Competencias Avanzadas en Ciberseguridad

German Rivera Martínez.

Realizado: julio del 2024.

Caso : 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, describir de forma extensa cómo se llevaría a cabo la implantación del marco de ciberseguridad del NIST. Dentro de dicha implantación concretar y razonar las medidas de seguridad por cada una de las dimensiones que se llevarían a la práctica.

1. Identificación de la Organización Objetivo

Organización: Tico Hot Spice S.A. (Ficticia)

- **Contexto de Negocio**: Tico Hot Spice S.A. es una empresa costarricense dedicada a la producción y exportación de salsas picantes y aderezos al continente europeo.

- **Líneas de Servicio**:

  Producción: Elaboración de salsas picantes y aderezos en plantas especializadas.

  a) **Empaque**: Empaque de productos en envases adecuados para exportación.
  b) **Despacho**: Logística y transporte de productos hacia los mercados europeos.
  c) **I y D**: Investigación y desarrollo de nuevas recetas y mejora de productos existentes.
  d) **Ventas y Marketing**: Promoción y venta de productos en mercados internacionales.
  e) **Atención al Cliente**: Servicio postventa y soporte a clientes.

- **Infraestructura Tecnológica**:
  a) **Red de comunicaciones**: WAN para conectar oficinas centrales, fábricas y centros de distribución.
  b) **Servidores**: Servidores físicos y virtuales para aplicaciones empresariales (ERP, CRM, SCM).
  c) **Dispositivos de usuario final**: Computadoras de escritorio, laptops, tablets y teléfonos inteligentes.
  d) **Seguridad**: Firewalls, sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), y soluciones de SIEM.
  e) **Almacenamiento de Datos**: Sistemas de almacenamiento en la nube y locales para la gestión de datos.

2. Implantación del Marco de Ciberseguridad del NIST

El Marco de Ciberseguridad del NIST se divide en cinco funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar en Tico Hot Spice S.A.

Identificar

- **Gestión de Activos (Asset Management)**:
    a) Inventario completo de todos los activos tecnológicos, incluyendo hardware, software y datos críticos.
    b) Uso de herramientas de gestión de activos (AMS) para mantener un registro actualizado.
    c) Clasificación de activos según su importancia y sensibilidad para el negocio.

- **Entorno de Negocio (Business Environment)**:
    a) Identificación de las funciones críticas de negocio y su interdependencia con la tecnología.
    b) Análisis de impacto en el negocio (BIA) para priorizar recursos y esfuerzos de ciberseguridad.
    c) Evaluación de la cadena de suministro para identificar posibles riesgos asociados con terceros.

- **Gobernanza (Governance)**:
    a) Cración de políticas y procedimientos de ciberseguridad alineados con normativas y mejores prácticas internacionales.
    b) Establecimiento de roles y responsabilidades claras en ciberseguridad.
    c) Creación de un comité de ciberseguridad para supervisar la implementación y cumplimiento de políticas dentro de la compañía.

- **Evaluación de Riesgos (Risk Assessment)**:
    a) Realización de evaluaciones de riesgos continuas para identificar y monitorea vulnerabilidades y amenazas.
    b) Uso de metodologías como OCTAVE o FAIR para evaluar y cuantificar riesgos.
    c) Evaluación de riesgos específicos para cada línea de servicio y proceso crítico.

- **Estrategia de Gestión de Riesgos (Risk Management Strategy)**:
    a) Desarrollo de estrategias para mitigar riesgos identificados y minimizar impactos.
    b) Implementación de controles de seguridad apropiados y eficientes.
    c) Revisión y actualización periódica de la estrategia de gestión de riesgos para adaptarse a nuevos desafíos.

Proteger

- **Control de Acceso (Access Control)**:
    a) Implementación de autenticación multi factor (MFA) para todos los usuarios.
    b) Políticas de gestión de identidades y acceso basado en roles (RBAC).
    c) Uso de soluciones de gestión de identidades y accesos (IAM) para automatizar y reforzar controles de acceso.

- **Concienciación y Formación (Awareness and Training)**:
    a) Programas de capacitación en ciberseguridad para todos los empleados.
    b) Simulaciones de phishing y otras amenazas para aumentar la conciencia de seguridad.
    c) Cursos y talleres periódicos para mantener al personal actualizado sobre las últimas amenazas y mejores prácticas.

