PAS 96 : 2017

Guía para la protección y defensa de los alimentos y bebidas de ataque deliberado

Department for Environment Food & Rural Affairs

Food Standards Agency
food.gov.uk

bsi.

Publicaciones e información de derechos de autor

El aviso de copyright BSI está representada en este documento indica que el documento fue emitido el pasado.

ISBN 978 0 580 98 099 2

ICS 67.020

historia de la publicación

Primero publicado en marzo de 2008 Segunda edición de

marzo 2010 Tercera edición de octubre 2014 Cuarta (actual)

2017 edición de noviembre

Contenido

Prefacio

Este PAS fue patrocinado por el Departamento de Asuntos de Medio Ambiente, Alimentación y Rurales (DEFRA) y la Food Standards Agency (FSA). Su desarrollo fue facilitado por BSI Normas limitada y se publicó bajo licencia de The British Standards Institution. Que entró en vigor el 16 de noviembre 2017.

Se agradece a las siguientes organizaciones que participaron en el desarrollo de esta PAS como miembros del grupo de dirección:

- Agrico UK Limited
- Federación Británica de Alimentos Congelados (BFFF)
- Campden BRI
- Crowe Clark Whiteh yo ll LLP
- Danone
- Departamento de Asuntos de Medio Ambiente, Alimentación y Rurales (DEFRA)
- Food Standards Agency
- GIST Limited
- Europa McDonald
- Centro Nacional de Seguridad Cibernética (NSCS)
- Sodexo Limited
- Tesco Reino Unido
- tulipán Limited
- University College de Londres
- Willis Towers Watson

El reconocimiento también se da a los miembros de un panel de revisión más amplia que fueron consultados en el desarrollo de esta PAS.

Este PAS no debe ser considerado como un estándar británico. Será retirada cuando se publique su contenido en, o como, un estándar británico.

El proceso de PAS permite una guía que se desarrolló rápidamente con el fin de satisfacer una necesidad inmediata en la industria. Un PAS se puede considerar para su posterior desarrollo como un estándar británico, o constituyen parte de la entrada del Reino Unido en el desarrollo de un europeo o Norma Internacional.

Sustitución

PAS PAS Este remplaza 96: 2014, que se retira.

Información sobre este documento

Esta es una revisión completa de la PAS 96: 2014, e introduce los siguientes cambios principales:

- referencias normativas e informativas se han actualizado;
- subcláusula 3.7 Cyber-crimen ha sido revisado;
- subcláusula 6.2.4 añadido a las vulnerabilidades de cobertura relacionadas con los ataques cibernéticos;
- dos nuevos estudios de caso de ficción se han añadido como los incisos A.5 y A.6 para ilustrar los problemas de seguridad cibernética;
- Anexo B actualiza;
- Anexo D añadió que cubre 10 pasos a la seguridad cibernética;
- Se han realizado algunas modificaciones en la redacción.

El uso de este documento

A modo de guía, esta PAS toma la forma de orientaciones y recomendaciones. No debe ser citado como si se tratara de una especificación o un código de prácticas y demandas de cumplimiento no se pueden hacer a la misma.

convenciones de presentación

La orientación en este estándar se presenta en roman tipo (es decir en posición vertical). Las recomendaciones se expresan en frases en las que el director verbo auxiliar es “debe”.

Comentario, explicación y material informativo en general se presentan en letra cursiva más pequeño, y no constituyen un elemento normativo.

consideraciones contractuales y legales

Esta publicación no pretende incluir todas las disposiciones necesarias de un contrato. Los usuarios son responsables de su correcta aplicación.

El cumplimiento de un PAS puede conferir inmunidad no de las obligaciones legales.

Introducción

La industria alimentaria ve la seguridad de sus productos como su principal preocupación. Con los años, la industria y los reguladores tienen sistemas de gestión de seguridad alimentaria desarrollados que significa que grandes brotes de intoxicación alimentaria son ahora bastante inusual en muchos países. Estos sistemas suelen utilizar Análisis de Peligros y Puntos Críticos de Control (HACCP), que son aceptados a nivel mundial. [1)]

HACCP ha demostrado ser eficaz contra la contaminación accidental.

los principios del HACCP sin embargo, no se han utilizado de forma rutinaria para detectar o mitigar los ataques deliberados contra un sistema o proceso. Tales ataques incluyen contaminación deliberada, intrusión electrónica, y el fraude. actos deliberados pueden tener consecuencias para la seguridad alimentaria, pero pueden dañar a las organizaciones de otras maneras, como dañar la reputación comercial o extorsionar.

El factor común detrás de todos estos actos deliberados son las personas. Estas personas pueden estar dentro de un negocio de comida, pueden ser empleados del proveedor de la empresa alimentaria, o pueden ser extraños completas sin conexión con el negocio de comida. La cuestión clave es su motivación, que puede apuntar a causa daño a la salud humana, la reputación del negocio, o hacer ganancias financieras a expensas de la empresa. En cualquiera de estas situaciones es en interés de la empresa alimentaria para protegerse de este tipo de ataques.

El propósito de PAS 96 es guiar a los gerentes de empresas alimentarias a través de enfoques y procedimientos para mejorar la capacidad de resistencia de las cadenas de suministro a fraude u otras formas de ataque. Su objetivo es asegurar la autenticidad y la seguridad de los alimentos, reduciendo al mínimo la posibilidad de un ataque y mitigar las consecuencias de un ataque exitoso.

PAS 96 describe Amenaza Puntos Críticos de Control de Evaluación (TACCP), una metodología de la gestión de riesgos, que se alinea con HACCP, pero tiene un enfoque diferente, que puede necesitar el aporte de los empleados de diferentes disciplinas, tales como recursos humanos, compras, seguridad y tecnología de la información.

En él se explica el proceso TACCP, describe los pasos que pueden disuadir a un atacante o dar la detección temprana de un ataque, y utiliza estudios de casos ficticios (véase el Anexo A) para mostrar su aplicación. En términos generales, TACCP coloca gerentes de empresas alimentarias en la posición de un atacante para anticipar su motivación, la capacidad y la oportunidad de llevar a cabo un ataque, y luego les ayuda a diseñar protección. También ofrece otras fuentes de información e inteligencia que ayuda puede identificar las amenazas emergentes (véase el anexo B).

El proceso TACCP asume y se basa en un negocio operación eficaz del sistema existente, ya que muchas precauciones tomadas para garantizar la seguridad de los alimentos es probable que también disuadir o detectar actos deliberados. También complementa los procesos de gestión de riesgos de negocio y de gestión de incidencias existentes.

