BICTORI

EMPOWER LEADERS

PROTOCOLO

DE CIBERSEGURIDAD

MECEI360°

CORPORATE CERTIFICATION

STRENGTHENING BRANDS FOR THE FUTURE

PRODUCTS/SERVICES - INTERNAL CLIENT - EXTERNAL CLIENT - SOCIAL RESPONSIBILITY

BICTORI
EMPOWER LEADERS

PROTOCOLO DE CIBERSEGURIDAD

MECEI-MD-R5 | A1-14.6.2024

La seguridad de Bictori está totalmente garantizada por nuestros expertos: desde la prevención de amenazas, hasta la detección y respuesta rápida en tiempo real. Al ofrecer una infraestructura de nivel empresarial, BICTORI utiliza las siguientes plataformas para acceso digital:

- **Gmail** (Correo corporativo) / Meetings.
- **Wix** (Hosting website).
- **ADICORPI** (Portal Corporativo).
- **Redes Sociales** (Linkedin).

Acuerdo a las Políticas de la Compañía y Código Corporativo:

- Todos los colaboradores son responsables del uso seguro de los sistemas y datos que manejen.
- Se deberá reportar inmediatamente cualquier comportamiento inusual, sospechoso o anómalo en los dispositivos, plataformas o cuentas corporativas.
- No se permitirá compartir contraseñas ni credenciales de acceso con terceros bajo ninguna circunstancia.
- Se requiere el uso de contraseñas seguras (mínimo 10 caracteres, incluyendo mayúsculas, minúsculas, números y símbolos).
- Se debe cambiar la contraseña cada 90 días.
- Es obligatorio el uso de autenticación de dos factores (2FA) para acceso a plataformas.
- Sólo se permite el uso de dispositivos autorizados y protegidos con antivirus actualizado.
- Queda prohibido conectarse a redes Wi-Fi públicas para realizar tareas relacionadas con información sensible de la empresa.

- Los dispositivos deben bloquearse al ausentarse del puesto de trabajo.
- La información personal de candidatos, clientes y empleados debe almacenarse en plataformas seguras y autorizadas.
- Queda prohibido descargar, copiar o transferir información sensible a dispositivos personales o unidades externas sin autorización.
- Todos los correos, documentos y archivos que contengan datos sensibles deben estar cifrados o protegidos con contraseña.
- No se deben abrir archivos adjuntos ni enlaces sospechosos.
- Verificar siempre el remitente de un correo antes de responder o proporcionar información.
- En caso de recibir un correo de phishing, reenviar inmediatamente al área de soporte técnico y no interactuar con su contenido.
- Todos los sistemas y aplicaciones deben mantenerse actualizados.
- Responsabilidad de aplicar los parches de seguridad recomendados por los proveedores.
- La empresa realizará respaldos automáticos de la información crítica de forma periódica.
- Todos los colaboradores deberán guardar documentos importantes en las carpetas o nubes designadas por la empresa.
- Se realizarán capacitaciones obligatorias periódicas sobre buenas prácticas de ciberseguridad.
- Todos los nuevos colaboradores deberán firmar un documento de cumplimiento de políticas y acuerdo de confidencialidad antes de recibir acceso a los sistemas.

- Ante cualquier incidente de seguridad, los pasos a seguir son: Reportar de inmediato al área de tecnología o responsable de seguridad. Suspender el uso del sistema o dispositivo afectado. Seguir las indicaciones del protocolo interno para mitigación del incidente.

CERTIFICACIÓN MECEI360°

La compañía posee auditorías internas y externa para verificar, validar, ejecutar acciones, y reducir riesgos para los 4 pilares de la compañía: Cliente interno, cliente externo, productos/servicios, y responsabilidad social.