE SOFTWARE Y SERVICIO DE PROCESAMIENTO A TERCEROS

En caso de venta de software se deberá revisar la documentación y los procedimientos que describen una aplicación (o una versión de la misma), antes de que sean entregados al comprador, a efectos de verificar que no se está divulgando información reservada y/o confidencial.

En el caso de brindar servicio de procesamiento a terceros, se deberá implementar una adecuada separación de entornos de manera de no poner en riesgo la seguridad de la información de UTE ni la del servicio que se brinda.
En el caso de ventas de servicios de consultoría, se deben establecer las garantías necesarias para proteger la confidencialidad de la información de UTE
Los usuarios de UTE no tendrán acceso a los recursos informáticos, los sistemas de información ni a los datos del cliente, exceptuando aquellos que brindan el servicio de procesamiento (operación y administración), de acuerdo a los principios “necesidad de saber” y “necesidad de hacer”.

7.- RESPONSABILIDADES

La responsabilidad de la seguridad de la información corresponde a todas las personas que utilizan la información provista por UTE, sean funcionarios, becarios, consultores, proveedores, etc. Todos ellos están obligados a cumplir y hacer cumplir, en su marco de actuación, las políticas y procedimientos de seguridad vigentes.

7.1 RESPONSABILIDAD DE LA DIRECCIÓN

Es responsabilidad de la Dirección y de las gerencias y jefaturas de UTE, velar por el cumplimiento de esta Política, así como proveer los recursos necesarios para garantizar la seguridad de la información de la Empresa.

7.2 DE TODOS LOS USUARIOS

Se entiende por usuario a toda persona que hace uso de la información provista por UTE.

- Los usuarios deben notificarse de las políticas de acuerdo al procedimiento definido por la unidad Seguridad de la Información.
- Cada persona es responsable del uso adecuado de los recursos de TI que UTE le brinda para realizar sus funciones, así como del usuario y palabra clave (contraseña o password) que tiene asignado para el acceso a los sistemas de información. La contraseña debe ser 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 (digital, impreso, manuscrito, etc.).
- Los usuarios no deben:
  - Instalar software sin la previa autorización de U-TIC o la UARI según corresponda. En caso de instalar software deben tomar todas las medidas para cumplir con la presente Política.
  - Utilizar la información disponible en la Empresa, para otro fin que no sea el requerido para el desempeño de sus funciones. La tecnología informática así como la información que a través de ella se accede, es de uso y aplicación exclusiva a la función que cada usuario debe realizar para UTE. Está prohibido el uso de los recursos informáticos para la realización de actividades no laborales, como por ejemplo y no en exclusividad: actividades personales, con fines sociales, o de entretenimiento, el uso de juegos de computadoras, el acceso a, distribución o almacenamiento de material pornográfico, proselitista, racista, discriminatorio u ofensivo.

- Los usuarios deben reportar inmediatamente toda falla en el funcionamiento de los sistemas de información a la unidad responsable funcional del sistema en cuestión para determinar las causas reales y sus efectos.
- Los usuarios que detecten o sospechen cualquier incidente de seguridad deberán proceder de acuerdo a lo definido en el punto “Incidentes de seguridad” de la presente política.
- Cuando un empleado, consultor o personal contratado termina su relación laboral con UTE, debe devolver a su jefe de unidad todos los elementos que fueron suministrados por la Empresa para desarrollar sus tareas. Esto incluye computadoras portátiles, documentación, llaves, tarjetas magnéticas, etc.
- Está prohibida:

- La realización de pruebas de controles, pruebas de vulnerabilidad y/o pruebas de penetración, así como la instalación y/o el uso de herramientas informáticas que permitan alterar, burlar o desactivar los sistemas de seguridad; cualquiera sea el fin que con dichas pruebas o herramientas se persiga, salvo a aquellos funcionarios debidamente autorizados y en razón de la función que cumplen en la Empresa.
- La divulgación de información sobre el diseño, funcionamiento y posibles vulnerabilidades de los controles de seguridad informática utilizados en la Empresa,
- La divulgación de información sobre los incidentes de seguridad detectados y los efectos que provocaron en la Empresa.
- La instalación, escritura, generación, compilación, copia, propagación, ejecución o intento de introducir un código diseñado para dañar o afectar el rendimiento de cualquier computadora, sistema de archivo o software,
- La escritura y ejecución de cualquier programa o proceso que por sus características pueda utilizar recursos en una forma que comprometa los niveles de servicio.

