POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - EXTERNA

NDD TECH LTDA

PAUTAS

Estos son los principios básicos que rigen la Política de Seguridad de NDD Tech, establecidos de acuerdo con las necesidades de la empresa:

1. A NDD tiene la responsabilidad de custodiar la información de sus clientes directos e indirectos, proveedores y empleados. Por lo tanto, la creación de un ambiente que garantice la disponibilidad y protección es esencial para la continuidad del negocio de la Compañía.

2. Toda la información debe ser clasificada formalmente en cuanto a su confidencialidad, integridad y disponibilidad, independientemente de su forma de almacenamiento, digital o no.

3. Los Datos Personales e información relacionada con personas naturales identificadas o identificables deben ser protegidos obligatoriamente de acuerdo con la Ley General de Protección de Datos (LGPD) y tratados como confidenciales cuando no exista una justificación legítima en contrario.

4. Se deben tomar precauciones adicionales con respecto a los Datos Personales Sensibles, aquellos que pueden revelar origen racial, étnico, opinión política, convicción religiosa, filosófica, afiliación sindical, datos genéticos o biométricos, relacionados con la salud u orientación sexual.

5. La información debe tener un ciclo de vida programado. La información considerada confidencial, cuando ya no sea necesaria, debe ser destruida mediante mecanismos apropiados. La eliminación o reutilización de medios que contengan esta información debe realizarse de manera que dificulte su recuperación.

6. Cualquier individuo que tenga acceso a las dependencias de NDD debe ser identificado. El acceso de terceros a áreas donde exista procesamiento físico o digital de información debe estar justificado por la estricta necesidad y siempre debe realizarse bajo la supervisión de un empleado de NDD responsable de la información en ese sector.

7. Todos los equipos en la Compañía deben estar inventariados e identificados de manera individual.

8. Las credenciales de acceso, o tarjetas de acceso a instalaciones y/o sistemas, son personales, no compartibles e intransferibles. El usuario es responsable de todas las actividades realizadas mediante autenticación con sus credenciales, por lo tanto, debe velar por su protección y confidencialidad, y realizar las acciones de mantenimiento adecuadas para cada tipo de credencial, como el cambio periódico de contraseñas.

9. Los empleados de NDD, durante la vigencia y después de la terminación del contrato de trabajo o prestación de servicios, no pueden apropiarse de información o medios, equipos, componentes o

accesorios que la contengan, como por ejemplo: correos electrónicos corporativos, hojas de cálculo, archivos de datos o videos.

10. La responsabilidad de mantener la seguridad es compartida por todos los empleados. NDD deberá impartir capacitaciones para promover la conciencia y preparación. Las violaciones de las normas mencionadas a continuación, incidentes o fallos de seguridad deben ser notificados inmediatamente al equipo de Seguridad de la Información de NDD.

11. Si existe la mera posibilidad de filtración de Datos Personales, también se debe notificar inmediatamente al Encargado de Protección de Datos (DPO).

Seguridad Física

1. Todo Todo individuo que ingrese a las instalaciones de NDD debe usar una tarjeta de identificación.

2. Las personas externas a la Compañía deben ser identificadas en la recepción y su ingreso a las instalaciones de NDD se realizará mediante autorización y acompañamiento del empleado de la Compañía.

3. Cualquier computadora o portátil que salga de NDD necesitará autorización previa del gerente responsable.

4. Los proveedores de servicios de NDD son responsables de las acciones o daños causados por sus empleados al patrimonio de NDD, así como deben garantizar la confidencialidad de la información a la que acceden.

5. Los documentos o papeles que contengan información confidencial, cuando ya no sean necesarios, deben ser triturados o destruidos de manera que impida su lectura.

6. Los medios de solo lectura (discos CD-ROM, CD-R, DVD, etc.) que contengan información confidencial, cuando ya no sean necesarios, deben ser rotos o destruidos para evitar su uso indebido.

7. Los medios regrabables (discos duros o SSD, pendrives, tarjetas SD, cintas, discos CD o DVD del tipo RW, u similares) que contengan información confidencial, cuando ya no sean necesarios, deben ser borrados con el procedimiento seguro adecuado indicado por el equipo de Seguridad de la Información antes de su reutilización o eliminación.

8. Los equipos y sus componentes internos serán inventariados periódicamente y solo los empleados autorizados pueden realizar cambios en los equipos y piezas.

Credenciales de Acceso

1. Las credenciales, identificaciones y contraseñas de acceso deben ser individuales y mantenerse en secreto, no deben ser transferidas o compartidas.

2. Cada empleado cambiará su contraseña de forma sistemática y automática, con una validez máxima de 42 (cuarenta y dos) días, y es su responsabilidad elegir contraseñas robustas, complejas y largas.

3. Las contraseñas deben ser diferentes entre los sistemas utilizados, deben contener números, letras mayúsculas, minúsculas y caracteres especiales.

4. NDD adopta el concepto de privilegio mínimo, en el que los colaboradores solo deben tener acceso a la información estrictamente necesaria para cumplir con sus funciones.

