1. OBJETIVO

Dar a conocer las políticas y lineamientos de Seguridad de la Información necesarios para implementar los controles establecidos en el Anexo A de la NTP ISO/IEC 27001, los cuales permiten alcanzar los objetivos definidos para la seguridad de la información en las empresas del Grupo Distriluz.

2. ALCANCE

Aplica a todos las áreas, personal y terceros relevantes (según corresponda) que formen parte o brinden servicios a las empresas que conforman el GRUPO DISTRILUZ.

3. BASE LEGAL Y NORMATIVA

a. Resolución N° 129-2014/CNB-INDECOPI aprueba la Norma Técnica Peruana “NTP-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición”.
b. ISO/IEC 27000:2018 "Tecnología de la información. Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Visión general y vocabulario".
c. ISO/IEC 27001:2013 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición.
d. NTP-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición.
e. ISO/IEC 27002:2013 “Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información”.
f. NTP ISO/IEC 27002:2017 “Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información”.

4. TÉRMINOS, DEFINICIONES Y ABREVIATURAS

a. **Administrador de bases de datos:** Personal que administra las tecnologías de la información y la comunicación, siendo responsable de los aspectos técnicos, tecnológicos, científicos, inteligencia de negocios y las legalidades de las bases de datos, y de su calidad de datos.

b. **Administrador *root*:** Usuario con permiso de altos privilegios sobre un sistema, base de datos o software.

c. **Confidencialidad:** Propiedad de que la información no esté disponible o sea revelada a personas, organizaciones o procesos no autorizados.

d. **Control:** Medida que modifica un riesgo.
Nota 1: Los controles incluyen cualquier proceso, la política, dispositivo, práctica, u otras acciones que modifiquen un riesgo.
Nota 2: Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.

e. **Control de acceso:** Los medios para asegurar que el acceso a los activos está autorizado y restringido basado en los negocios y la seguridad requisitos.

f. **Cuenta genérica:** Cuenta destinada a representar un servicio, colectivo o evento que permite el acceso a distintos servicios.

g. **Dispositivos móviles:** Se considerarán los dispositivos móviles como: laptops, *tablets* y celulares.

h. **Incidente de seguridad de la información:** Única o una serie de eventos de seguridad de la información no deseados o inesperados que tiene una probabilidad significativa de comprometer operaciones de negocio y amenazar la seguridad de la información.

i. **Integridad:** Propiedad salvaguardar la exactitud e integridad de los activos.

j. **Política:** Intenciones y dirección de una organización formalmente expresadas por la alta dirección.

k. **Sistema de gestión:** Conjunto de elementos interrelacionados o que interactúan en una organización para establecer políticas, objetivos y procesos, para lograr esos objetivos.
Nota 1: Un sistema de gestión puede abordar una sola disciplina o varias disciplinas.
Nota 2: Los elementos del sistema incluyen la estructura de la organización, funciones y responsabilidades, la planificación, operación, etc.
Nota 3: El alcance de un sistema de gestión puede incluir la totalidad de la organización, específico y funciones identificadas en la organización, las secciones específicas e identificadas de la organización, o uno o más funciones a través de un grupo de organizaciones.

l. **Sistema de Gestión de Seguridad de la Información:** Parte del sistema de gestión global, basada en un enfoque hacia los riesgos del negocio, cuyo fin es establecer, implementar, mantener y mejorar la seguridad de la información.

m. **Sistema de información:** Aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo de la información.

n. **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
Nota 1: Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.

o. **Usuario privilegiado:** Es aquel que tiene autorización administrativa completa sobre un sistema, software, base de datos o activo de información.

p. **OSCD:** Oficial de Seguridad de la Información y Confianza Digital

q. **SGSI:** Sistema de Gestión de Seguridad de la Información.

