Comprometidos con la competitividad y el cumplimiento normativo, en DOSNÓMADAS la seguridad de la información es una prioridad. A través de la implementación de procesos de planificación, controles, supervisión y mejora continua, DOSNÓMADAS asegura la confidencialidad, integridad y disponibilidad de los servicios que ofrece.

La Dirección garantiza la implementación, el mantenimiento y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), cumpliendo con estándares internacionales y persiguiendo las siguientes metas:

- Evaluar y tratar los riesgos de la seguridad de la información.
- Gestionar las incidencias, potenciales o reales, de la seguridad de la información.
- Concienciar y capacitar a los empleados y colaboradores.
- Garantizar la continuidad del servicio.
- Cumplir la legislación de protección de datos personales y cualquier otra normativa aplicable en el ámbito de la seguridad de la información.

De acuerdo con la norma ISO/IEC 27001:2022, DOSNÓMADAS ha establecido un Sistema de Gestión de Seguridad de la Información (SGSI) que cumple de forma adecuada con todos los requisitos necesarios para garantizar la confidencialidad e integridad de la información.

1. Alcance

La presente política de seguridad será de aplicación en toda la empresa, ya sean recursos humanos o tecnológicos, bienes tangibles o intangibles, procesos internos o externos, a los proveedores o cualquier otra persona o entidad que interactúe con la información de la empresa o con los activos que la contienen.

La Dirección de DOSNÓMADAS ejercerá la supervisión de las medidas de seguridad de la información implementadas. No obstante, el cumplimiento de estas medidas constituirá una responsabilidad inherente a las funciones de empleados y colaboradores.

2. Seguridad física

2.1 Acceso al edificio

- El acceso al edificio de la empresa por individuos externos o sus colaboradores estará controlado mediante la identificación y registro en la recepción, además de la autorización previa del responsable de la unidad organizativa que se pretenda visitar, así como una puerta de seguridad a las instalaciones, que permitan detectar intentos de accesos no autorizados.

2.2 Acceso a dependencia críticas o restringidas

- El acceso a dependencias que se consideren críticas (Centro de Procesamiento de Datos, Archivo, etc.) será controlado por medio de sistemas que controlen el acceso, tales como cámaras de vigilancia, que permiten alertar de intentos de acceso no autorizados.

- Estas dependencias contarán con rótulos que indiquen su nivel de seguridad.

- El acceso de personas no autorizadas a estas dependencias, se producirá acompañado de personal interno autorizado de la empresa.

- Todos los empleados deben tener especial cuidado de no permitir el paso a personas no autorizadas a áreas críticas o restringidas.

2.3 Equipamiento de puesto de trabajo

- Todo equipo informático o de comunicación que procese información de la empresa o posea conectividad con los sistemas de esta, debe estar correctamente protegido mediante elementos que fijen los dispositivos a componentes fijos del entorno.

- Este equipamiento no podrá moverse de ubicación sin autorización expresa del departamento del Responsable de Seguridad.

- Ningún equipo de trabajo que procese información de la empresa o posea conectividad con los sistemas de esta podrá abandonar las instalaciones, a menos que la propia actividad de la empresa lo requiera.

2.4 Protección física de la información

- Todo el personal interno y externo de la organización será responsable del adecuado uso de la información suministrada para el desempeño de su labor profesional, por lo que se debe velar por su integridad, confidencialidad y disponibilidad.

- Toda información crítica, secreta y privada en cualquiera de sus formas (impresa, electrónica, etc.) debe ser resguardada y estar provista de la seguridad necesaria para evitar el uso indebido por parte del personal no autorizado.

- Toda la información que posea la organización en formato físico, será destruida mediante un proceso de trituración una vez ya no sea necesaria, evitando así un uso indebido de esta.

3. Red y comunicaciones

3.1 Control de la red

- La red de la empresa, así como las comunicaciones que transcurren sobre ella deben estar correctamente protegidos y limitado su acceso.

- Toda la información considerada crítica que sea transportada a través de redes de proveedores deberá ser correctamente cifrada.

- Las redes inalámbricas que se habiliten para el uso de comunicación de la empresa deberán tener la mayor protección posible tecnológicamente en todo momento.