Los usuarios deberán contar con autorización previa basada en estrictas razones de servicio, de U-TIC, o las UARIs según corresponda, para el ingreso a, la salida de y el cambio de ubicación en las instalaciones de la Empresa de cualquier equipamiento informático o de comunicaciones. Dichas unidades podrán, en forma expresa e individualizada, realizar excepciones a esta política, notificando al usuario que se hace responsable de cumplir con las medidas de seguridad definidas para ese equipo.

Se considera información confidencial toda información o conocimiento que sea provista en tal carácter al usuario, que esté clasificada como tal por UTE, o que contenga datos personales que requieran previo consentimiento informado de su titular para su divulgación. Es obligación de todos los usuarios:

- Mantener estricta y absoluta confidencialidad y reserva respecto de toda la información o conocimiento clasificado como confidencial
- Aplicar las correspondientes medidas de seguridad que sean razonables y prudentes para proteger la información referida y, en particular, aquella que se clasifique como reservada o confidencial,
- Utilizar la información confidencial solamente para el fin establecido, quedando prohibido todo uso o reproducción para beneficio propio o de terceros;
- Advertir a toda persona a la que se revele información confidencial, con la debida autorización, de su naturaleza confidencial
- Reportar a la unidad Seguridad de la Información toda divulgación de información confidencial no autorizada de la que tuviera conocimiento.

Es responsabilidad de los usuarios de dispositivos móviles de UTE:

- El cumplimiento de las condiciones de uso establecidas por U-TIC en lo relativo al hardware y al software en él instalado, tanto cuando estos sean utilizados dentro como fuera de la Empresa.
- Llevar el dispositivo al Centro de Atención de Usuarios cuando sea solicitado por U-TIC ya sea por razones de auditoría, administración o configuración.
- Tener el debido cuidado de la integridad física del dispositivo.
- Tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo.
- En caso de pérdida, robo, el usuario deberá notificar inmediatamente al Centro de Atención a Usuarios de la situación y realizar la denuncia policial correspondiente.

- Realizar los respaldos y verificar que el antivirus se encuentre activo y actualizado.
- Evitar el bloqueo de las limitaciones del fabricante y/o proveedor (root/jailbreak), o realizar cualquier otro método de cambio de las protecciones con las que se entregó el dispositivo.
- El cumplimiento de la Ley Nº 19.061 artículo 13 el cual 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.

7.3 DE LOS RESPONSABLES DE UNIDADES

- Todos los responsables de las unidades de la Empresa deben:
  - Controlar el cumplimiento de la presente Política de Seguridad de información por parte de su personal a cargo. En caso de detectar incumplimientos deberán adoptar las medidas que correspondan.
  - Implantar controles basados en la separación de tareas, de modo de asegurar que ningún individuo tenga control exclusivo sobre la información con alto grado de sensibilidad o criticidad, procesada por los sistemas informáticos de la Empresa.
- Son además responsables de solicitar:
  - El alta o modificación de usuarios para los sistemas de información y otros recursos tecnológicos,
  - La baja del personal (de la Empresa o externo) que se desvincula de UTE,
  - La revocación de los derechos de acceso a los sistemas de información de los usuarios que no los requieran para desempeñar sus tareas.
- Deben notificar al personal contratado y representante de cada empresa proveedora, vinculados a su unidad, que tengan acceso a información de UTE, del Compromiso de Confidencialidad Corporativo y mantener dicho registro por el tiempo de Vigencia que el mismo establece en su Cláusula Tercera.

