Políticas de Seguridad de la Información

Introducción

La seguridad de la información es fundamental para proteger los activos y la propiedad intelectual de una empresa. Esta política de seguridad de información establece los estándares de seguridad, que ayudarán a garantizar la integridad, confidencialidad y disponibilidad de la información.

Ámbito de aplicación

Esta política se aplica a todos los empleados, contratistas, socios comerciales y terceros que manejen información confidencial en nombre de la empresa. Los empleados deben cumplir con los requisitos establecidos en esta política, independientemente de su ubicación geográfica.

Responsabilidades

Es responsabilidad de cada empleado proteger la información confidencial y cumplir con los estándares de seguridad establecidos en esta política. La gerencia de la empresa es responsable de asegurar que esta política sea efectiva y adecuada para proteger la información confidencial.

Normas de seguridad

Acceso y control de contraseñas:

- Los empleados deben tener contraseñas seguras y cambiarlas regularmente.
- Las contraseñas no deben ser compartidas y en caso de escribirlas en papel, este debe ser privado y estar protegido del acceso público.
- Las cuentas deben bloquearse después de un tiempo de inactividad.
- Los empleados deben dejar bloqueado su equipo de trabajo cada vez que deban ausentarse temporalmente de su puesto de trabajo.
- Los empleados deben apagar su equipo de cómputo al finalizar labores.

- Las contraseñas confiadas a los colaboradores, ya sean internas o correspondientes a servicios de la marca, son estrictamente privadas e intransferibles. Se prohíbe su divulgación, publicación o compartición por cualquier medio. Asimismo, está prohibido almacenar dichas contraseñas en plataformas o servicios en la nube

Protección de dispositivos:

- Todos los dispositivos deben estar protegidos con una contraseña o PIN.
- Los dispositivos deben tener una solución antivirus y antimalware instalada y actualizada regularmente.
- No se permitirá el uso de dispositivos personales para funciones corporativas ni para almacenar información confidencial.
- Se prohíbe conectar cualquier dispositivo no corporativo a la red de datos de la compañía sin previa autorización y/o acompañamiento del área de TI. Se requiere autorización para usar puntos de red de datos.
- No se permite instalar, distribuir o utilizar software sin licencia
- La configuración e instalación de cualquier software en los dispositivos será realizada y/o autorizada por el personal de TI siempre que este cumpla con la legalidad y autorización de uso en el entorno corporativo.

Uso de correo electrónico y redes sociales:

- No se permitirá el uso de correo electrónico personal para comunicaciones de trabajo.
- No se permitirá el uso del correo empresarial para comunicaciones personales.
- Los empleados no pueden compartir información confidencial en las redes sociales.

- Los empleados deben seguir las normas y los tips de seguridad difundidos por las áreas de tecnología.
- Los empleados deben reportar al personal de TI cualquier duda o sospecha de riesgo informático (cualquier correo sospechoso).
- Las redes sociales serán usadas exclusivamente en el ámbito laboral.
- La información confidencial enviada por correo electrónico deberá ser a través de archivos adjuntos preferiblemente.

Uso de sitios o servicios de terceros en la nube para compartir información:

- No se compartirá información confidencial a través de servicios o almacenamientos en la web como WeTransfer o Google Drive.
- En caso de ser necesario transportar información a través de los canales mencionados, se deberá solicitar el apoyo del área de sistemas para garantizar la seguridad de los enlaces o proporcionar un mecanismo seguro con una cuenta empresarial asociada a un servicio como Microsoft 365.
- No se permite el uso de medios de almacenamiento personales, sean estos físicos o en la nube, para almacenar o transportar información de la compañía.
- No está permitido el uso de OneDrive, Google Drive y similares que sean de uso personal. Existe un procedimiento para compartir archivos con fines colaborativos.
- Todos los archivos de trabajo que no sean temporales deben ser almacenados y trabajados en la carpeta de red compartida, la cual cuenta con respaldo diario y políticas de seguridad de acceso y permisos de usuario.

Almacenamiento y eliminación de información:

- La información confidencial debe ser almacenada en lugares seguros y protegidos.
- La información confidencial debe ser eliminada permanentemente cuando ya no sea necesaria.

- No se pueden almacenar archivos personales, como imágenes, audio o video, en los repositorios de información de la empresa, a menos que sea estrictamente necesario para el trabajo.

Captura de video o fotografía en áreas restringidas:

- No se permite la captura de fotos o video de áreas restringidas.
- En caso de ser necesario, se debe tener autorización de gerencia.

Mensajería instantánea:

- WhatsApp, Skype y otros medios similares no son adecuados para compartir información confidencial. Se prohíbe enviar, difundir o compartir información confidencial de la compañía con terceros a través de estos medios. Las excepciones solo se permiten en el marco publicitario con la respectiva autorización del área comercial o de mercadeo.

Acceso remoto:

- Los empleados deben seguir las políticas de seguridad establecidas por la empresa cuando accedan a la información confidencial de forma remota.
- Los accesos son controlados por políticas de firewall y de Windows.
- No está estipulado el trabajo remoto generalizado. Sin embargo, se proporcionará información a directivos o personal autorizado mediante herramientas controladas por el área de TI, como SharePoint.

Copias de seguridad y recuperación:

- La información confidencial debe ser respaldada regularmente y almacenada de forma segura.
- Debe existir un plan de recuperación ante desastres y realizarse pruebas regularmente.

Incidentes de seguridad:

- Los incidentes de seguridad deben ser informados a la gerencia de la empresa.

- Se debe realizar una investigación y evaluación del incidente para tomar medidas correctivas.
- Los incidentes que representen un riesgo real a la seguridad serán informados a todas las partes interesadas para mitigar riesgos.

Cumplimiento legal:

- La empresa debe cumplir con todas las leyes y regulaciones aplicables.
- Los empleados deben seguir todas las políticas y procedimientos establecidos por la empresa.
- Se debe cumplir con las normativas y lineamientos aplicables relacionados con la información, incluyendo las políticas de protección de datos personales.

Uso de dispositivos móviles:

- No está permitido el uso de dispositivos personales para el manejo de información corporativa.
- Los dispositivos móviles utilizados para comunicaciones internas y con clientes estarán debidamente protegidos y contarán con un acta de entrega. Los responsables se comprometen a usarlos solo para las finalidades establecidas por la compañía. Cualquier uso indebido estará sujeto a acciones disciplinarias.

Horarios de disponibilidad de los servidores:

- El acceso al sistema ERP, a la red interna y a los servidores está restringido a los horarios laborales establecidos. Fuera de estos horarios, el acceso a dichos servicios está bloqueado mediante políticas implementadas en el servidor. Cualquier solicitud de acceso adicional deberá gestionarse previamente con el área de TI mediante un correo corporativo dirigido a la mesa de ayuda, con copia al coordinador de TI, y contará con la aprobación de la gerencia.

Cumplimiento de Normas o políticas afines:

- Es obligatorio acatar y cumplir las políticas establecidas a nivel de grupo por la Dirección de los concesionarios en materia de sistemas de información. Asimismo, se deben respetar las normativas legales y los lineamientos aplicables relacionados con la protección de la información, incluyendo las políticas de protección de datos personales.

Conclusiones

Esta política de seguridad de información debe ser revisada regularmente para asegurar que se siga aplicando de forma adecuada. Es responsabilidad de todos los empleados asegurar que la información confidencial esté protegida de forma segura y que se sigan los estándares de seguridad establecidos en esta política.

Cordialmente,

Javier Valencia Duque

CC.: 75080261

Gerente General