3.2 Acceso y uso de internet

- El acceso a Internet en las instalaciones de la empresa se realizará exclusivamente con los accesos dispuestos por la empresa para tal fin.

- Queda prohibido el uso de plataformas de mensajería o de redes sociales a no ser que la persona esté autorizada previamente por la dirección para el desarrollo de su labor profesional en la empresa.

- Se restringirá el acceso de los usuarios a aquellas áreas de Internet que se identifiquen como inseguras o inapropiadas.

- Todo el personal interno y externo de la organización deberá adecuarse a la legislación vigente sobre derechos de reproducción y todo lo relacionado con derechos de autor que se aplica en Internet.

3.3 Conexiones con terceros

- Se llevarán a cabo inspecciones anuales a los sistemas de comunicación y de aplicaciones de terceros con el fin de verificar que la información se esté manejando con las medidas de seguridad acordadas.

- Toda la información transmitida por medios como correo electrónico, chats, etc deberán seguir procedimientos establecidos para asegurar la confidencialidad e integridad de la información.

3.4 Correo electrónico

- Los usuarios del correo electrónico de la organización no deben utilizar cuentas de correo electrónico que pertenezcan a otros usuarios.
- Los usuarios de correo electrónico no deben hacer uso del mismo para fines personales quedando su uso únicamente restringido al ámbito profesional.
- No se debe transmitir información confidencial por correo electrónico, a no ser que esté en formato protegido.

3.5 Dispositivos móviles

- El uso de teléfonos móviles y tabletas corporativas queda restringido únicamente al entorno de la empresa, quedando prohibido su uso para temas personales.
- El software instalado en teléfonos móviles y tabletas debe ser validado por la Dirección.
- Queda prohibida la instalación de aplicaciones que puedan poner en peligro la seguridad de la información de la empresa, así como aplicaciones de mensajería, redes sociales, juegos, etc.

4. Protección de los sistemas de información

En general, todo el equipamiento informático de la empresa, debe estar convenientemente protegido considerando la configuración de los sistemas operativos, el acceso no autorizado a los mismos, malware y actualizaciones de seguridad.

4.1 Adquisición de hardware

- La organización implementará un esquema de adquisición de hardware aprobado por la dirección de la empresa.
- Dicho esquema estará compuesto por dispositivos de probada reputación frente a vulnerabilidades relativas a la seguridad de la información.

4.2 Instalación y configuración de los sistemas

- En los servidores y equipos de usuarios, los servicios y protocolos que sean innecesarios para la función de cada servidor deberán ser deshabilitados.
- Todos los equipos informáticos de los usuarios deberán estar debidamente

protegidos con un software antivirus actualizado anualmente.

- La instalación de aplicaciones se realizará con la debida autorización expresa de la Organización.

- Todos los equipos informáticos estarán sincronizados con las fuentes de tiempo correspondientes.

- Todos los equipos deben contar con los últimos parches de seguridad proporcionados por los proveedores que sean importantes para el buen funcionamiento del sistema. Los parches importantes de seguridad deben instalarse dentro del plazo máximo de un mes desde su lanzamiento.

4.3 Adquisición de software

- Las aplicaciones adquiridas de terceros, deberán incluir en sus especificaciones puntos de seguridad de la información.

4.4 Administración del software

- La empresa deberá contar con un inventario actualizado del software de su propiedad, el comprado a terceros, el adquirido bajo licencia o el de libre distribución.

- La instalación de software en los equipos de la organización deberá ser realizada por el personal interno de la empresa con la debida autorización desde la Dirección. Esta autorización se basará en la evaluación de la aplicación y la debida justificación para ser instalada.

4.5 Detección de vulnerabilidades

- Deberán ejecutarse anualmente evaluaciones internas de vulnerabilidades por medio de herramientas especializadas para ayudar a mantener un estado seguro de la red, las aplicaciones y los servidores.

- Deberá ejecutarse por lo menos anualmente una revisión de vulnerabilidades de la red, servidores, aplicaciones externas y aplicaciones internas. El análisis de las vulnerabilidades internas se realizará mediante la Revisión por la Dirección.