7.4 DE LOS RESPONSABLES FUNCIONALES DE APLICACIONES INFORMÁTICAS

A los efectos de la presente política se entiende por responsables funcionales a la máxima autoridad jerárquica responsable del proceso de Negocio atendido por la aplicación informática, o a quien éste designe.
Los responsables funcionales de cada sistema de información son los encargados de:

- Definir los roles o perfiles funcionales asociados a las funciones que los usuarios realizan en dicho sistema,
- Autorizar las solicitudes y asignación de los roles o perfiles correspondientes,
- Verificar periódicamente que los perfiles efectivamente implantados en el sistema se corresponden con los definidos,
- Verificar periódicamente que los perfiles efectivos de los usuarios del sistema se corresponden con los autorizados por los jefes,
- Evaluar cada riesgo significativo en la seguridad de los sistemas de información, y realizar las gestiones necesarias para tomar una decisión específica sobre el grado de riesgo a asumir y las medidas a adoptar.
- Participar en el desarrollo, mantenimiento y ejecución del Plan de Continuidad del Negocio.
- Clasificar la información de sus sistemas de acuerdo a la categorización propuesta en esta política.

- Disponer la destrucción de la información confidencial al término de su vida útil.
- Cuando una unidad consume un servicio de información provisto y administrado por otra unidad se deberá establecer un Acuerdo de Nivel de Servicio. En dicho acuerdo quedará establecido quién es el dueño del recurso de información, qué responsabilidades le competen a cada parte, las condiciones en que se utilizará y compartirá el mismo y cuándo y en qué forma será mantenido.

7.5 DE LA UNIDAD SEGURIDAD DE LA INFORMACIÓN

El control de la seguridad de la información es responsabilidad de la unidad Seguridad de la Información de UTE. En el caso que existan razones de servicio que lo justifiquen, la mencionada unidad podrá delegar actividades del control de la seguridad en otras unidades de la Empresa lo cual deberá documentarse. La unidad en la que se deleguen las actividades del control de la Seguridad deberá actuar siempre de acuerdo a las políticas de la empresa y en coordinación con la unidad Seguridad de la Información.

La unidad Seguridad de la Información es responsable de:

- Instrumentar y difundir las políticas y procedimientos relativos a la seguridad informática, así como de revisar 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. Establecerá, además, los mecanismos para notificar estas políticas y sus modificaciones a todos los usuarios de los sistemas de información de UTE.
- Actuar como coordinador en temas de seguridad de la información entre todas las unidades de UTE.
- Diseñar los procedimientos para el reporte y administración de problemas, que permitan registrar los mismos, reducir su incidencia y prevenir su recurrencia. Los usuarios deben estar en conocimiento de estos procedimientos, los que serán difundidos en los planes de formación correspondientes.
- Informar periódicamente a los responsables funcionales de cada sistema de información sobre las incidencias de seguridad detectadas y los efectos que provocaron en la Empresa.
- Coordinar y dar soporte a las actividades de planificación de continuidad del negocio.
- Conservar bajo custodia, la información relativa a violaciones, problemas o investigaciones relacionadas con la seguridad de la información durante al menos cinco (5) años. Esta política se aplica a las bitácoras de los sistemas, y toda la documentación generada durante las investigaciones realizadas.
- A solicitud de los respectivos responsables debe autorizar los accesos a los recursos informáticos de todos los usuarios ajenos a la Empresa, dejando constancia de ello en la aplicación a través de la cual se realiza la solicitud. Estos accesos tendrán siempre una fecha de expiración no posterior a la fecha de finalización de la relación que une al usuario con la Empresa. El software de control de accesos debe bloquear automáticamente los usuarios que alcancen la fecha de expiración.
- Controlar los perfiles de acceso asignados a los administradores de recursos y las tareas de administración realizadas con dichos perfiles.

La unidad Seguridad de la Información en razón del cumplimiento de sus funciones, y tomando los recaudos necesarios para minimizar el riesgo de afectar la continuidad del negocio, están autorizada a:

- Realizar pruebas de controles, pruebas de vulnerabilidad y/o pruebas de penetración. Cuando estas pruebas involucren recursos informáticos de ambientes productivos, será obligatorio contar con el visto previo del responsable funcional correspondiente. La planificación de estas pruebas (incluyendo el análisis de riesgos realizado) así como los resultados de las mismas deben documentarse e informarse al responsable funcional correspondiente. Esta documentación deberá conservarse durante 5 años.
- La divulgación de información sobre el diseño, funcionamiento y posibles vulnerabilidades de los controles de seguridad informática utilizados en la Empresa,
- La divulgación de información sobre los incidentes de seguridad detectados y los efectos que provocaron en la Empresa.