5. POLITICA DE TELETRABAJO

a. Todas las políticas presentes son aplicables en teletrabajo, trabajo remoto o futuras condiciones equivalentes.

b. El colaborador debe cumplir con la presente política, así como la normativa vigente aprobada por el área TIC relacionada a mantener la seguridad de la información.

c. El colaborador debe guardar confidencialidad de la información proporcionada por las Empresas del GRUPO DISTRILUZ para la prestación de servicios.

d. El colaborador que se encuentre laborando bajo la modalidad de teletrabajo debe contar con un acceso que le permita acceder a los recursos y servicio internos del Grupo Distriluz. Es responsabilidad del área de Gestión de personas o quien haga las veces evaluar y autorizar a través de correo electrónico la configuración de los accesos correspondientes a la Jefatura TIC Regional.

e. La Jefatura inmediata que autoriza la solicitud de acceso remoto es responsable de evaluar la adecuada correspondencia con aquellos roles que realmente requieren el acceso por cumplimiento de sus funciones. El área TIC conforme a lo indicado en la solicitud de acceso establecerá el mecanismo de control para preservar la seguridad de la información del Grupo Distriluz a la que accederá el colaborador.

f. El colaborador que cuente con acceso remoto, debe proteger la información a la que tiene acceso de amenazas como el acceso no autorizado, alteración indebida o software malicioso.

g. La Jefatura TIC de cada empresa del Grupo Distriluz proveerá mecanismos tecnológicos seguros para brindar el servicio de acceso remoto garantizando la seguridad de la información.

h. Todos los equipos en los que se trabaje y accedan a la red de Distriluz (incluye Laptops, servidores y pcs de escritorio), deben tener instalado como mínimo una de las 2 últimas versiones del sistema operativo Windows que existan en el mercado, estos deben estar con las actualizaciones de los parches vigentes y deben tener instalado un antivirus actualizado.

6. POLITICA DE DISPOSITIVOS MÓVILES

a. Las características en las capacidades de los equipos deberán ser definidos en función de la importancia de la información procesada o almacenada en cada tipo de usuario que utiliza un dispositivo móvil de la empresa.

b. El área de Seguridad y Control Patrimonial debe asegurar el control de dispositivos de cómputos móviles propios de Distriluz o de terceros, tanto al ingreso como salida de las instalaciones de las empresas del Grupo Distriluz, a través de un formato mecanizado o manual, inventario, correo electrónico, etc.

c. Todos los dispositivos móviles (laptops, tablets, teléfonos móviles) deben tener configuraciones de control de seguridad mínima como:

- Mecanismo de autenticación o inicio de sesión.
- Bloqueo de inactividad.
- Instalar y mantener actualizado el software antivirus y/o antimalware.
- Encriptación de la información (de ser necesario).

d. Todos los usuarios de dispositivos móviles de cómputo que contengan información confidencial o de uso interno deben usar la versión más actualizada del software. Los parches o actualizaciones serán obtenidos de manera formal, provenientes del fabricante.

e. El usuario tiene prohibido la copia, almacenamiento o envío de la información a cualquier otro dispositivo o servicio que no esté autorizado por el Grupo Distriluz.

f. En el caso de pérdida o robo de un dispositivo móvil, se deberá reportar al área TIC y al área de Control Patrimonial para la desactivación de las cuentas correspondientes.

g. El usuario debe devolver el dispositivo móvil asignado en estado operativo, al término de sus funciones o al cambio de puesto o cuando el servicio contratado culminé.

7. POLÍTICA PARA EL USO ACEPTABLE DE LOS ACTIVOS

a. El uso de la información y de los activos de información debe ser para propósitos de las actividades de la empresa de acuerdo con las políticas, procedimientos o cualquier lineamiento que definan.

b. No se debe compartir información que haya sido clasificada como confidencial o restringida, salvo autorización del propietario de información, el cual recibirá los sustentos necesarios para que pueda ser compartida.

c. Se deben cumplir con lo establecido en los requisitos legales, contractuales y normativos relativos al uso de activos de información.

d. El personal que ponga en riesgo los activos de información, se le aplicará medidas disciplinarias de acuerdo con el proceso disciplinario vigente establecido en el Reglamento Interno de Trabajo.

e. Todos los activos a los que tenga acceso un personal se encuentran bajo su responsabilidad y deben de proteger su integridad y confidencialidad.