5. Gestión de la información

5.1 Clasificación de la información

- Para evitar la pérdida, robo o transferencia no autorizada de la información clasificada o propiedad intelectual, toda la información contenida en los sistemas de la organización deberá ser clasificada de acuerdo a su nivel de sensibilidad. Para ello, se establecen las siguientes categorías:

    - CONFIDENCIAL: Información considerada sensible y controlada, que solamente puede ser divulgada interna o externamente a persona o grupo reducido de personas debidamente autorizadas.
    - INTERNO: Información de divulgación interna segura, no recomendada para divulgación externa.
    - PÚBLICA: Información que puede ser divulgada interna y externamente sin riesgos para la organización.

- Los responsables de la información serán los encargados de clasificar, proteger y autorizar el acceso a la información. Los responsables asumen el papel de tutores de la información, ya que la propiedad siempre será la propia organización.

- Toda información debe etiquetarse según la categoría definida.

5.2 Almacenamiento de la información

- Los datos confidenciales de autenticación de los usuarios no deberán almacenarse nunca, aunque estos estén cifrados.

- Toda información administrada por la organización debe tener una copia de respaldo completa y actualizada.

- La organización debe contar con un procedimiento para la restauración de copias de seguridad o backups.

- Toda la información de tipo legal debe ser conservada de acuerdo con las normas legales vigentes.

- El tratamiento de los datos de carácter personal y su nivel de protección será comunicado a los usuarios.

- La organización establecerá y mantendrá procedimientos para la adquisición, uso y gestión de sus servicios en la nube.

- La organización implementará controles de acceso rigurosos que restrinjan el tráfico entre segmentos a las comunicaciones estrictamente necesarias y autorizadas.

- Toda la información contable, de impuestos y de tipo legal debe ser conservada de acuerdo con las normas legales vigentes.

5.3 Administración de la información

- Cualquier tipo de información interna no puede ser vendida, transferida o intercambiada con terceros para ningún propósito diferente al del negocio. En caso de que la información sea requerida por auditores internos o externos, la entrega de dicha información deberá ser autorizada por el propietario de la información solicitada.

- El acceso a depósitos de información debe restringirse únicamente a personal autorizado.

5.4 Eliminación de datos

La eliminación de la información debe seguir procedimientos seguros y debidamente aprobados por el Director de Seguridad de la Información.

6. Acceso lógico

6.1 Contraseñas

- El acceso a los sistemas debe realizarse por medio de un código de identificación y contraseña únicos para cada usuario.

- Se establece una complejidad mínima de contraseña: Debe contener:

    - Mínimo de 8 caracteres
    - Al menos un número
    - Al menos una letra mayúscula
    - Al menos una letra minúscula
    - Al menos un carácter especial

- La contraseña deberá cambiarse de forma anual, avisando al usuario de este hecho 15 días antes de la caducidad, quedando obligado a realizar el cambio una vez caducada la contraseña.

- No se podrá repetir la última contraseña utilizada anteriormente.

6.2 Acceso de perfiles de usuario y privilegios

- La Dirección implementará los medios necesarios para proteger la integridad de la identificación, perfil y contraseña de acceso de usuario.

- Los perfiles de usuario serán definidos de acuerdo a la función y cargo que desempeñen en la empresa, de tal forma que la información solo sea accedida y/o modificada por los usuarios autorizados.

- La identificación del usuario (ID usuario) debe ser única para cada usuario habilitado en los sistemas de la organización.

- La identificación, el perfil y la contraseña de acceso del usuario serán de uso personal e intransferible.

- Los usuarios serán responsables de todas las actividades llevadas a cabo con su identificación, perfil y contraseña de acceso.

- La organización gestionará la capacidad de sus recursos de información críticos mediante la planificación, monitorización y ajuste proactivo para asegurar su disponibilidad y rendimiento, considerando las necesidades actuales y futuras del negocio.

- El sistema operativo deberá bloquear la cuenta del usuario después de 5 intentos fallidos y consecutivos. El bloqueo permanecerá hasta que un responsable de seguridad lo habilite de nuevo previa identificación del usuario.

- Los usuarios no abandonarán su equipo de trabajo sin haber realizado el bloqueo de su sesión.

- Queda restringido el uso de usuarios tipo ADMINISTRADOR o similares únicamente a las tareas estrictamente que necesiten este tipo de usuarios.