UTE a través de la unidad Seguridad de la Información se reserva el derecho de:

- Bloquear preventivamente los permisos de acceso a cualquier usuario, si su conducta interfiere con la normal operación de los sistemas de información o no cumple con las presentes Políticas de Seguridad.
- Monitorear e inspeccionar todo uso de sus recursos de tecnología de información y ante situaciones irregulares iniciar investigaciones administrativas.

Las UARIs deberán informar a la unidad Seguridad de la Información las violaciones y problemas reportados en su ámbito de forma de contar con un único repositorio de incidentes.

7.6 DE AUDITORÍA INTERNA

En razón del cumplimiento de sus funciones y tomando los recaudos necesarios para minimizar el riesgo de afectar la continuidad del negocio, están autorizados a:

- La realización de pruebas de controles, pruebas de vulnerabilidad y/o pruebas de penetración. Cuando estas pruebas involucren recursos informáticos de ambientes productivos, las mismas deberán contar con la autorización del responsable funcional o su línea jerárquica. La documentación de estas pruebas (incluyendo el análisis de riesgos realizado) debe conservarse durante 5 años.
- La divulgación de información sobre el diseño, funcionamiento y posibles vulnerabilidades de los controles de seguridad informática utilizados en la Empresa,
- La divulgación de información sobre los incidentes de seguridad detectados y los efectos que provocaron en la Empresa.
- Auditar y controlar las actividades que involucren el manejo de información confidencial.

7.7 DE LAS UNIDADES ADMINISTRADORAS DE RECURSOS DE INFORMACIÓN (UARI)

U-TIC y las UARIs deben:

- Desarrollar un plan de seguridad. En los planes de seguridad deben especificar y fundamentar los apartamientos a las políticas. Estos apartamientos deben estar debidamente justificados ya sea por limitaciones técnicas o como consecuencia del análisis de riesgo realizado y deben ser aprobados por la línea jerárquica correspondiente.
- Realizar un análisis de riesgos en sus respectivos ámbitos de competencia.

- Identificar los procesos y parámetros de seguridad críticos que definen el alcance de los sistemas de control de acceso.
- Realizar periódicamente una revisión general de las instalaciones y de su equipamiento informático que incluya la verificación de los contratos de seguros sobre la base de un análisis costo-beneficio y a las directrices impartidas por la Empresa.
- Mantener actualizado el inventario del equipamiento informático.
- Elaborar y mantener actualizado el plan de continuidad operativa de los sistemas de información
- Administrar el hardware y software de base.
- Justificar la eventual desactivación de cualquiera de las bitácoras.
- Mantener los antivirus activos y actualizados.
- Supervisar los perfiles de acceso asignados a los administradores de recursos y las tareas por ellos realizadas.
- Cuando una unidad consume un servicio de información provisto y administrado por otra unidad se deberá establecer un Acuerdo de Nivel de Servicio. En dicho acuerdo quedará establecido quién es el dueño del recurso de información, qué responsabilidades le competen a cada parte, las condiciones en que se utilizará y compartirá el mismo y cuándo y en qué forma será mantenido
- Coordinar las interfases necesarias para garantizar la integración de la información corporativa.
- Revisar las licencias de software y controlar a los efectos de evitar la instalación de software no autorizado en los equipos.

Las UARIs en razón del cumplimiento de sus funciones, y tomando los recaudos necesarios para minimizar el riesgo de afectar la continuidad operativa de los sistemas de información, están autorizados a la realización de pruebas de controles, pruebas de vulnerabilidad y/o pruebas de penetración necesarias para chequear y controlar sus dispositivos de seguridad. En el caso que los dispositivos sean compartidos por más de una UARI, dichas pruebas deberán realizarse en conocimiento de todos los responsables. Cuando estas pruebas involucren recursos informáticos de ambientes productivos, será obligatorio contar con el visto previo del responsable funcional correspondiente. La planificación de estas pruebas (incluyendo el análisis de riesgos realizado) así como los resultados de las mismas deben documentarse por escrito e informarse al responsable funcional correspondiente. Esta documentación deberá conservarse durante 5 años.