El enfoque de esta PAS es en la protección de la integridad y salubridad de los alimentos y el suministro de alimentos. Cualquier atacante intención, ya sea desde el interior de un negocio de comida o su cadena de suministro o externo a ambos, es probable que intente eludir o evitar los procesos de gestión de rutina. Debe ayudar a mitigar las empresas alimentarias cada una de estas amenazas, pero el enfoque también puede ser utilizado para otras amenazas de negocio.

Ningún proceso puede garantizar que los alimentos y el suministro de alimentos no son el objetivo de la actividad delictiva, pero el uso de PAS 96 puede hacer que sea menos probable. Se tiene la intención de ser una guía práctica y fácil de utilizar y así está escrito en el lenguaje cotidiano y se va a utilizar en un sentido común en lugar de manera legalista.

1) Más información y orientación con respecto a HACCP se pueden encontrar en la publicación del Codex Alimentarius, *Principios Generales de Higiene de los Alimentos* [1].

1 Alcance

Este PAS proporciona orientación sobre la prevención y mitigación de las amenazas a la comida y el suministro de alimentos. En él se describe una metodología de la gestión de riesgos, la amenaza Puntos Críticos de Control Evaluación (TACCP), que puede ser adaptada por las empresas alimentarias de todos los tamaños y en todos los puntos en las cadenas de suministro de alimentos. Mientras que las preocupaciones por la seguridad e integridad de la comida y la bebida son de suma importancia y gran parte del PAS se centra en ellos, es necesario hacer hincapié en que su alcance se refiere a 'todas las amenazas' y la protección de todos los elementos del suministro de alimentos. Esto incluye la viabilidad de negocios dentro de la cadena de suministro.

Se pretende que sea de utilidad para todas las organizaciones, pero es de particular utilidad para los gerentes de pequeñas y medianas empresas de alimentos de tamaño sin fácil acceso a asesoramiento especializado.

2 Términos y definiciones

A los efectos de esta PAS, se aplican los siguientes términos y definiciones.

la seguridad cibernética 2.1

protección de los dispositivos, servicios y redes - y la información sobre ellos - de robo o daño

{FUENTE: NCSC Glosario [2]}

2,2 defensa alimentos

procedimientos adoptados para garantizar la seguridad de los alimentos y bebidas y sus cadenas de suministro de ataque malicioso e ideológicamente motivado que conduce a la contaminación o la interrupción de suministro

***NOTA** La seguridad alimentaria término se refiere a la confianza con la que las comunidades ven la comida que está disponible para ellos en el futuro. Excepto en el sentido limitado de que un ataque exitoso puede afectar a la disponibilidad de alimentos, la seguridad alimentaria no se utiliza y está fuera del alcance de este PAS.*

fraude 2.3 de alimentos

acto u omisión deshonesto, en relación con la producción o suministro de alimentos, que está prevista para el beneficio personal o para la pérdida de causa a otra parte [2)]

***NOTA 1** Aunque hay muchos tipos de fraude alimentario los dos tipos principales son:*

1) la venta de comida, que es apto y potencialmente perjudiciales, tales como:

- *reciclaje de subproductos animales de nuevo en la cadena alimentaria;*
- *embalaje y venta de carne de vacuno y aves de corral con un origen desconocido;*
- *venta de bienes a sabiendas que están más allá de su "fecha de caducidad;*

[2)] La Agencia de Normas Alimentarias del Reino Unido discute el crimen de alimentos y comida en el fraude: https://www.food.gov.uk/enforcement/thenational-food-crime-unit/what-is-food-crime-and-food-fraud [3].

2) la descripción errónea deliberada de los alimentos, tales como:

- *productos sustituidos con una alternativa más barata, por ejemplo, el salmón de piscifactoría vendido como salvaje, y el arroz Basmati adulterada con variedades más baratas;*
- *hacer declaraciones falsas sobre la fuente de los ingredientes, es decir, su geográfica, vegetal o animal.*

***NOTA 2** fraude alimentario también puede implicar la venta de la carne de animales que han sido robados y / o ilegalmente sacrificados, así como animales de caza salvajes como ciervos que pueden haber sido escalfados.*

2.4 Protección de alimentos

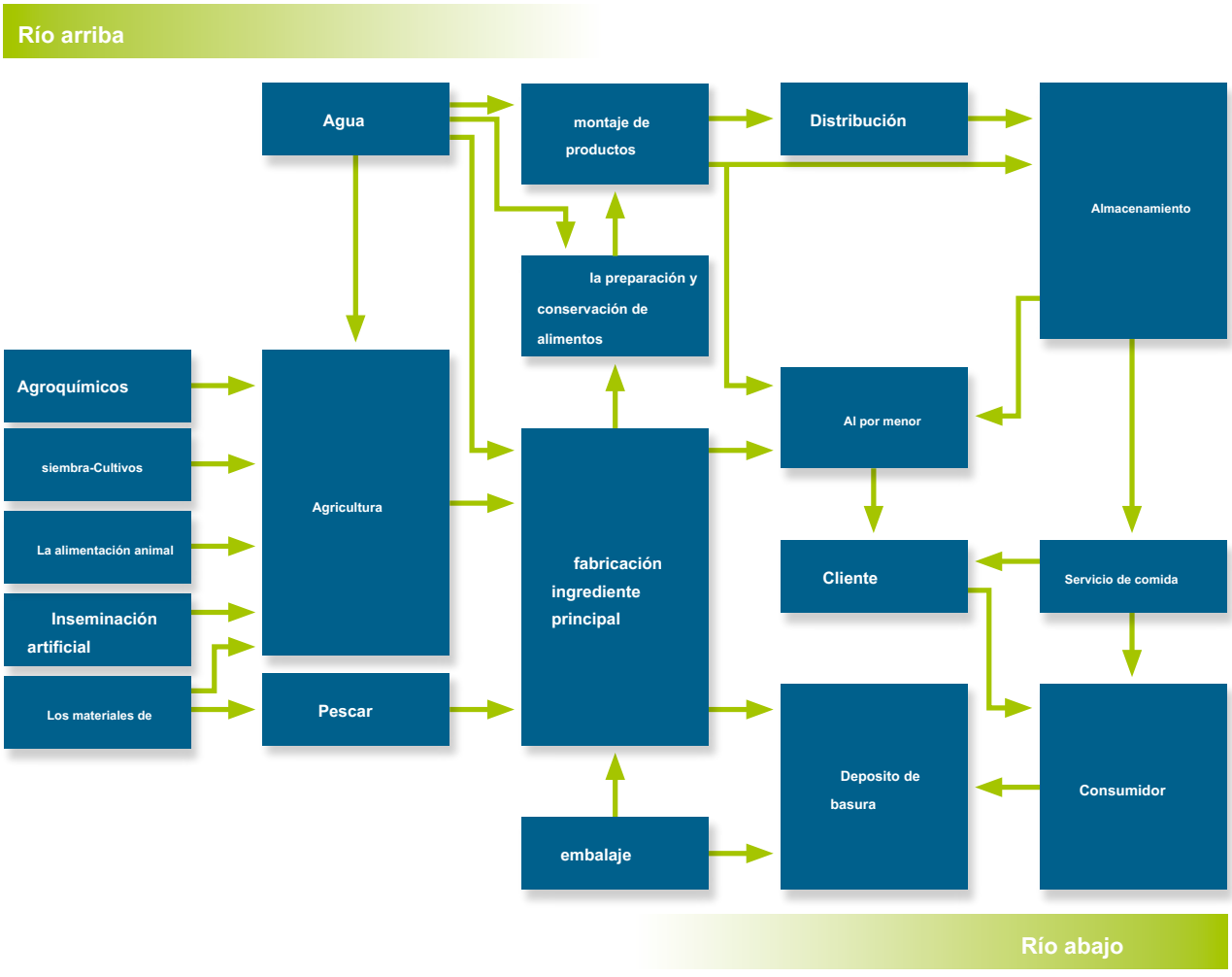
procedimientos adoptados para prevenir y detectar ataques fraudulentos en los alimentos