- **Seguridad de Datos (Data Security)**:
    a) Encriptación de datos en tránsito y en reposo para proteger la confidencialidad e integridad de la información.
    b) Implementación de soluciones de prevención de pérdida de datos (DLP) para evitar fugas de información.
    c) Políticas de retención y eliminación de datos para asegurar el cumplimiento regulatorio y la minimización de riesgos.

- **Procesos y Procedimientos de Protección de Información (Information Protection Processes and Procedures)**:
    a) Documentación de procedimientos claros para la protección de información y respuesta a incidentes.
    b) Auditorías regulares para asegurar el cumplimiento de políticas y procedimientos.

c) Implementación de controles de acceso físico y lógico para proteger la infraestructura crítica.

- **Mantenimiento (Maintenance)**:
  a) Mantenimiento regular de sistemas y aplicaciones para asegurar su correcto funcionamiento y seguridad.
  b) Gestión de parches y actualizaciones para cerrar vulnerabilidades conocidas.
  c) Monitoreo y evaluación continua de la efectividad de las medidas de seguridad implementadas.

- **Tecnología Protectora (Protective Technology)**:
  a) Implementación de firewalls de próxima generación para proteger la red.
  b) Uso de soluciones de Endpoint Detection and Response (EDR) para proteger dispositivos finales.
  c) Despliegue de tecnologías de protección avanzada como sandboxing y honeypots para detectar y mitigar amenazas sofisticadas.

Detectar

- **Anomalías y Eventos (Anomalies and Events)**:
  a) Detección de comportamientos anómalos y eventos de seguridad en tiempo real.
  b) Configuración de alertas para notificar incidentes potenciales.
  c) Análisis de patrones y tendencias para identificar posibles amenazas.

- **Monitoreo Continuo de Seguridad (Security Continuous Monitoring)**:
  a) Monitoreo continuo de la seguridad utilizando soluciones de SIEM.
  b) Análisis de amenazas para identificar y responder rápidamente a incidentes.
  c) Implementación de sistemas de monitoreo de red y comportamiento de usuarios (UEBA) para detectar amenazas internas y externas.

- **Procesos de Detección (Detection Processes)**:
  a) Definición de procesos claros para la detección y respuesta a incidentes de seguridad.
  b) Coordinación con equipos internos y externos para una respuesta efectiva.
  c) Documentación y revisión regular de los procesos de detección para asegurar su efectividad y adecuación.

Responder

- **Planificación de Respuesta (Response Planning)**:
    a) Desarrollo de un plan de respuesta a incidentes (IRP) detallado y realización de simulaciones periódicas.
    b) Definición de roles y responsabilidades en caso de incidentes de seguridad.
    c) Establecimiento de un centro de operaciones de seguridad (SOC) para la gestión centralizada de incidentes.

- **Comunicaciones (Communications)**:
    a) Establecimiento de protocolos de comunicación claros durante incidentes de seguridad.
    b) Coordinación con partes interesadas internas y externas.
    c) Uso de canales de comunicación seguros para la transmisión de información sensible durante incidentes.

- **Análisis (Analysis)**:
    a) Análisis exhaustivo de incidentes para entender su alcance, origen y impacto.
    b) Documentación de hallazgos y lecciones aprendidas.
    c) Evaluación de la efectividad de las medidas de mitigación implementadas y ajuste de las mismas según sea necesario.

- **Mitigación (Mitigation)**:
    a) Implementación de medidas para mitigar los efectos de incidentes de seguridad.
    b) Revisión y ajuste de controles de seguridad basados en los análisis de incidentes.
    c) Colaboración con proveedores y socios para asegurar una respuesta integral y coordinada.

- **Mejoras (Improvements)**:
    a) Mejora continua basada en análisis post-incidente y retroalimentación.
    b) Actualización de planes y procedimientos de respuesta a incidentes.
    c) Formación y capacitación continua del personal en respuesta a incidentes.

Recuperar

- **Planificación de Recuperación (Recovery Planning)**:
    a) Desarrollo de un plan de recuperación ante desastres (DRP) y realización de pruebas periódicas.
    b) Definición de procesos para la recuperación de operaciones y sistemas críticos.
    c) Coordinación con proveedores y socios para asegurar una recuperación rápida y eficiente.

- **Mejoras (Improvements)**:
    a) Evaluación y mejora de los planes de recuperación basados en lecciones aprendidas.
    b) Ajustes a los procesos de recuperación para aumentar su efectividad.
    c) Implementación de soluciones de continuidad de negocio (BCP) para asegurar la disponibilidad de servicios críticos.