5. Los procesos de concesión y revocación de acceso son responsabilidad de los equipos de SRE (Site Reliability Engineering) e Infraestructura de TI y deben ser centralizados en esos equipos y ejecutados según los flujos documentados.

Uso de la Red

1. O El acceso a Internet se proporciona para actividades y fines de la Compañía. Los accesos con fines particulares lícitos pueden realizarse ocasionalmente, preferiblemente fuera del horario laboral, siempre que no violen otras normas.

2. Está prohibido usar la red para acceder o enviar contenido pornográfico, ofensivo o difamatorio, así como para acosar a terceros, ya sean empleados o no.

3. El uso con fines particulares de redes sociales como Facebook o Twitter y sitios de videos como YouTube, Vimeo y Netflix durante el horario laboral se considera inapropiado y puede estar bloqueado en cualquier momento a criterio de la Compañía.

4. Cualquier sitio conocido por su contenido prohibido o inapropiado puede estar en listas de bloqueo automático. Cualquier error en la clasificación de un sitio específico puede ser comunicado al equipo responsable de los proxies para su corrección.

5. El acceso a Internet puede y será monitoreado y registrado por la Compañía. Los registros estarán disponibles para la Compañía durante el tiempo que esta considere apropiado.

6. No se permite instalar, usar o configurar equipos (hardware o software) que proporcionen acceso a la red corporativa sin autorización formal y conocimiento del Equipo de Seguridad de la Información. Especialmente, no se permite la instalación de puntos de acceso wifi, bluetooth, módems, hubs, switches, vpn, routers o software de acceso remoto para fines personales.

7. El correo electrónico corporativo es administrado por NDD y debe tener activa permanentemente la protección contra el spam.

8. Todos los mensajes enviados por correo electrónico desde la dirección profesional son propiedad de la Compañía, por lo tanto, deben usarse para asuntos de interés de NDD y no debe esperarse privacidad de su contenido.

9. Está prohibido enviar o participar en cadenas, incluso de solidaridad, premios o información utilizando el correo electrónico corporativo proporcionado por NDD.

10. Está prohibido enviar mensajes con contenido electoral, difamatorio, ofensivo, discriminatorio, obsceno, pornográfico o que pueda interpretarse como discriminación racial, sexual, religiosa o política.

11. No se permite distribuir, a través de correo electrónico, grupos de discusión, foros y formas similares de comunicación, mensajes no solicitados del tipo "cadena" y mensajes en masa, comerciales, de propaganda política o correo electrónico no solicitado.

12. Las computadoras portátiles, laptops, tablets y otros equipos personales o de terceros no deben conectarse directamente a la red de la Compañía sin autorización. Dichos equipos, cuando estén autorizados, pueden conectarse a la red wifi y tener acceso a servicios internos a través de VPN gestionada por la Compañía.

Protección de Estaciones y Servidores

1. Todos los computadores y servidores de NDD deben tener instalado un antivirus.

2. El usuario no debe impedir el funcionamiento y actualización del antivirus sin autorización y conocimiento del equipo de administración del antivirus.

3. Si se detecta algún problema con el antivirus, el usuario deberá comunicarlo inmediatamente al equipo de Infraestructura, que tomará las medidas necesarias.

4. Todos los computadores y servidores de NDD deben tener instalados agentes de monitoreo, los cuales no deben ser desinstalados sin autorización del equipo de Infraestructura y Seguridad de la Información.

Uso de Programas

1. Las estaciones de trabajo se proporcionan con los programas mínimos necesarios, incluido el sistema operativo y las aplicaciones, para cumplir con su función básica en NDD.

2. Se consideran legítimos los software instalados y utilizados de acuerdo con sus licencias de uso y que no contravengan las normas de NDD ni la legislación.

3. No está permitida la instalación de ningún software, gratuito o no, en los equipos de NDD sin la autorización del equipo de Infraestructura y Seguridad de la Información. Si necesita algún software específico, contáctese a través de un ticket abierto en el portal de Helpdesk (haciendo clic aquí).

4. El uso o la instalación de software sin licencia de uso o en nombre de terceros sin autorización constituye un delito de piratería, y tanto el usuario como el instalador están sujetos a sanciones administrativas, legales y penales según lo establecido por la ley.

5. Se realizarán ocasionalmente verificaciones en el inventario de equipos, tanto en hardware como en software, para identificar desviaciones de las normas.

Copias de Seguridad o Backup

1. Cada Cada usuario es responsable de realizar copias de seguridad de sus archivos laborales en Sharepoint y en los sistemas de archivos proporcionados por NDD.

2. Los archivos generados en las estaciones de trabajo deben guardarse en Sharepoint, ya que solo allí se realiza la copia de seguridad, y en caso de eliminación accidental pueden recuperarse rápidamente. Si un archivo o carpeta se guarda únicamente en la computadora y se elimina accidentalmente, no se puede recuperar.

