Anexo A – Política de Seguridad

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.

2. Seguridad física

2.1 Acceso a los edificios

- El acceso a los edificios de la será controlado mediante un sistema que controlen el acceso a mismo, tales como tarjetas de proximidad que limiten la entrada la salida de personas, además se contará con cámaras de vigilancia y detectores de intrusión 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, Departamento de I+D, etc.) será controlado por medio de sistemas que controlen el acceso en dos pasos, tales como tarjetas de proximidad más sistemas biométricos que limiten la entrada/salida, además, estos accesos contarán con cámaras de videovigilancia, detectores de intrusión y otros medios que permitan alertar de intentos de accesos no autorizados.

- Estas dependencias además deberán contar con rótulos que indiquen su nivel de seguridad.

- El acceso de personas no autorizadas a estas dependencias, se deberá producir 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 ser correctamente protegido mediante elementos que fijen estos dispositivos a elementos fijos del entorno.
- Este equipamiento no podrá moverse de ubicación sin autorización expresa del departamento de T.I.

- Ningún equipo de trabajo que procese información de la empresa o posea conectividad con los sistemas de esta, podrá abandonar las instalaciones de la empresa si autorización expresa del departamento de T.I.

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 por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

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 mediante elementos de red tales como Firewalls.

- Se deberá propiciar la segmentación de las redes de comunicaciones.

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

- El tráfico de la red de la empresa deberá ser monitorizado por elementos de red tales como IDS/IPS con almacenamiento de logs para el posterior análisis si fuera necesario.

- Las redes inalámbricas que se habiliten para el uso de comunicación de la empresa deberán tener la mayor protección disponible tecnológicamente en cada momento. (Actualmente WPA2-PSK) y control de acceso mediante servidor de autenticación corporativo.

3.2 Acceso y uso de internet

- El acceso a Internet en las instalaciones de la empresa se realizará exclusivamente por 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 monitorizan las actividades en Internet como accesos a correo web, salas de chat, mensajería instantánea, redes sociales, juegos online, etc.

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

3.3 Conexiones con terceros

- La conexión entre los sistemas internos de la organización y otros sistemas de terceros debe ser aprobada y certificada por el Departamento de TI con el fin de no comprometer la seguridad de la información interna.

- Se llevarán a cabo inspecciones 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 por ejemplo el fax, 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 uso profesional de sus actividades en la empresa.

- No se debe transmitir información confidencial por correo electrónico, a no ser que este 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 de debe ser validado por el departamento de T.I.

- 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 desarrollado por el departamento de T.I. y aprobada 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 usuarios deberán estar debidamente protegidos con un software antivirus actualizado y deben generar logs para su posterior análisis en caso de que fuera necesario.

- La instalación del sistema operativo de todos los sistemas de la empresa se realizará a través de una imagen validada por el departamento de T.I.
- Queda prohibida la instalación de aplicaciones sin la autorización expresa del departamento de T.I.

- 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

- La organización implementará un esquema de adquisición de software de terceros que incluya un contrato con el proveedor que contemple cláusulas para la protección de la información y del software adquirido, la documentación correspondiente y los medios de respaldo necesarios.

- Las aplicaciones adquiridas de terceros o desarrolladas internamente, 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 desarrollado internamente, el adquirido bajo licencia o el de libre distribución.

- Los ambientes de desarrollo, pruebas y producción deberán permanecer separados para su adecuada administración, operación, control y seguridad.

- La instalación de software en los equipos de la organización deberá ser realizada por el personal del Departamento de TI con la debida autorización del mismo. Esta autorización se basará en la evaluación de la aplicación y la debida justificación para ser instalada.

- Los programas que se encuentren en el ambiente de producción, solamente podrán ser modificados de acuerdo con los procedimientos internos establecidos y en todos los casos se considerarán planes de contingencia y recuperación.

4.5 Desarrollo software

- La organización implementará una metodología formal para el desarrollo de software seguro y las actividades de mantenimiento que cumplirán con las políticas, normas, procedimientos, controles y otras definiciones del proyecto aplicables en el desarrollo de sistemas y exigibles por el negocio.

- Los controles implementados deberán ser como mínimo los exigidos en los puntos relacionados a adquisición de software. Su revisión deberá estar incluida en los planes de auditoría de sistemas.

- Para el desarrollo de software solamente podrán ser utilizados generadores y herramientas de los cuales se tenga certeza de su comportamiento seguro y confiable, y que, además, haya sido aprobado por el Departamento de TI.

- Las aplicaciones desarrolladas por la empresa deberán seguir el modelo de tres capas (Presentación, Aplicación y Datos) convenientemente separadas.

- Las aplicaciones web deberán ser desarrolladas en base a directrices de codificación segura (por ejemplo, OWASP). Las aplicaciones web públicas deberán ser chequeadas por métodos manuales o automáticos por lo menos una vez al año o después de cada cambio.

4.6 Detección de vulnerabilidades

- Deberán ejecutarse trimestralmente 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. Esta tarea deberá ser ejecutada por una empresa especializada en este tipo de servicio.

5. Gestión de la información

5.1 Clasificación de la información

- 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.
  - USO 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 y todos los datos que se divulguen por cualquier medio deben mostrar la clasificación de sensibilidad de la información.

5.2 Almacenamiento de la información

- Las bases de datos que contengan datos críticos deben estar en el segmento de red de datos críticos, segregada de la red externa.

- 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, en un sitio externo a la ubicación en que se procesan dichos datos.

- La organización debe contar con un procedimiento para la restauración de copias de seguridad o backups. Este, estará administrado por el Departamento de TI.

- 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 documentación deberá ser autorizada por el propietario de la información solicitada.

- El acceso a depósitos de información (almacenamiento físico o medio magnético) 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 Departamento de TI.

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.

- La gestión de contraseñas de la empresa debe ser implementada con un sistema Single Sing On que permite el uso de una única contraseña para todos los sistemas de la empresa.

- 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 especia

- La contraseña deberá cambiarse cada 90 días, 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 las seis últimas contraseñas utilizadas anteriormente.

6.2 Acceso de perfiles de usuario y privilegios

- El Departamento de TI 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 único 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.

- El sistema operativo deberá bloquear la cuenta del usuario después de tres 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 bloque de su sesión.

- El sistema debe bloquear sesión automáticamente pasados 5 minutos de inactividad del usuario.

- Queda restringido el uso de usuarios tipo ROOT o ADMINISTRADOR o similares únicamente a las tareas estrictamente que necesiten este tipo de usuarios, permitiendo el uso de las mismas exclusivamente al personal de T.I.