Compliance y Ciberseguridad.

German Rivera Martínez.

julio del 2023.

Caso 1: identificar una organización objetivo, sea ficticia o real, describiendo su contexto de negocio, líneas de servicio, infraestructura tecnológica, etc. A partir de dicha información, y describiendo las suposiciones que sean necesarias, realizar las siguientes actividades de cara al cumplimiento del RGPD y LOPDGDD:

1- Descripción de la organización.

Empresa (ficticia): Tropicalito Exports S.A.

1. **Ubicación**: Oreamuno, Cartago, Costa Rica.

2. **Líneas de servicio**: Exportación de pulpas y concentrados de frutas tropicales (piña, mango, maracuyá, cas) a diferentes países de Europa.

3. **Infraestructura tecnológica**:
    1. **ERP**: Gestión de operaciones.
    2. **CRM**: Relación con clientes y proveedores.
    3. **Página web**: Comercio vía web.
    4. **Redes internas**: Conexión segura entre oficinas, planta y bodegas.
    5. **Servidores**: Servidores locales y en la nube para respaldo y para operaciones.

2- Identificación de actividades de tratamiento y describir los campos requeridos.

Actividad de Tratamiento	Finalidad	Base Jurídica	Categorías de Datos	Plazo de Conservación	Medidas de Seguridad
Gestión de datos de clientes	Procesar pedidos y gestionar relaciones comerciales	Contrato y consentimiento	Nombre, dirección, correo electrónico, número de teléfono, historial de pedidos	5 años después de la última interacción	Encriptación, acceso restringido
Gestión de datos de empleados	Administración de personal, nómina y cumplimiento legal	Contrato y obligaciones legales	Nombre, dirección, número de seguridad social, detalles bancarios, historial	2 años después de la finalización del contrato	Encriptación, acceso restringido
Marketing y comunicaciones	Enviar promociones y actualizaciones a clientes	Consentimiento	Nombre y dirección de email.	Hasta que el cliente retire el consentimiento	Encriptación, opción de darse de baja
Videovigilancia	Seguridad de las instalaciones	Interés legítimo	Imágenes y videos de empleados y visitantes.	30 días, a menos que se requiera para investigación	Encriptación, acceso restringido

3- Acciones para cumplir con los principios de privacidad por defecto y diseño.

Acción	Descripción
Minimización de datos	Recolectar solo los datos necesarios para cada propósito específico.
seudonimización y encriptación	Aplicar técnicas para proteger los datos almacenados y transmitidos.
Transparencia	Informar claramente a los interesados sobre el uso de sus datos y obtener su consentimiento cuando sea necesario.
Acceso restringido	Limitar el acceso a los datos solo al personal autorizado que lo necesite para realizar su trabajo.
Auditorías regulares	Realizar auditorías periódicas para asegurar el cumplimiento de las políticas de privacidad y detectar posibles brechas.
Consentimiento explícito	Obtener el consentimiento explícito de los interesados cuando sea necesario y mantener registros de los mismos.
Evaluación continua	Evaluar continuamente las prácticas de tratamiento de datos y ajustarlas conforme a las mejores prácticas y la normativa vigente.

4- Análisis de riesgos.

Significado de los colores según importancia de probalidad:

1. **Rojo**: Alto riesgo (alta probabilidad y alto impacto)
2. **Anaranjado**: Riesgo medio-alto (alta probabilidad y medio impacto o media probabilidad y alto impacto)
3. **Amarillo**: Riesgo medio (media probabilidad y medio impacto)
4. **Verde**: Bajo riesgo (baja probabilidad y bajo impacto)

Riesgo	Probabilidad	Impacto	Medidas	Color
Pérdida de datos de clientes	Media	Alto	Copias de seguridad regulares, sistemas de detección de intrusos.	Anaranjado
Acceso NO autorizado a datos de empleados	Baja	Alto	Control de acceso, autenticación multi factor.	Amarillo
Fuga de información sensible	Alta	Alto	Encriptación de datos, políticas estrictas de uso de datos.	Rojo
Fallo en el sistema ERP	Media	Medio	Mantenimiento regular, redundancia en sistemas.	Amarillo
Ciberataques (phishing, malware)	Alta	Alto	Capacitación en ciberseguridad, soluciones antivirus y anti malware.	Rojo
Uso indebido de datos por parte de empleados	Media	Medio	Políticas claras de uso de datos, monitoreo de actividades internas.	Amarillo

5- Evaluación de impacto en privacidad (DPIA).