suministro 2,5 comida

elementos de lo que comúnmente se llama una cadena de suministro de alimentos

***NOTA** Un ejemplo de una cadena de suministro de alimentos se da en la Figura 1. Figura 1 no pretende ser exhaustiva.*

Figura 1 - cadena A de suministro de alimentos



2.6 peligros

algo que puede causar la pérdida o el daño que surge de un evento de origen natural o accidental o es resultado de la incompetencia o la ignorancia de las personas involucradas

2.7 Análisis de Peligros y Puntos Críticos de Control (HACCP)

sistema que permite identificar, evaluar y controlar peligros significativos para la inocuidad de alimentos

{FUENTE: Codex Alimentarius. *Principios Generales de Higiene de los Alimentos [*1]}

2.8 privilegiada

individuo dentro o asociado con una organización y con acceso a sus activos, pero que pueden hacer mal uso que el acceso y presentar una amenaza para sus operaciones

la seguridad del personal 2.9

procedimientos utilizados para confirmar la identidad de un individuo, calificaciones, experiencia y derecho al trabajo, a la conducta y monitor como un empleado o contratista

NOTA 1 *No debe confundirse con la 'seguridad personal'.*

NOTA 2 *principios de seguridad personal se utilizan para asegurar la fiabilidad de personal dentro de una organización, pero se pueden aplicar al personal de los proveedores dentro de los procesos de acreditación de vendedor.*

2.10 amenaza

algo que puede causar la pérdida o el daño que surge de la mala intención de la gente

NOTA *Amenaza no se utiliza en el sentido de la conducta que amenaza o promesa de consecuencia desagradable de un incumplimiento de una demanda malicioso.*

2.11 Evaluación de amenazas y Puntos Críticos de Control (TACCP)

la gestión sistemática de los riesgos a través de la evaluación de amenazas, identificación de vulnerabilidades y la aplicación de controles a los materiales y productos, compras, procesos, instalaciones, personas, redes de distribución y sistemas de negocios por un equipo de expertos y de confianza con la autoridad para implementar cambios en los procedimientos

3 Tipos de amenaza

3.1 Consideraciones generales

actos deliberados contra los alimentos y el suministro de alimentos toman varias formas. Cláusula *3* describe las características de las principales amenazas a la autenticidad y la seguridad de los alimentos

- adulteración por motivos económicos (EMA) y la contaminación malicioso, y explica la naturaleza de otras amenazas, en particular el rápido crecimiento de mal uso de técnicas digitales.

3,2 adulteración Económicamente motivado (EMA)

NOTA *Los detalles de muchos otros casos están disponibles en la base de datos de Fraude de Alimentos de la Convención de la Farmacopea de Estados Unidos en http://www.foodfraud.org/ [4].*

Caso 1

En 2016, los funcionarios de aduanas en Nigeria confiscaron 2,5 toneladas de arroz que se sospechaba estaba hecho de plástico. [3]

caso 2

El aceite de oliva ha sido un objetivo frecuente de la adulteración, a menudo por otros aceites vegetales. En 2017, las autoridades italianas interrumpieron un anillo de crimen organizado que se exportaba aceite de oliva falsa a los Estados Unidos. [4] Del mismo modo, las autoridades brasileñas informaron que un porcentaje muy elevado de los aceites de oliva analizadas no cumplían con los estándares de calidad requeridos por su etiquetado. [5]

caso 3

La policía española ha acusado a un fabricante hamburguesa de carne de cerdo y la soja utilizando picada para aumentar el contenido de carne percibido de sus productos durante muchos años. [6] No está claro si las hamburguesas de ternera en realidad contenían suficiente para adaptarse a cualquier regulación oficial.

caso 4

En 2014 el Dairy Board de Kenia afirmó que los vendedores ambulantes estaban poniendo en riesgo la vida mediante la adición de conservantes (formalina y peróxido de hidrógeno) en un (probablemente inútil) tratará de extender la vida útil de la leche. [7]

caso 5

El personal en un empacador de carne Europea consideró, erróneamente, que podrían evitar un producto que se está llevando condenado como la fiebre aftosa, cubriéndola con desinfectante.

La motivación de EMA es de carácter financiero, para ganar un aumento de los ingresos por la venta de un producto alimenticio de una manera que engaña a los clientes y consumidores. Esto puede ser por cualquiera de hacer pasar un material más barato como uno más caro (véase el caso 1), o puede ser que un ingrediente menos costoso se utiliza para reemplazar o extender el más caro (ver los casos 2 y 3).

La evitación de la pérdida también puede ser un incentivo para la adulteración (ver casos 4 y 5). suministro limitado de un material clave puede animar a un productor de improvisar para completar un pedido en vez de corto entrega declarar al cliente.

La intención de EMA no es para causar enfermedad o muerte, sino que puede ser el resultado. Este fue el caso en 2008, cuando la melamina se utilizó como una fuente de nitrógeno a fraudulentamente aumentar el contenido de proteína medido de la leche, lo que resulta en más de 50 000 bebés hospitalizados y seis muertes después de haber consumido la fórmula infantil contaminada. [8]

[3] Más información está disponible en: http://www.bbc.co.uk/ noticias / mundo-África-38391998 [5].

[4] Más información está disponible en: https: // www. oliveoiltimes.com/olive-oil-business/italy-arrests-33-accusedolive-oil-fraud/55364 [6].

[5] estudio adicional caso se puede encontrar: https: // www. oliveoiltimes.com/olive-oil-business/brazil-reveals-widespreadolive-oil-fraud/56395 [7].