- **Comunicaciones (Communications)**:
    a) Comunicación clara y efectiva durante el proceso de recuperación.
    b) Coordinación con todas las partes interesadas para una recuperación rápida y eficiente.
    c) Uso de herramientas de comunicación y colaboración para facilitar la gestión de la recuperación.

Medidas de Seguridad por Dimensión

Identificar

- **Gestión de Activos (Asset Management)**:
    a) Implementación de un sistema de gestión de activos (AMS) para llevar un registro detallado de todos los dispositivos y software.
    b) Auditorías periódicas para asegurar la precisión del inventario de activos.
    c) Clasificación de activos según su importancia y sensibilidad para el negocio.

- **Evaluación de Riesgos (Risk Assessment)**:
    a) Evaluaciones de riesgo trimestrales utilizando metodologías como OCTAVE o FAIR.
    b) Análisis de impacto en el negocio (BIA) para priorizar recursos y esfuerzos de ciberseguridad.
    c) Evaluación de riesgos específicos para cada línea de servicio y proceso crítico.

Proteger

- **Control de Acceso (Access Control)**:
    a) Uso de autenticación multifactor (MFA) y políticas de contraseñas robustas.
    b) Implementación de soluciones de gestión de identidades y acceso (IAM) con políticas de control de acceso basado en roles (RBAC).
    c) Monitoreo y revisión regular de accesos y permisos para asegurar su adecuación.

- **Seguridad de Datos (Data Security)**:
    a) Implementación de soluciones de Data Loss Prevention (DLP) para evitar fugas de información.
    b) Encriptación de datos en tránsito y en reposo para proteger la confidencialidad e integridad de la información.
    c) Políticas de retención y eliminación de datos para asegurar el cumplimiento regulatorio y la minimización de riesgos.

- **Tecnología Protectora (Protective Technology)**:
    a) Actualización regular de firewalls y antivirus.
    b) Uso de soluciones de Endpoint Detection and Response (EDR) y tecnologías de sandboxing para analizar y detener amenazas avanzadas.
    c) Implementación de soluciones de protección de aplicaciones web (WAF) para proteger contra ataques específicos.

Detectar

- **Monitoreo Continuo de Seguridad (Security Continuous Monitoring)**:
    a) Uso de soluciones SIEM (Security Information and Event Management) para monitoreo en tiempo real.
    b) Implementación de sistemas de monitoreo de red y comportamiento de usuarios (UEBA) para detectar amenazas internas y externas.

c) Revisión y ajuste continuo de las reglas de monitoreo y alertas para asegurar su efectividad.

- **Anomalías y Eventos (Anomalies and Events)**:
  a) Configuración de alertas y reglas personalizadas para detectar comportamientos anómalos.
  b) Análisis de patrones y tendencias para identificar posibles amenazas.
  c) Integración de fuentes de inteligencia de amenazas (TI) para mejorar la detección y respuesta.

Responder

- **Planificación de Respuesta (Response Planning)**:
  a) Desarrollo y pruebas regulares de un plan de respuesta a incidentes (IRP).
  b) Simulaciones de incidentes para evaluar la efectividad del plan y ajustar según sea necesario.
  c) Establecimiento de un centro de operaciones de seguridad (SOC) para la gestión centralizada de incidentes.

- **Comunicaciones (Communications)**:
  a) Establecimiento de un equipo de comunicación de crisis.
  b) Protocolos claros de comunicación interna y externa durante incidentes de seguridad.
  c) Uso de canales de comunicación seguros para la transmisión de información sensible durante incidentes.

Recuperar

- **Planificación de Recuperación (Recovery Planning)**:
  a) Implementación de un plan de recuperación ante desastres (DRP) y pruebas de recuperación periódicas.
  b) Definición de procesos para la recuperación de operaciones y sistemas críticos en caso de desastres.
  c) Coordinación con proveedores y socios para asegurar una recuperación rápida y eficiente.

- **Mejoras (Improvements)**:
  a) Evaluaciones post incidente para identificar áreas de mejora.

b) Ajustes a los procesos de recuperación para aumentar su efectividad.
c) Implementación de soluciones de continuidad de negocio (BCP) para asegurar la disponibilidad de servicios críticos.

Procesos de Negocio Críticos.