U-TIC tiene el rol de coordinación e integración para la definición de las políticas y estándares de TI en UTE y es responsable de las soluciones informáticas corporativas.

7.8 DE LOS ADMINISTRADORES DE LA SEGURIDAD DE REDES

U-TIC y las UARIs deben proteger con mecanismos de control de acceso físico y/o lógico a los componentes de la red de comunicaciones de UTE, para evitar los accesos no autorizados. Si estos componentes están ubicados en instalaciones de otras unidades, las mismas serán responsables de implementar y mantener los mecanismos de control de acceso físico requeridos.

U-TIC y las UARIs en su ámbito de acción deberán actuar en forma coordinada en materia de administración y mantenimiento del hardware y software correspondiente a la red de comunicaciones de UTE.

TIC es la unidad responsable de:

- Ampliar, modificar y administrar la red de telecomunicaciones de la Empresa, garantizando que la misma cumpla con los mecanismos de control descritos en el capítulo “Controles de la comunicación de datos”. Toda modificación o ampliación de la red corporativa de comunicaciones de UTE, deberá ser coordinada en forma previa con U-TIC.
- Dotar a los sistemas de comunicaciones niveles definidos y coherentes de integridad de datos, confidencialidad y disponibilidad.

U-TIC es responsable de la definición de las directrices para la conexión segura a través de un módem desde o hacia equipos informáticos y otros dispositivos de UTE.
Es responsabilidad de cada UARI la implementación de los procedimientos que aseguren el cumplimiento de dichas directrices.
Con respecto a las redes inalámbricas cabe destacar las siguientes responsabilidades:

- La adquisición del equipamiento para las redes corporativas de área local es responsabilidad exclusiva de U-TIC.
- La instalación de cada equipo debe ser ejecutada únicamente por personal de U-TIC.
- Los requerimientos de equipamiento para las redes corporativas de área local deben ser solicitados a U-TIC.
- U-TIC tiene la responsabilidad de controlar y determinar con qué frecuencia transmitirán los equipos y cuál será la ubicación de esos dispositivos con el objetivo de mitigar riesgos y minimizar interferencias.
- U-TIC debe establecer los estándares, procedimientos y controles para que las implementaciones inalámbricas resulten suficientemente seguras y verificar que estas condiciones se mantengan.

7.9 DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información coordinado por la Gerencia Tecnologías de la Información y Comunicaciones está conformado por representantes de las Gerencias Generación, Trasmisión, 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:

- Elaborar las nuevas versiones de las políticas de Seguridad de la Información
- Velar por el cumplimiento de las Políticas de Seguridad de la Información de UTE.
- Difundir el Compromiso de Confidencialidad Corporativo a todas las áreas y la obligatoriedad de su utilización.

7.10 DE LAS UNIDADES INVOLUCRADAS EN PROCEDIMIENTOS DE CONTRATACION

Las unidades técnicas, al momento de requerir a la Gerencia de Abastecimientos, el inicio de un procedimiento de contratación, y según el objeto a contratar, incorporarán en los pliegos particulares, la exigencia, por parte del adjudicatario, de firmar el Compromiso de Confidencialidad Corporativo, el que será exigido por dicha unidad técnica previo al inicio de ejecución del contrato, y mantenido en custodia, de acuerdo a lo establecido en el numeral 7.3.

7.11 DE TERCERAS PARTES

Se entiende por terceras partes a todas las personas que brinden sus servicios a UTE o que reciben servicios de UTE, proveedores, socios de negocio y clientes de servicios de consultoría.

Las terceras partes deben estar en conocimiento y cumplir con la presente Política de Seguridad de Información.
Estas obligaciones deben estar debidamente especificadas en los acuerdos contractuales que tengan con UTE dependiendo de la naturaleza del servicio. Las unidades de UTE que oficien como contraparte deben facilitar el cumplimiento de las mismas.