Actividad de Tratamiento	Evaluación de Impacto	Medidas
Uso de cámaras de seguridad en las instalaciones	Realizar una DPIA debido a la monitorización constante de empleados y visitantes	Informar a los interesados, limitar el acceso a las grabaciones, encriptar los datos de video.
Gestión de datos de salud de empleados	Realizar una DPIA por el tratamiento de datos sensibles de salud	Acceso restringido, consentimiento explícito.

6- Plan de implementación de medidas.

Medida	Descripción
Política de protección de datos	Desarrollar y implementar una política de protección de datos que cumpla con el RGPD y la LOPDGDD.
Capacitación continua	Realizar sesiones de capacitación continua para todos los empleados sobre protección de datos y ciberseguridad.
Auditorías internas	Realizar auditorías internas periódicas para garantizar el cumplimiento de las políticas de privacidad.
Actualización de sistemas	Asegurar que todos los sistemas y software estén actualizados con los últimos parches de seguridad.
Implementación de herramientas de privacidad	Utilizar herramientas de gestión de privacidad que faciliten el cumplimiento normativo.
Evaluación de proveedores	Evaluar y asegurar que todos los proveedores cumplan con las normativas de protección de datos.
Plan de respuesta a incidentes	Desarrollar y probar regularmente un plan de respuesta a incidentes de seguridad de datos.

Caso 2. Identificar una organización objetivo, sea ficticia o real, describiendo su contexto de negocio, líneas de servicio, infraestructura tecnológica, etc. A partir de dicha información, y describiendo las suposiciones que sean necesarias, realizar las siguientes actividades de cara al diseño e implantación de un plan de cumplimiento de la normativa penal

1- Identificación de delitos con componente penal.

Delito	Probabilidad	Impacto	Medidas	Color
Acceso ilegal a sistemas informáticos	Media	Alto	Implementar firewalls, monitoreo continuo, capacitación en ciberseguridad.	Anaranjado
Fraude electrónico	Baja	Alto	Sistemas de detección de fraude, controles de acceso estrictos.	Amarillo
Robo de propiedad intelectual	Alta	Alto	Encriptación de información sensible, políticas de acceso estrictas.	Rojo
Manipulación de datos	Media	Medio	Auditorías regulares, controles de integridad de datos.	Amarillo
Sabotaje interno	Baja	Alto	Políticas de acceso, monitoreo de actividades internas.	Amarillo

2- Plan de actuación desde el área de ciberseguridad.

Delito	Prevención	Detección
Acceso ilegal a sistemas informáticos	Implementar políticas de seguridad, uso de software actualizado, monitoreo de actividades sospechosas	Sistemas de detección de intrusiones (IDS/IPS), alertas de seguridad
Fraude electrónico	Verificación de transacciones, autenticación multi factor.	Monitoreo de transacciones inusuales, análisis de patrones de fraude
Robo de propiedad intelectual	Encriptación de información, políticas de acceso	Monitoreo de accesos a información sensible, alertas de acceso no autorizado
Manipulación de datos	Auditorías regulares, controles de integridad de datos	Herramientas de monitoreo de integridad de datos, alertas de cambios sospechosos
Sabotaje interno	Políticas de acceso, monitoreo de actividades internas	Sistemas de monitoreo de comportamiento, alertas de actividades inusuales

3- Indicadores y métricas.

Indicador	Métrica
Número de incidentes de seguridad detectados	Mensual, trimestral, anual
Tiempo de respuesta a incidentes	Media de horas desde la detección hasta la resolución
Número de sesiones de capacitación realizadas	Mensual, trimestral
Porcentaje de sistemas actualizados	Mensual
Número de auditorías realizadas	Trimestral, anual

4- Catálogo de evidencias y cadena de custodia.

Evidencias	Medidas para la cadena de custodia
Logs de acceso, registros de incidentes, copias de seguridad	Protocolo de manejo de evidencias, almacenamiento seguro, registro de acceso a evidencias

5- Implementación del plan de cumplimiento.

Actividad	Descripción
Creación del comité de ciberseguridad	Formar un comité que supervise y revise todas las actividades relacionadas con ciberseguridad.
Desarrollo de políticas	Redactar y implementar políticas claras sobre el uso de TI y protección de datos.
Implementación de tecnologías	Adquirir e implementar tecnologías de seguridad como firewalls, IDS/IPS, soluciones anti malware.
Capacitación y concienciación	Realizar programas de capacitación y concienciación en seguridad para todos los empleados.
Revisión y mejora continua	Establecer un proceso de revisión y mejora continua de todas las medidas de seguridad y políticas implementadas.