[6] Más información está disponible en: https: // www. euroweeklynews.com/3.0.15/news/on-euro-weekly-news/spainnews-in-english/144405-police-uncover-major [8].

[7] Más información está disponible en: http: // www. standardmedia.co.ke/article/2000107380/naivasha-hawkersusing-formalin-to-preserve-milk [9].

[8] Para más detalles sobre este caso adulteración ver la OMS y la FAO publicación, aspectos toxicológicos de la melamina y ácido cianúrico http://www.who.int/foodsafety/publications/ melamina-cianúrico-ácido / en / [10].

El factor común en muchos casos de EMA es que el adulterante es ni un peligro para la seguridad de los alimentos, ni identificarse fácilmente, ya que esto sería contrario al objetivo del atacante. adulterantes comunes [9] incluir agua y azúcar; ingredientes que pueden utilizarse adecuadamente y declaran pero de uso abusivo fraude alimentario.

EMA es probable que sea más eficaz para un atacante, y por lo tanto presentar una amenaza mayor para un negocio de comida, aguas arriba en la cadena de suministro de alimentos (véase la figura 1) cerca de la producción de ingredientes primarios. Una adulteración éxito (desde el punto de vista del atacante) continúa sin ser detectado. EMA puede necesitar una información privilegiada, pero podría ser revelado por la verificación, por ejemplo, la auditoría financiera podría revelar:

- compras que son inexplicables por recetas, tales como colorantes Sudán, que no tienen lugar en la fabricación de especias; o
- diferencias entre las cantidades vendidas y las cantidades compradas, tales como carne picada y carne bovina vendido comprado, con la carne de caballo para compensar la diferencia.

3,3 contaminación malicioso

caso 6

En 2005, una de las principales panadería británica informó de que varios clientes habían encontrado fragmentos de vidrio y agujas de coser en el interior del envoltorio de los panes. [10]

caso 7

En 1984, la secta Rajneeshee en Oregon trató de afectar el resultado de una elección local por contaminación de los alimentos en diez diferentes barras de ensaladas, lo que resulta en 751 personas afectadas por intoxicación por salmonela. [11]

caso 8

En 2013, un proveedor importante refrescos se vio obligado a retirar producto de un mercado clave cuando se envió una botella que había tenido su contenido reemplazados con ácido mineral. Los atacantes incluyen una nota que indica que más se distribuirían al público si la compañía no cumplió con sus demandas.

caso 9

En 2007, una panadería encontró montones de cacahuetes en la fábrica. Se retiró del producto y cerrado por una semana larga y profunda limpia para re-establecer su condición de libre de tuerca.

La motivación para la contaminación malintencionada puede ser a causa localizado (véase el caso 6) o generalizada (véase el caso 7) enfermedad o muerte.

En el caso 7, el atacante no quería que la contaminación para ser detectados antes de que se consume, por lo tanto el contaminante tenía que ser una toxina efectiva con poco efecto sobre la palatabilidad de la comida.

La motivación en caso 8 era publicidad. La opinión pública habría estado en contra de los atacantes si el daño había sido causado a los miembros del público, pero el proveedor no podía correr ese riesgo.

Los materiales que podrían ser utilizados por un atacante para ganar publicidad, o para extorsionar dinero, se encuentran con más facilidad que las que se necesitan para causar daño generalizado. El caso de alergenos (véase el caso 9) muestra el daño, el impacto y costo que pueda ser causado a un negocio con poco riesgo para el atacante.

La contaminación cerca de punto de consumo o venta, como en el caso 7, (aguas abajo en la Figura 1) es más probable que causa daño a la salud de un ataque a los cultivos o ingredientes primarios.

3.4 La extorsión

caso 10

En 1990, un ex oficial de policía fue condenado por extorsión después de la contaminación de los alimentos para niños con el vidrio y exigiendo dinero por parte del fabricante multinacional. [12]

caso 11

En 2008, un hombre fue encarcelado en Gran Bretaña después de haber sido condenado por amenazar con bombardear un gran supermercado y contaminar sus productos. [13]

[9] Para más información sobre adulterantes ver la base de datos de la Farmacopea de los Estados Unidos Versión Convención fraude alimentario 2.0 en: http://www.foodfraud.org/#/food-fraud-databaseversion-20 [11].

[10] Para más detalles sobre este caso de contaminación intencionada ver el archivo Food Standards Agency en: http: // webarchive. nationalarchives.gov.uk/20120206100416/http://food.gov.uk/ noticias / Archivo de Noticias / 2006 / dic / Kingsmill [12].

[11] Para más información, véase la publicación American Medical Association, un brote en la comunidad grande de salmonelosis causada por la contaminación deliberada del restaurante Ensalada Bares [13].

[12] Para más detalles sobre este caso alimentos manipulación ver la publicación Q Food en: http://www.qfood.eu/2014/03/1989-glassin-baby-food/ [14].

[13] Para más detalles sobre este caso de extorsión ver el artículo de The Guardian en: http://www.theguardian.com/uk/2008/jan/28/ukcrime [15].

La motivación de extorsión por parte de un individuo o grupo es financiera, para obtener dinero de la organización víctima. Dicha actividad es atractivo para la mente criminal cuando el producto, como alimentos para bebés (ver caso 10), es sensible o cuando una empresa se ve tan rico (véase el caso

11).

Un pequeño número de muestras se puede utilizar para mostrar la empresa que el atacante tiene la capacidad y es suficiente para causar preocupación pública y el interés de los medios.

3.5 El espionaje

caso 12

Una consultora de negocios utiliza el robo de la propiedad intelectual de un producto de aperitivo innovadora ficticia como un ejemplo de espionaje comercial. 14)

caso 13

En julio de 2014, Reuters informó que una mujer fue acusado en los EE.UU., con el intento de robar patentado

la tecnología de semillas de Estados Unidos como parte de una conspiración para el contrabando de tipos de maíz especializado para su uso en China. 15)

La principal motivación de espionaje es para los competidores que buscan ventajas comerciales para el acceso de la propiedad intelectual. Pueden infiltrarse en el uso de información privilegiada para informar, o pueden atacar de forma remota a través de los sistemas de tecnología de la información. Por otra parte, las organizaciones pueden tratar de ejecutivos tiente para revelar información confidencial o utilizar la grabación encubierta para capturar este tipo de material, o pueden simplemente robar el material, tal como sugiere el caso 13.