ANEXO A

A continuación se detallan las unidades que administran recursos informáticos en UTE (UARIs), explicitando para cada una de ellas su ámbito de acción.

UARI	Unidad	Ámbito de Acción
U-TIC	Tecnologías de la Información y Comunicaciones	Red corporativa, Redes L0AN (excluye LANs de UARIs), Complejo de Procesamiento de Datos (CPDs). Red LAN de U-TIC, Red WAN de comunicaciones de UTE, Red operativa (excluye SCADAs locales), Sistemas de comunicaciones (TDM, Radio, Telefonía, Onda portadora)
U-DNC	División Despacho de Cargas	Red LAN DNC Red SCADA DNC
U-TRA	Transmisión	Redes SCADA TRA y redes de gestión asociadas y redes de control en las subestaciones. Relés de Protección de Transmisión y redes de gestión asociadas
U-GEN-HID	División Generación Hidráulica	SCADAs Centrales Hidráulicas
U-GEN-EOL	Generación Eólica	SCADAs Parques Eólicos
U-PEE	División Despacho de Cargas	Red LAN PEE
U-SEC	Secretaría General	Red LAN Directorio y Secretaría General
U-DIS-ACD	Automatización y Control de Distribución	Redes SCADA DIS y redes de gestión asociadas
U-GEN-TER	Dpto. Mantenimiento y estudios de control y automatismos - Centrales Térmicas	SCADAs Centrales Térmicas

A continuación se detallan algunas de las responsabilidades específicas de cada UARI que complementan o detallan lo definido en el capítulo 7 de las "Políticas de Seguridad de la Información".

UARI: U-TIC Tecnologías de la Información y Comunicaciones
RESPONSABILIDADES

- Administración de PCs, servidores, impresoras, notebooks y dispositivos móviles en la red Corporativa. (Cuando se justifique por razones de servicio, U-TIC puede otorgar permisos de administración local a determinados usuarios sobre PCs específicos).
- Compra, mantenimiento y actualización de Hardware y Software. (Excluyendo el hardware y software que venga integrado en las soluciones informáticas específicas de uso operativo).
- Gestión de soluciones tecnológicas (Software y Hardware) para cubrir necesidades de la Gestión.
  (No incluye la administración funcional, en los casos que esta actividad sea

realizada por la unidad "dueña" de la aplicación).
Compra y administración de switches, y access points (inalámbricos) para la red corporativa. (Incluye los equipos de tecnología SNA)

- Instalación y mantenimiento de cableado en redes LAN, racks, patcheras para la red corporativa y LAN internas.
- Administración y configuración de sitios y servicios WEB corporativos.
- Administración y configuración del correo electrónico corporativo.
- Administración y configuración de las bases de datos corporativas.
- Administración y configuración del dominio NTUTE y sus respectivos usuarios.
- Administración y configuración del hardware y software de seguridad (firewalls, antivirus, IDS, etc.) en la red corporativa, en forma coordinada con Seguridad de la Información. La actualización de firmas para anti-virus se coordina con el resto de los administradores de dominio.)
- Gestión de respaldos de la información.
- Proveer el servicio de acceso desde fuera de la Empresa a la red corporativa.
- Definición de ubicación y frecuencia de transmisión de los equipos inalámbricos.
- Compra y administración de equipos de comunicaciones (switches para la red operativa y routers)
- Contratación con proveedores de servicios de telecomunicaciones
- Compra y administración de equipamiento para establecer enlaces entre locales (incluye enlaces por fibra óptica, radio enlaces, etc.).
- Instalación y mantenimiento de cableado por cobre y fibra óptica para la red operativa.
- Instalación y mantenimiento de cableado de fibra óptica para la red corporativa.
- Administración de los Sistemas de comunicaciones. (TDM, Radio, Telefonía y Onda Portadora.)
- Administración y configuración de sitios y servicios WEB del sector.
- Administración y configuración de la base de datos del sector.
- Administración y configuración del dominio específico del sector (TELECOM) y sus respectivos usuarios, en relación de confianza con el dominio NTUTE.
- Administración de firewalls para protección de red operativa del acceso desde la red corporativa y desde el exterior de la empresa (acceso remoto), en forma coordinada con Seguridad de Información.
- Brindar servicios de voz sobre IP (La administración del software en las estaciones de trabajo y las definiciones y configuraciones de calidad de servicio en los equipos de comunicaciones de la red corporativa lo hace U-TIC)