f. Todo activo digital que contiene información confidencial y/o restringida no debe ser desatendido, se deben utilizar bloqueos para asegurar su integridad y confidencialidad de la información.

g. Todo activo físico que contiene información confidencial y/o restringida no debe ser desatendido, debe quedar resguardado con controles adecuados para asegurar su integridad y confidencialidad de la información.

h. Todo incidente de seguridad de la información que involucre a información confidencial reservada o a los activos que soportan dicha información deben ser reportados por los canales establecidos.

i. Todos los activos e información a los cuales el colaborador posea deben ser devueltos al cese de este.

j. La información solo debe ser transmitida a través de medios formales, evitando uso de medios no autorizados como correo personal o canales de mensajería.

8. POLÍTICA PARA LA GESTIÓN DE MEDIOS REMOVIBLES

Se ha establecido la siguiente política específica para el uso de medios removibles que contienen información clasificada como “confidencial”:

a. Los usuarios que usen medios removibles como memorias USB, discos externos, DVDs y CDs deben evitar utilizarlos en equipos internos o externos que no cuenten con las medidas de seguridad mínimas requeridas como un antivirus y software licenciado. Además, son responsables del aseguramiento físico de estos, en tal sentido, cuando no se estén usando deben quedar resguardados en un cajón con llave u otro espacio seguro.

b. Los medios removibles no deben quedarse conectados en equipos desatendidos por largos períodos de tiempo.

c. El uso de los medios removibles, deben ser autorizados por las Gerentes de línea y/o Jefaturas inmediatas.

9. POLÍTICA DE CONTROL DE ACCESOS

Los siguientes lineamientos están siendo implementados progresivamente en los diversos sistemas y servicios TIC:

a. La seguridad de este tipo de autentificación se basa en dos premisas:
- La contraseña debe ser personal e intransferible.
- La contraseña es lo suficientemente 'fuerte" para no ser descifrada.

b. La contraseña para ser considerada 'fuerte" (segura) debe poseer las siguientes características:
1) Debe tener al menos ocho (08) caracteres.
2) Utiliza caracteres los cuatro grupos siguientes:
    a. Letras minúsculas.
    b. Letras mayúsculas.
    c. Números (por ejemplo, 1, 2, 3).
    d. Símbolos (por ejemplo, $, @, !, %)
3) No ser, ni derivar palabras del diccionario, de la jerga o de un dialecto.
4) No derivarse del nombre del usuario o de algún pariente cercano.
5) No derivarse de información personal (de teléfono, de DNI, fecha de nacimiento, dirección, etc.).
6) No utilizar palabras en idiomas extranjeros.
7) No invertir palabras reconocibles.
8) No utilizar números ni teclas secuenciales.

c. Para iniciar sesión se le brinda al usuario una clave temporal, la cual es forzada a cambiarse en el primer inicio de sesión y/o cuando se solicita reseteo de la clave.

d. Está prohibido intentar ingresar a la infraestructura tecnológica con la cuenta de usuario de otro empleado.

e. El nivel de acceso a un sistema de información se otorgará de acuerdo con:

- La clasificación de la Información.
- Funciones del usuario.
- Perfiles de acceso estandarizados.
- Pedido, autorización y administración de acceso.
- Revisión periódica.
- Retiro y modificación de derechos de acceso.

f. Los permisos de acceso serán gestionados incorporando el principio de menor privilegio y separación de funciones.

g. El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información debe ser asignado de acuerdo con la identificación previa de requerimientos de la empresa y de seguridad de la información.

h. Los accesos con altos privilegios (usuarios administradores) deben ser controlados igualmente mediante un proceso formal.

i. Periódicamente se debe revisar que los accesos de las cuentas de usuario de personal cesado o rotado de puesto hayan sido eliminados y/o deshabilitados.

j. Periódicamente se debe revisar que los accesos concedidos a los usuarios sean los que les corresponde de acuerdo con las funciones que desempeñan.

k. El acceso a repositorios con código fuente debe ser controlado.