3.6 La falsificación

caso 14

En 2013, los agentes del orden incautaron 9 000 botellas de vodka falso de Glen de una fábrica ilegal. dieciséis)

caso 15

En 2011, 340 botellas de una famosa marca australiana de vino fueron capturados, tras las quejas de mala calidad para el propietario, que no tenía ningún vínculo con Australia. 17)

La motivación para la falsificación es el beneficio económico, por el fraude de imitación fraudulenta bienes inferiores como las marcas establecidas y de buena reputación. Tanto el crimen organizado y de la pequeña empresa puede causar pérdidas financieras y daños a su reputación. El primero, por ejemplo, puede utilizar las tecnologías de impresión sofisticados para producir etiquetas de los productos que son indistinguibles de los auténticos. Este último puede robar paquetes auténticos o incluso contenedores de uso de recarga individuales para su reventa.

Los criminales organizados pueden tratar de imitar el contenido de los alimentos de cerca para la detección e investigación de retardo. delincuentes de poca monta pueden ser tentados por una 'ganancia rápida' y estar menos preocupados en la seguridad de los alimentos.

14) Para más información sobre este caso ficticio está disponible de Murray Associates en: https: // contraespionaje. worldsecuresystems.com/tscm-the-missing-business-schoolcourse.html [16].

15) Para obtener más información, visite: http://www.grainews.ca/daily/ chino-mujer-detenidos-en-trama-a-robo-us-maíz-tecnología [17].

dieciséis)) Para más información sobre este ejemplo de falsificación, véase: http://thecounterfeitreport.com/product/322/ [18].

17) Para más información sobre este caso de la falsificación ver http://www.news.com.au/finance/offshore-raids-turn-up-fakeaussie-jacobs-creek-wines/story-e6frfm1i-12260 [19].

3.7 La ciberdelincuencia

caso 16

En 2014, el fraude financiero Acción del Reino Unido aconseja gerentes de restaurantes que estar alerta ya que los estafadores están tratando de apuntar a sus clientes de una nueva estafa telefónica. Ellos restaurantes de teléfono que afirman que hay un problema con su sistema de pagos con tarjeta, a continuación, se dijo que el restaurante para redirigir el pago con tarjeta a un número de teléfono proporcionado por el estafador. [18]

tecnologías de la información y las comunicaciones modernas ofrecen nuevas oportunidades y rápido aumento de negligencia. En caso de que el defraudador 16 utiliza la ingeniería social para tratar de defraudar a los negocios y consumidores. Es común que el atacante para tratar de explotar la ignorancia individual de las tecnologías involucradas. El fraude en este caso es 'ciber-enabled', que es una estafa conocida hace más fácil por las comunicaciones electrónicas. En total, en Inglaterra y Gales para el año hasta septiembre de 2016, la Oficina Nacional de Estadísticas informó sobre 3,6 millones de fraudes y casi 2 millones de casos de abuso de la informática. [19]

caso 17

En 2016, los informes sugirieron que los delincuentes habían cortado Deliveroo cuentas para pedir comida en las tarjetas de las víctimas. [20]

caso 18

En 2015, con sede en Michigan Biggby café reportó una violación de base de datos con el posible robo de información de los clientes derivados de las aplicaciones de tarjetas de fidelidad. [21]

El fraude en ambos casos 17 y 18 podría llevarse a cabo de forma remota a través de Internet con pocas posibilidades de detección y la justicia para el autor.

caso 19

En 2016 el Departamento de Agricultura de Estados Unidos FBI y alertó a los agricultores a su creciente vulnerabilidad a ataques cibernéticos a través de su uso de la tecnología de agricultura de precisión. [22]

Tal ataque podría ser el espionaje industrial cibernético habilitado, o la piratería - el acceso no autorizado a sistemas informáticos, tal vez con intención maliciosa.

caso 20

En 2016 un gran supermercado descubrió que las escalas en sus autoservicio registro de salida habían sido corrompidos para permitir denegación de servicio distribuido (DDoS) ataques en los sitios web públicos.

DDoS puede ser una verdadera molestia para las empresas, y dar lugar a pérdidas reales cuando el sitio de la compañía es una plataforma de comercio importante. El 'Internet de las cosas' (IO) se vuelve más y más importante; Informe sobre las amenazas conjunta NCSC / NCA [23] expone la vulnerabilidad de los dispositivos conectados a Internet (aparentemente inocuos) y su mal uso por parte de delincuentes.

El robo de identidad es quizás más familiar para el público, pero las organizaciones puede ser consciente de que su identidad sea robada para permitir fraude en las adquisiciones, en el que los bienes están ordenados en su nombre, pero desvían a los locales defraudadores que salen del proveedor engañados y supone comprador para llevar el costo y el litigio.

[18] Para más información sobre este restaurante fraude https://www.financialfraudaction.org.uk/news/2014/08/13/ ver la estafa de alerta-restaurantes-and-comensales orientada-en-nueva-estafa / [20].

[19] ONS Conjunto de datos: El crimen en Inglaterra y Gales: tablas experimentales: Tabla E1: El fraude y el mal uso del ordenador por la pérdida (de dinero o bienes) - número y la tasa de incidentes y el número y porcentaje de víctimas de https://www.ons.gov. UK / peoplepopulationandcommunity / crimeandjustice / conjuntos de datos / crimeinenglandandwalesexperimentaltables [21].

[20] Para más información, véase: https: // negocio-reportero. co.uk/2016/11/23/cyber-criminals-use-hacked-deliverooaccounts-order-food-victims-cards/ [22].

[21] Para más información, véase: http: //www.canadianbusiness. com / negocio-noticias / Michigan-basada en Biggby-café-reportsdatabase-brecha-posible-robo-de-cliente la información [23].

[22] La industria privada Notificación PIN 160331-001 Smart Farming Puede aumentar cibernético Orientación Sector Agricultura y Alimentos de EE.UU. contra https://info.publicintelligence.net/FBISmartFarmHacking.pdf ver [24].

[23] La amenaza cibernética a Reino Unido Empresas en https://www.ncsc.gov. uk / noticias / NCSC-y-NCA-amenaza-informe-provee de profundidad analysisevolving-amenaza [25].

4 Comprender el atacante

4.1 Generalidades

El éxito de un ataque deliberado a la comida o el suministro de alimentos depende de varias cosas:

un) ¿El atacante tiene la motivación y la unidad para superar los bloques obvias y menos obvias a sus acciones? Si los bloques parecen masiva y parece poco probable éxito, muchos posibles atacantes buscarían un blanco más fácil.

si) ¿El atacante tiene la capacidad para llevar a cabo el ataque? Un grupo es más probable encontrar los recursos y aprender las habilidades necesarias.

C) ¿El atacante tiene la oportunidad de llevar a cabo ¿el ataque? Un ataque físico necesita acceso físico al objetivo, sino un ataque cibernético que sólo necesite acceso a una computadora.

re) Sería el atacante ser disuadido por la posibilidad de detección y / o las sanciones potenciales?