UARI: U-DNC
RESPONSABILIDADES

- Administración de PCs, servidores, impresoras y notebooks en el Dominio de la red de su ámbito de acción.
- Administración de soluciones tecnológicas (Software y Hardware) para cubrir necesidades específicas.
- Compra de Hardware y Software específico de uso operativo para el negocio eléctrico (SCADAs, RTU, etc.).
- Compra y administración de switches y access points (inalámbricos) para

redes locales. Estas tareas pueden ser delegadas en U-TIC.
- Instalación y mantenimiento de cableado para las redes locales del sector.
- Administración y configuración de sitios y servicios WEB del sector.
- Administración y configuración de la base de datos del sector.
- Administración y configuración del dominio específico del sector y sus respectivos usuarios, en relación de confianza con el dominio NTUTE.
- Administración y configuración de hardware y software de seguridad (firewalls) en la red corporativa protegiendo servidor Web de DNC, en forma coordinada con Seguridad de Información.
- Administración de Hardware y software de seguridad (firewalls, antivirus, IDS, etc.) para protección de sus sistemas en su ámbito en forma coordinada con Seguridad de Información.
- Gestión de los respaldos de información de su respectivo ámbito de acción.

UARI: U-TRA (Transmisión)

RESPONSABILIDADES

- Administración de PCs, servidores, impresoras y notebooks en el Dominio de la red de su ámbito de acción.
- Gestión de soluciones tecnológicas de Hardware y Software (diseño, desarrollo y mantenimiento) para cubrir necesidades específicas.
- Compra de Hardware y Software específico de uso operativo para el negocio eléctrico (SCADAs, RTU, etc.).
- Compra y administración de switches y access points (inalámbricos) para redes locales. Estas tareas pueden ser delegadas en U-TIC.
- Instalación y mantenimiento de cableado para las subredes locales operativas.
- Administración y configuración de sitios y servicios WEB del sector.
- Administración y configuración de la base de datos del sector.
- Administración y configuración de los dominios específicos y sus respectivos usuarios.
- Administración de Hardware y software de seguridad (firewalls, antivirus, IDS, etc.) para protección de sus sistemas en su ámbito en forma coordinada con Seguridad de Información.
- Gestión de los respaldos de información de su respectivo ámbito de acción.
- Administración de PCs, servidores, impresoras y notebooks en el Dominio de la red de su ámbito de acción.

UARI: U-GEN-HID (U-GEN-HID: División Generación Hidráulica)

RESPONSABILIDADES

- Administración de PCs, servidores, impresoras y notebooks en el Dominio de la red de su ámbito de acción.
- Gestión de soluciones tecnológicas de Hardware y Software (diseño, desarrollo y mantenimiento) para cubrir necesidades específicas.
- Compra de Hardware y Software específico de uso operativo para el negocio eléctrico (SCADAs, RTU, etc.).
- Compra y administración de switches y access points (inalámbricos) para

redes locales. Estas tareas pueden ser delegadas en U-TIC.
- Instalación y mantenimiento de cableado para la red operativa.
- Administración y configuración de Base de datos del sector.
- Administración y configuración del dominio específico del sector y sus respectivos usuarios, en relación de confianza con el dominio NTUTE.)
- Administración de Hardware y software de seguridad (firewalls, antivirus, IDS, etc.) para protección de sus sistemas en su ámbito en forma coordinada con Seguridad de Información.
- Gestión de los respaldos de información de su respectivo ámbito de acción.