Proceso	***Descripción***	***Intervinientes***	***Evidencias***
Producción	Producción y procesamiento de salsas	Empleados, proveedores	Registros de producción, informes de calidad
Empaquetado	Empaquetado y etiquetado	Empleados	Documentos de control de calidad, registros de empaquetado
Exportación	Logística y transporte	Transportistas	Documentos de envío, registros de seguimiento
Investigación y Desarrollo	Desarrollo de nuevos productos y mejora de productos existentes	Empleados de IyD, proveedores	Documentos de investigación, registros de pruebas
Ventas y Marketing	Promoción y venta de productos	Equipo de ventas y marketing	Registros de ventas, informes de marketing
Atención al Cliente	Soporte postventa y atención al cliente	Equipo de soporte al cliente	Registros de interacciones con clientes, informes de satisfacción

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 en materia de gestión de evidencias electrónicas:

1. Identificación de la Organización Objetivo

Organización: Tico Hot Spice S.A.

- **Contexto de Negocio**: Exportación de salsas picantes y aderezos a la Unión Europea.
- **Líneas de Servicio**: Producción, empacado, distribución y exportación de salsas picantes y aderezos.

2. Gestión de Evidencias Electrónicas

Identificación de Procesos de Negocio Críticos

- **Proceso de Producción**: Incluye la producción y procesamiento de salsas y aderezos.
- **Proceso de Empacado**: Clasificación, empacado y etiquetado de productos.
- **Proceso de Exportación**: Logística y transporte de productos al mercado europeo.
- **Proceso de Investigación y Desarrollo**: Desarrollo de nuevos productos y mejora de productos existentes.
- **Proceso de Ventas y Marketing**: Promoción y venta de productos en mercados internacionales.
- **Proceso de Atención al Cliente**: Servicio postventa y soporte a clientes.

Identificación de Intervinientes, Escenarios de Responsabilidad y Catálogo de Evidencias

- **Intervinientes**: Empleados, proveedores, clientes, transportistas, equipo de I y D, equipo de ventas y marketing, equipo de soporte al cliente.

- **Escenarios de Responsabilidad**:
    a) **Producción**: Control de calidad, gestión de insumos.
    b) **Empaquetado**: Verificación de cantidades, control de calidad.
    c) **Exportación**: Seguimiento de envíos, documentación aduanera.
    d) **Investigación y Desarrollo**: Gestión de proyectos de I+D, pruebas y validaciones.
    e) **Ventas y Marketing**: Campañas de marketing, gestión de ventas.
    f) **Atención al Cliente**: Resolución de consultas y quejas, mantenimiento de la satisfacción del cliente.

- **Catálogo de Evidencias**:
    a) **Producción**: Registros de producción, informes de calidad.
    b) **Empaquetado**: Documentos de control de calidad, registros de empaquetado.
    c) **Exportación**: Documentos de envío, registros de seguimiento.
    d) **Investigación y Desarrollo**: Documentos de investigación, registros de pruebas y validaciones.
    e) **Ventas y Marketing**: Informes de campañas de marketing, registros de ventas.
    f) **Atención al Cliente**: Registros de interacciones con clientes, informes de cumplimiento de satisfacción.

Protección de las Evidencias.

- **Producción**: Almacenamiento seguro de registros en bases de datos con acceso restringido.
- **Empacado**: Uso de sistemas de gestión documental con auditoría de acceso.
- **Exportación**: Encriptación de documentos de envío y seguimiento, y almacenamiento seguro.
- **Investigación y Desarrollo**: Protección de la propiedad intelectual mediante encriptación y acceso restringido.
- **Ventas y Marketing**: Protección de datos de clientes y estrategias de marketing mediante encriptación y políticas de acceso.
- **Atención al Cliente**: Almacenamiento seguro de registros de interacciones con clientes y protección de datos personales.

Tabla 2: Procesos de Negocio Crítico

Proceso	***Descripción***	***Intervinientes***	***Evidencias***
Producción	Producción y procesamiento de salsas	Empleados, proveedores	Registros de producción, informes de calidad
Empaquetado	Empaquetado y etiquetado	Empleados	Documentos de control de calidad, registros de empaquetado
Exportación	Logística y transporte	Transportistas	Documentos de envío, registros de seguimiento
Investigación y Desarrollo	Desarrollo de nuevos productos y mejora de productos existentes	Empleados de I+D, proveedores	Documentos de investigación, registros de pruebas
Ventas y Marketing	Promoción y venta de productos	Equipo de ventas y marketing	Registros de ventas, informes de marketing
Atención al Cliente	Soporte postventa y atención al cliente	Equipo de soporte al cliente	Registros de interacciones con clientes, informes de satisfacción