l. La integridad La integridad de las redes debe ser protegida, integrando la segmentación de las redes donde sea apropiado.

m. En caso de que el empleado trabaje con sus equipos personales, estos deben ser revisados por el área TIC para recomendar la mejor configuración, teniendo en cuenta las normas de ciberseguridad y seguridad informática, a fin de garantizar una adecuada cohesión con la red empresarial; estos equipos no deben usarse en la red empresarial mientras el usuario no cumpla con las indicaciones del área TIC.

n. Los accesos remotos deben ser gestionados y monitoreados frecuentemente, así como la vigencia de los permisos otorgados.

o. Todos y cada uno de los equipos de cómputo deben ser asignados a un responsable (puesto de trabajo), por lo que es de su competencia hacer buen uso de estos. Además, la Jefatura es responsable de la devolución de los equipos de sus colaboradores de área.

p. Las cuentas de usuario para trabajar en los diferentes sistemas o servicios TIC deben ser personales e intransferibles.

q. Los usuarios que hagan uso de un segundo factor de autenticación (biométrico, token, mensaje de texto, etc.) para el ingreso a las aplicaciones deberán prestarles un cuidado similar a las contraseñas y no compartirlos.

r. La caducidad de las contraseñas de los usuarios no debe superar los 3 meses, siendo lo ideal contraseñas de un solo uso (OTP).

s. En el caso de aplicaciones críticas, el administrador de accesos, el servidor y base de datos se deben guardar copia de las contraseñas de usuarios privilegiados en un sobre cerrado. Se tiene que cumplir con las siguientes consideraciones con respecto a la gestión de usuarios privilegiados:

1) La mejor practica es no permitir cuentas de desarrollador en ambientes de producción. Puede concederse acceso condicional en situaciones de emergencia, debiendo implementarse controles adicionales para asegurar que los cambios probados adecuadamente.
2) No todo usuario privilegiado debe poder crear copias de seguridad, ya que esto le da acceso a propiedad intelectual. Los usuarios aprobados deben ser identificados por escrito con los procedimientos adecuados.
3) Los administradores de bases de datos no deben tener la misma autoridad que un administrador root. Puede considerarse cifrar el contenido de algunos campos sensibles en la base de datos, o el uso de herramientas de control de acceso y auditoría.

t. Las cuentas genéricas deben contar con un periodo de vigencia para las aplicaciones gestionadas a través del Directorio activo. Para el caso de los sistemas que no son gestionados por el directorio activo, pero si tienen un sistema de alertas deben contar con un periodo de vigencia. Para el caso de sistemas que no tienen un sistema de alertas, se deberá programar manualmente.

u. El sistema de registro de eventos(logs) debe ser administrado por usuarios privilegiados.

v. Los usuarios no deben tener acceso al nivel administrador de su PC. Excepcionalmente de forma temporal y previa autorización se les podrá brindar este tipo de acceso.

10. POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS Y GESTIÓN DE CLAVES

a. Se debe desarrollar e implementar mecanismos adecuados para el uso de controles criptográficos para la protección de información con el objetivo de salvaguardar la confidencialidad, integridad/autenticidad, no repudio contra pérdida accidental, destrucción o daño de la información.

b. Estos mecanismos deben ser como mínimo los siguientes:

- Solo se utilizan controles criptográficos para la protección de la información de acuerdo con estándares internacionales.
- Para verificar la autenticidad o integridad de la información almacenada o transmitida sea confidencial o sensible, se utilizará como mecanismo criptográfico el uso de firmas digitales basadas en certificados digitales.