4.2 El extortionist

El extorsionista quiere obtener beneficios financieros de un ataque, pero no quiere ser atrapado, y se concentra en evitar la detección. Su objetivo es más probable que sea un negocio de alto perfil con mucho que perder de publicidad negativa. Pueden trabajar solos y ser ingeniosos, reservado e interesada. Los ataques cibernéticos en todo el mundo a través de 'ransomware' han demostrado tanto la facilidad con extorsionadores ahora pueden atacar a múltiples víctimas y lo difícil que es para llevarlos ante la justicia. [24] Algunos individuos pueden afirmar que son capaces de tomar medidas contra un negocio, mientras que carecen de la capacidad para llevarlo a cabo; la empresa puede juzgar la reclamación como no es creíble, pero todavía decidir responder de manera apropiada.

4.3 El oportunista

El oportunista puede mantener una posición influyente dentro de una operación para ser capaz de evadir los controles internos. Pueden tener algunos conocimientos técnicos, pero su principal activo es el acceso. Es probable que se desanime por la posibilidad de detección, por lo que las visitas no anunciadas por clientes o auditores, o ad hoc muestreo para el análisis puede disuadir a sus acciones.

Un proveedor que no pueden correr el riesgo de falta de entrega a un cliente puede correr el riesgo de que no se detectó la adulteración de vez en cuando. El éxito en una ocasión puede que sea más fácil para intentar una repetición. Este oportunista puede convencerse de que la adulteración es legítimo, por ejemplo, el pollo en una salchicha de cerdo seguiría siendo carne.

4.4 El extremista

El extremista lleva su causa o campaña tan en serio que distorsionan su contexto y pasar por alto cuestiones más amplias. La dedicación a su causa puede no tener límites y su determinación para el progreso que puede ser grande.

Extremistas lo desea, puede causar daño y son propensos a disfrutar de la publicidad después del evento. Puede que no importa, y puede ser una ventaja, si ellos mismos se vean perjudicados. El riesgo de fracaso es un impedimento, pero el riesgo de captura después de que el evento no es. Por lo general son ingeniosos e innovadores en la elaboración de formas de atacar.

Algunos grupos temáticos individuales pueden querer interrumpir las operaciones de negocio y reputación, sino que temer un daño masivo para el público podría dañar su causa y conducirlos a perder apoyo.

4.5 El individuo irracional

Algunas personas no tienen ningún motivo racional para sus acciones. Sus prioridades y preocupaciones se han distorsionado por lo que son incapaces de tener una visión equilibrada del mundo. Algunos pueden haber diagnosticado clínicamente problemas de salud mental.

Este individuo puede ser disuadido fácilmente mediante sencillos pasos que les impiden acceder a su objetivo o hacer la detección fácil.

[24] Para más información ver la amenaza cibernética a Reino Unido Empresas, PG 7 disponibles en: https://www.ncsc.gov.uk/news/NCSC-y-NCA-amenaza-informe-proporciona profundidad-análisis-evolvingthreat [25] .

4.6 El individuo contrariedad

El individuo contrariedad cree que una organización ha sido injusto con ellos y busca venganza. Por ejemplo, pueden ser un empleado agraviado o ex empleado, proveedor o cliente. Pueden tener un conocimiento experto de la operación y el acceso a la misma.

Este atacante es probable que sea un individuo y no como parte de un grupo. Si una información privilegiada, que podrían ser peligrosos, pero son más propensos a querer causar vergüenza y pérdida financiera que daño al público. Si no es una información privilegiada, este individuo tiene más probabilidades de reclamación o presumir de haber hecho algo que realmente ser capaz de hacerlo.

4.7 Los delincuentes cibernéticos y otros agentes maliciosos digitales

Ciber criminales pretenden subvertir los controles sobre los sistemas de información y de las comunicaciones informatizadas con el fin de evitar que trabajar con eficacia, a robar o dañar los datos que contienen, y / o para interrumpir negocio en Internet. Su motivación puede ser criminal o incluso política, pero también puede ser de demostrar su experiencia y capacidad para vencer a cualquier sistema de protección diseñado para detenerlos.

Tradicionalmente, este tipo de atacante tiene información y experiencia en tecnología de comunicaciones que pueden causar daño comercial. Sin embargo, como se advirtió en el Reino Unido Conjunto NCSC / NCA informe sobre las amenazas [25], "Las líneas entre esos ataques que cometen siguen a desdibujarse, con grupos delictivos imitando estados ..... y actores más avanzados utilizando con éxito 'fuera de la plataforma' software malicioso a los ataques de lanzamiento ". [25] Esto puede suponer una amenaza creciente para la seguridad alimentaria a medida que aumenta la actividad de Internet.

4.8 El profesional del crimen

El crimen organizado se puede ver el fraude alimentario como un delito relativamente simple, con grandes ganancias en perspectiva, pocas posibilidades de aprehensión, y sanciones modestas si es condenado. El comercio mundial de alimentos en los que se mueven los materiales de alimentos, a menudo con poca antelación, a través de las fronteras de la zona de aplicación parece alentar el criminal profesional. El anonimato de Internet y la posibilidad de intrusión a distancia hace que los sistemas electrónicos en el delito cibernético cada vez más atractivo para los criminales profesionales.

Pueden ser disuadidos por una estrecha colaboración entre las operaciones de alimentos y autoridades nacionales e internacionales de policía.

[25] NCSC y NCA La cibernética amenaza a Reino Unido Empresas disponible en: https://www.ncsc.gov.uk/news/ncsc-and-nca-threatreport-provides-depth-analysis-evolving-threat [25].

5 Evaluación de amenazas y Puntos Críticos de Control (TACCP)

5.1 temas generales

TACCP debe ser utilizado por las empresas alimentarias como parte de sus procesos más amplios de gestión de riesgos, o como una forma de comenzar a evaluar los riesgos de forma sistemática.

TACCP objetivos de:

- reducir la probabilidad (probabilidad) de un ataque deliberado;
- reducir las consecuencias (impacto) de un ataque;
- proteger la reputación de la organización;
- clientes, prensa y tranquilizar a la opinión pública que son medidas proporcionadas en el lugar para proteger los alimentos;
- satisfacer las expectativas internacionales y apoyar el trabajo de los socios comerciales; y
- demuestran que se toman las precauciones razonables y la debida diligencia se ejerce en la protección de los alimentos.

por, en términos generales:

- identificar las amenazas específicas a los negocios de la empresa;
- evaluar la probabilidad de un ataque al considerar la motivación del atacante prospectivo, la vulnerabilidad del proceso, la oportunidad y la capacidad que tienen de llevar a cabo el ataque y la certeza de la información en la que se basa la evaluación;
- evaluar el impacto potencial teniendo en cuenta las consecuencias de un ataque con éxito;
- juzgar la prioridad que debe darse a diferentes amenazas mediante la comparación de su probabilidad e impacto;
- priorización de las amenazas basadas en el riesgo, y comunicar una priorización tales través de los socios comerciales para la aceptación de riesgo compartido;
- decidir sobre los controles necesarios y proporcionados para desalentar el atacante y dar notificación temprana de un ataque; y
- el mantenimiento de los sistemas de información y de inteligencia para permitir la revisión de las prioridades.

profesionales del sector de alimentos desea reducir al mínimo las posibilidades de pérdida de la vida, la mala salud, pérdidas financieras y daños a la reputación comercial que podría causar un ataque.