3. No está permitida la copia de datos confidenciales para su procesamiento o almacenamiento en servicios externos de terceros no autorizados por NDD o sus clientes.

4. Siempre que sea posible, los datos confidenciales deben estar cifrados en las copias de seguridad.

5. Cada copia de seguridad debe someterse periódicamente a pruebas de restauración.

6. Los medios de almacenamiento deben guardarse en un lugar seguro, como un armario, la nube, una caja fuerte o una habitación con llave o control de acceso, y deben respetarse los tiempos de vida útil sugeridos por el fabricante.

7. Algunas copias de seguridad tienen un tiempo de vida útil determinado por ley, por lo que el equipo responsable de las copias de seguridad debe ser informado y velar por mantenerlas disponibles durante ese tiempo, así como los equipos necesarios para su recuperación cuando sea necesario.

Sistemas y Aplicaciones

1. Não No está permitida la transferencia de datos para su procesamiento o almacenamiento en servicios externos de terceros no autorizados expresamente por NDD o sus clientes.

2. El almacenamiento y la transferencia de datos confidenciales siempre deben estar cifrados con mecanismos aprobados por la Compañía.

3. NDD preferirá soluciones/aplicaciones que utilicen protocolos seguros tanto en la transferencia como en el almacenamiento de información. Las aplicaciones que no utilicen estos recursos deben ser validadas por el equipo de seguridad de la información antes de su uso.

4. NDD preferirá la utilización de sistemas de autenticación de doble o múltiple factor (MFA/2FA). Las aplicaciones que no utilicen estos recursos deben ser validadas por el equipo de seguridad de la información antes de su uso.

5. Los sistemas deben generar registros (logs) de eventos de seguridad. Para este fin, se deben utilizar funciones del Sistema de Seguridad en uso, recursos del sistema operativo, recursos de base de datos y/o recursos de la aplicación. Los registros deben contener al menos la siguiente información:

- Identificación de la aplicación y función;
- Momento del evento (marca de tiempo);
- Información que identifique la máquina o ubicación del evento;
- Datos relevantes manipulados por la aplicación.

El Sistema de Seguridad puede encargarse del registro de algunas de estas informaciones.

6. En el desarrollo y mantenimiento de sistemas es obligatorio utilizar software y repositorio de control y versionamiento de archivos (como fuentes, modelos, documentos, diagramas, páginas web) aprobados por la Compañía.

7. Cada desarrollador es responsable de la integridad de los archivos de sistema en los que está trabajando y debe utilizar preferentemente áreas de trabajo en servidores designados.

8. Todo desarrollador de aplicaciones debe seguir, cuando estén disponibles y sean aplicables, las recomendaciones de seguridad para el desarrollo.

Administración de Servidores

1. Todas Todas las instalaciones de nuevos servidores deben seguir procedimientos estándar e incluir paquetes, Service Packs, actualizaciones críticas obligatorias.

2. La instalación de las actualizaciones de seguridad debe ser realizada por el responsable directo de cada servidor, siguiendo las orientaciones de seguridad respecto al backup antes del procedimiento, adecuación del horario y plan de recuperación de fallos.

3. Los accesos remotos deben realizarse siempre utilizando mecanismos cifrados. Se deben desactivar los servicios de acceso remoto que no utilicen cifrado.

4. Los equipos utilizados deben tener un sistema operativo actualizado e implementar recursos de seguridad.

5. La activación de nuevos servicios de red estará condicionada a un análisis de riesgos (a realizar por el Equipo de Seguridad e Infraestructura), donde se considerarán como mínimo los siguientes aspectos: requisitos de seguridad del servicio, objetivo, objetivo del servicio, forma de acceso, forma de administración y volumen de tráfico.

6. No está permitida la instalación de servicios de red no autorizados por el Equipo de Seguridad e Infraestructura.

7. Todo el tráfico de información confidencial a través de medios compartidos estará protegido mediante cifrado.

8. El equipo de Seguridad de la Información puede indicar y utilizar herramientas de detección y prevención de intrusos para emitir alertas y registrar posibles intentos de intrusión.

Desarrollo Seguro

1. Desarrollar conforme a las mejores prácticas de SDL (Ciclo de Vida del Desarrollo Seguro), TOP10 de OWASP (Open Web Application Security Project) y TOP25 de SANS (sans.org).

2. Desarrollar aplicando los principios de Privacidad por Diseño y Privacidad por Defecto, buscando la seguridad y protección de los datos tratados.

3. Capacitar al equipo de desarrollo en prácticas de desarrollo seguro.

4. NDD cuenta con una política interna específica para el desarrollo seguro de sus productos siguiendo las mejores prácticas del mercado.

Registros y Auditoría

1. Os Los administradores deben habilitar, siempre que sea posible, los registros de seguridad (logs) para ayudar en el análisis en caso de posibles fallos y/o en la realización de auditorías.

2. Los registros de seguridad deben ser revisados periódicamente (manual o automáticamente).

Aprobado por:
DIRECCIÓN