UARI: U-GEN-EOL (U-GEN-EOL: Generación Eólica (GEN)

RESPONSABILIDADES

- Administración de PCs, servidores, impresoras y notebooks en el Dominio de la red de su ámbito de acción.
- Gestión de soluciones tecnológicas de Hardware y Software (diseño, desarrollo y mantenimiento) para cubrir necesidades específicas.
- Compra de Hardware y Software específico de uso operativo para el negocio eléctrico (SCADAs, RTU, etc.).
- Compra y administración de switches y access points (inalámbricos) para redes locales. Estas tareas pueden ser delegadas en U-TIC.
- Instalación y mantenimiento de cableado para la red operativa.
- Administración y configuración de Base de datos del sector.
- Administración y configuración del dominio específico del sector y sus respectivos usuarios, en relación de confianza con el dominio NTUTE.)
- Administración de Hardware y software de seguridad (firewalls, antivirus, IDS, etc.) para protección de sus sistemas en su ámbito en forma coordinada con Seguridad de Información..
- Gestión de los respaldos de información de su respectivo ámbito de acción.

UARI: U-PEE

RESPONSABILIDADES

- Administración de PCs, servidores, impresoras y notebooks en el Dominio de la red de su ámbito de acción.
- Gestión de soluciones tecnológicas de Hardware y Software (diseño, desarrollo y mantenimiento) para cubrir necesidades específicas.
- Compra de Hardware y Software específico de uso operativo para el negocio eléctrico.
- Compra y administración de switches y access points (inalámbricos) para redes locales.
- Administración y configuración de sitios y servicios WEB del sector.
- Administración y configuración de la base de datos del sector.
- Administración y configuración del dominio específico del sector y sus respectivos usuarios, en relación de confianza con el dominio NTUTE.)
- Administración de hardware y software de seguridad (firewalls, antivirus, IDS, etc.) para protección de sus sistemas en su ámbito en forma coordinada con la unidad Seguridad de Información.
- Gestión de los respaldos de información de su respectivo ámbito de acción.
- Estas tareas pueden ser delegadas en U-TIC, según el criterio de la UARI,

estableciéndose acuerdos de servicio cuando corresponda.

UARI: U-SEC Secretaría General

RESPONSABILIDADES

- Administración de PCs, servidores, impresoras y notebooks en el Dominio de la red de su ámbito de acción.
- Gestión de soluciones tecnológicas de Hardware y Software (diseño, desarrollo y mantenimiento) para cubrir necesidades específicas.
- Compra y administración de switches y access points (inalámbricos) para redes locales. Estas tareas pueden ser delegadas en U-TIC.
- Administración y configuración de sitios y servicios WEB del sector.
- Administración y configuración de las bases de datos del sector.
- Administración y configuración del dominio específico del sector (NTDIR y SEC) y sus respectivos usuarios.
- Administración y configuración de hardware y software de seguridad (firewalls, antivirus, IDS, etc.) en la red corporativa protegiendo dominio de SEC, en forma coordinada con Seguridad de Información.
- Gestión de los respaldos de información de su respectivo ámbito de acción.

UARI: U-DIS-ACD Automatización y Control de Distribución

RESPONSABILIDADES

- Administración de PCs, servidores, impresoras y notebooks en el Dominio de la red de su ámbito de acción.
- Gestión de soluciones tecnológicas de Hardware y Software (diseño, desarrollo y mantenimiento) para cubrir necesidades específicas.
- Compra de Hardware y Software específico de uso operativo para el negocio eléctrico (SCADAs, RTU, etc.).
- Compra y administración de switches y access points (inalámbricos) para redes locales. Estas tareas pueden ser delegadas en U-TIC.
- Administración y configuración de sitios y servicios WEB del sector.
- Administración y configuración de las bases de datos del sector.
- Administración y configuración de los dominios específicos y sus respectivos usuarios, en relación de confianza con el dominio NTUTE.
- Administración de Hardware y software de seguridad (firewalls, antivirus, IDS, etc.) para protección de sus sistemas en su ámbito en forma coordinada con Seguridad de Información.
- Instalación y mantenimiento de cableado para las subredes locales operativas.

UARI: U-GEN-TER (Mantenimiento y estudios de control y automatismos - Centrales Térmicas)

RESPONSABILIDADES

- Gestión de soluciones tecnológicas de Hardware y Software (diseño, desarrollo y mantenimiento) para cubrir necesidades específicas.
- Compra de Hardware y Software específico de uso operativo para el negocio eléctrico (SCADAs, RTU, etc.).

ÍNDICE