TACCP no puede dejar de individuos u organizaciones que afirman que han contaminado los alimentos, pero puede ayudar a juzgar si esa afirmación es probable que sea cierto. Dicha reclamación, si se juzga sea creíble, y cualquier incidente real debe ser tratada como una crisis. La organización tiene que tomar medidas para mantener las operaciones en funcionamiento e informar a los involucrados.

proceso 5.2 TACCP

En la mayoría de los casos TACCP debe ser una actividad de equipo, ya que es la mejor manera de llevar habilidades, especialmente las habilidades de gestión de personas, juntos. Para muchas pequeñas empresas el trabajo en equipo no es factible y que puede ser el trabajo de una persona. El equipo TACCP puede y debe modificar el proceso TACCP para mejor satisfacer sus necesidades y adaptarlo a otras amenazas como sea necesario para hacer frente a cuatro preguntas subrayado:

un) Que quieran atacarnos?

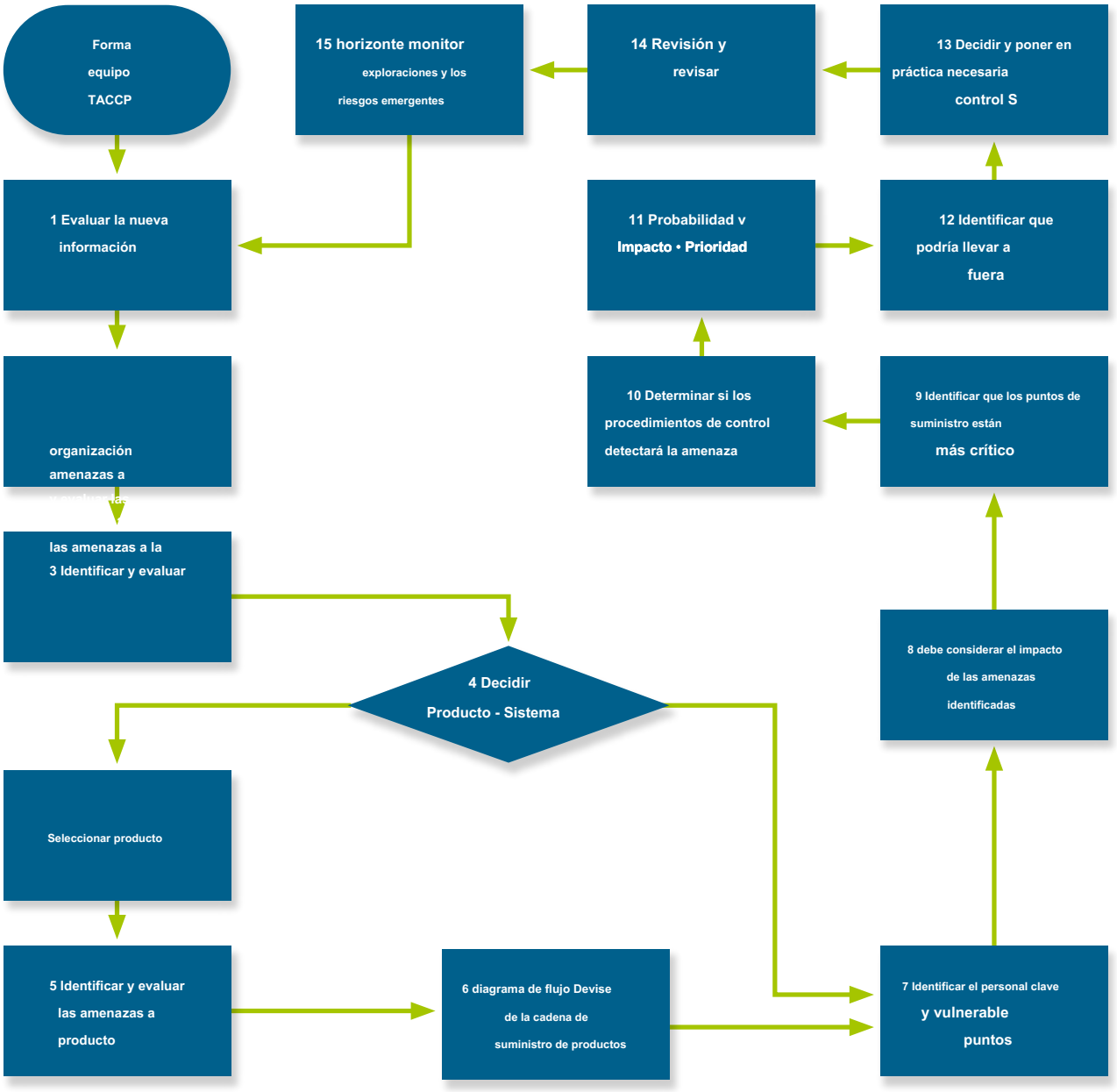
si) ¿Cómo podrían hacerlo?

C) ¿Dónde estamos vulnerables?

re) ¿Cómo podemos detenerlos?

El diagrama de flujo (véase la Figura 2) se describe el proceso TACCP y se centra en la adulteración deliberada y contaminación. Para más información sobre cada elemento del proceso TACCP expuesta en la Figura 2 se da en **la lista numerada correspondiente [véase 5.2, 1) - 5.2, 15)].**

Figura 2 - Esquema proceso TACCP



NOTA 1 *Un enfoque alternativo es el riesgo CARVER + choque que se describe en el Anexo C.*

NOTA 2 *La figura 2 está destinado a ser una ilustración únicamente indicativo.*

Un equipo TACCP de pie debe estar formado, lo que podría incluir a las personas con la siguiente experiencia:

- seguridad;
- recursos humanos;
- tecnología de los Alimentos;
- Ingeniería de Procesos;
- la producción y las operaciones;
- compras y adquisiciones;
- distribución y logística;
- tecnologías de la información;
- comunicaciones; y
- comercial / marketing.