- En el caso de aplicación de la firma digital se implementará de acuerdo a la Ley Nº 27269 – Ley de Firmas y Certificados Digitales Perú.
- El Grupo Distriluz puede utilizar la firma digital para resolver disputas asociadas al no repudio.
- Se debe utilizar protocolo WP3 como mínimo para las conexiones inalámbricas.
- Se deben utilizar protocolo https para las páginas internas y externas de la organización.
- Cuando se utilicen medios extraíbles, estos deben estar cifrados. La clave de descifrado debe pasarse al destinatario por separado; asignar a un responsable para generar y distribuir las claves y para almacenar las claves.

c. Para la gestión de claves criptográficas la Jefatura Regional TIC debe precisar el método o herramienta a utilizar para la generación, almacenamiento y archivo de las claves criptográficas.

d. La Jefatura Regional TIC será responsable de la generación, transferencia y archivo de claves criptográficas. Cada clave criptográfica deberá tener un periodo de expiración. Se definirán fechas de activación y desactivación de claves.

e. El Grupo Distriluz debe abastecer los recursos necesarios para garantizar la protección y seguridad del equipo utilizado para generar, almacenar y archivar las claves criptográficas tomando en consideración los respaldos y accesos correspondientes.

11. POLÍTICA DE EQUIPOS DE USUARIO DESATENDIDOS

a. Al dejar un equipo desatendido temporalmente, el usuario debe bloquear el acceso a su computador, laptop o servidores, independientemente del tiempo que permanezcan alejados.

b. Los equipos de cómputo deben ser protegidos mediante uso de contraseñas u otros controles cuando no estén siendo utilizados.

c. Al terminar la jornada de trabajo se deberá apagar el equipo, siempre y cuando no se encuentren ejecutándose procesos programados fuera de horario de oficina y respondan a labores propias del cargo del trabajador. En caso de ausentarse de la oficina por un período prolongado de tiempo, se deberán cancelar las sesiones de usuario dentro de las aplicaciones y proceder a apagarlo.

d. Toda computadora que va a ser desatendida deberá estar programada para activarse con un protector de pantalla que se active a los 5 minutos de haber sido desatendida.

e. Cuando un sistema de información sea desatendido, en la medida de lo posible, éste será bloqueado automáticamente en un tiempo determinado como máximo 15 minutos.

f. Se debe establecer un método de bloqueo (contraseñas, patrones, etc.) para los equipos que serán entregados a los usuarios, y que se bloquee pasado un tiempo no mayor a cinco minutos de inactividad

12. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

a. Es responsabilidad de todo usuario mantener sus escritorios o puestos de trabajo limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio para evitar el acceso no autorizado o fuga de información.

b. Se debe evitar exponer información confidencial e interna en los módulos, escritorios o estaciones de trabajo de la empresa.

c. El usuario no deberá tener escrito en un medio físico (papel adhesivo, papel convencional, superficies, etc.) su cuenta de red, credenciales de acceso de correo electrónico, aplicación, sistema de información, datos personales o información relevante que comprometa la seguridad de la información.

d. Cuando no se esté usando documentación y medios informáticos (Dispositivos USB, Discos Duros Portables, CD/DVDs, etc) deben asegurarse de:
   - Almacenarlos en lugares adecuados como locales cerrados y/o en los tipos de mobiliario de seguridad adecuados especialmente fuera de las horas de trabajo.
   - Evitar que usuarios no autorizados accedan a dichos medios.

e. Al ausentarse del puesto de trabajo se deberá guardar en un lugar seguro la documentación que contenga información confidencial o sensible.

f. Los documentos enviados a impresión, se deberán recoger inmediatamente, toda vez que esta sea considerada como confidencial o sensible.

g. Si luego de la utilización los documentos con información confidencial o restringida, dejan de ser necesarios deben destruirlos antes de desecharlos, si los datos o la información contenida es sensible la misma debe protegerse y el documento triturarse para evitar su recuperación.

h. Se deberá mantener el escritorio del sistema operativo libre de archivos o iconos que saturen la pantalla y confieran una práctica de almacenamiento riesgosa.

i. Los archivos que contengan información confidencial o sensible deben ser guardados en un repositorio de red que cuente con seguridad de acceso y respaldo.

13. INCUMPLIMIENTO DE LAS POLITÍCAS

El incumplimiento de estas políticas de seguridad de la información traerá consigo las consecuencias legales que apliquen a la normativa y proceso disciplinario de las Empresa del GRUPO DISTRILUZ.