NOTA 1 *El equipo puede incluir representantes de proveedores y clientes clave.*

NOTA 2 *Para una organización pequeña puede tener una persona para cubrir todas estas funciones.*

NOTA 3 *Mientras que el equipo de HACCP puede proporcionar un punto de partida adecuado, el equipo de la continuidad del negocio podría ser un mejor modelo. El equipo TACCP es típicamente un grupo establecido y permanente capaz de revisar continuamente sus decisiones.*

Dado que el proceso puede cubrir TACCP material sensible y podría ser de utilidad para un atacante potencial, todos los miembros del equipo no sólo deben tener conocimiento de los procesos reales, sino también confiable, discreta y consciente de las implicaciones del proceso.

El equipo TACCP debe:

1) evaluar toda la información nueva que ha llegado a su atención;

2) identificar a los individuos y / o grupos que pueden ser una amenaza para la organización y sus sistemas, especialmente los sistemas electrónicos, y evaluar su motivación, capacidad y determinación;

3) identificar a los individuos y / o grupos que pueden ser una amenaza para la operación específica (por ejemplo, locales, fábrica, sitio);

4) amenazas de productos de diferenciar de otras amenazas:

un) en busca de amenazas no son del producto, vaya a la Cláusula **11;**

si) en busca de amenazas de productos, seleccione un producto que es representante de un proceso particular;

NOTA 4 *Por ejemplo, un producto adecuado sería típico de una línea de producción particular y podría ser uno que es más vulnerable.*

5) identificar a los individuos y / o grupos que pueden querer orientar el producto específico;

6) dibujar un diagrama de flujo de proceso para el producto de pero no limitado por, 'la granja al tenedor', incluyendo, por ejemplo, la preparación doméstica. El diagrama de flujo entero debe ser visible a la vez. Particular atención se debe prestar a partes menos transparentes de la cadena de suministro que podría merecer un gráfico subsidiaria;

7) identificar tanto los puntos vulnerables donde un atacante podría esperanza de éxito y las personas que tendrían acceso a un examen de cada paso del proceso;

8) identificar posibles apropiado amenazas para el producto en cada etapa y evaluar el impacto que el proceso puede tener en la mitigación de las amenazas;

NOTA 5 *adulterantes modelo incluyen bajo costo ingredientes alternativos a componentes de alta calidad; contaminantes modelo podría incluir agentes altamente tóxicos, productos químicos industriales tóxicos, materiales nocivos fácilmente disponibles y sustancias inapropiadas como alergenos o étnicamente productos alimenticios insanos.*

NOTA 6 *Por ejemplo, la limpieza puede eliminar el contaminante, el tratamiento térmico puede destruirlo, y otros componentes de los alimentos puede neutralizarla.*

9) seleccionar los puntos del proceso donde la amenaza tendría el mayor efecto, y en los que mejor podrían ser detectados;

10) evaluar la probabilidad de procedimientos de control de rutina detectar tal una amenaza;

NOTA 7 *Por ejemplo, el análisis de rutina de laboratorio podría detectar agua añadida o grasas y aceites inusuales; gestión eficaz de la compra sería desafiar las órdenes de compra inusuales.*

11) anotar la probabilidad de la ocurrencia de amenazas, la puntuación el impacto que tendría, y trazar los resultados para mostrar la prioridad que debe darse (véase **6.3),** y revisar si esta evaluación de riesgos parece mal;

NOTA 8 *Se puede necesitar un poco de pensamiento lateral. El equipo TACCP podría preguntar, "Si estábamos tratando de socavar nuestro negocio, lo que sería la mejor manera?" Se puede considerar cómo un atacante selecciona atacan materiales:*

- ava ilability;
- costo;
- toxicidad;
- forma física; y / o
- seguridad en el uso, por ejemplo pesticidas en las granjas y agredir he materiales de sabor en las fábricas pueden ser contaminantes convenientes.

12) donde la prioridad es alta, identificar quién tiene acceso no supervisado al producto o proceso y si son dignos de confianza, y si esa confianza puede ser justificado;

13) identificar, registrar de forma confidencial, de acuerdo y poner en práctica medidas preventivas proporcional (controles críticos). El equipo TACCP debe tener un reporte confidencial y procedimiento de grabación que permite una acción de gestión de decisiones, pero no expone los puntos débiles a los que no tienen necesidad de conocer (ver estudios de caso en el anexo A);

14) determinar los mecanismos de revisión y revisará la la evaluación TACCP; y

NOTA 9 *Revisión de la evaluación TACCP debería tener lugar después de cualquier alerta o al año, y en los puntos donde surgen nuevas amenazas o cuando hay cambios en las buenas prácticas.*

15) mantener una vigilancia rutinaria de oficial y la industria publicaciones que dan una advertencia temprana de los cambios que pueden convertirse en nuevas amenazas o cambiar la prioridad de las amenazas existentes, incluidas las cuestiones más locales a medida que desarrollan.

NOTA 10 *Un esbozo de algunos sistemas de información y de inteligencia se da en el Anexo B.*

Evaluación 6

***NOTA** Las siguientes listas no pretenden ser exhaustivas de todas las preguntas que se le puede pedir para evaluar una amenaza.*

6.1 Evaluación de amenazas

El producto, las instalaciones y la organización y sus sistemas de información puede ser objetivo de un ataque de una serie de grupos e individuos (véase el numeral **4),**
y cada elemento debe evaluarse por separado. El equipo debe considerar TACCP proveedores bajo tensión financiera, empleados y ex empleados alienados, grupos monotemáticos, competidores comerciales, organizaciones de medios de comunicación, organizaciones terroristas, criminales y grupos de presión locales.

Comúnmente, una cadena de suministro corta que implica un menor número de personas puede ser menos riesgoso que una cadena de suministro más tiempo.

El equipo TACCP podría hacer las siguientes preguntas para evaluar una amenaza: Para el producto:

- ¿Ha habido significativos aumentos de los costos que han afectado a este producto?
- ¿Este producto tiene particular importancia religiosa, ética o moral para algunas personas?
- Este producto podría ser utilizado como un ingrediente en una amplia gama de alimentos populares?
- ¿El producto contiene ingredientes o de otro material de origen del extranjero?
- Se están convirtiendo en los principales materiales menos disponibles (por ejemplo, de la pérdida de cosechas) o alternativas abundante (por ejemplo, de la sobreproducción)?
- ¿Ha habido aumentos inesperados o disminuciones en la demanda?
- Son materiales de bajo coste sustitutos disponibles?
- Ha aumentado la presión sobre los márgenes comerciales de los proveedores?

Para las instalaciones:

- Son los locales ubicados en una zona sensible política o socialmente?
- Hacer el acceso a los locales de acciones o servicios clave con los vecinos controvertidos?
- Son nuevos reclutas, especialmente agencia y personal de temporada, seleccionados de manera apropiada?
- Son los servicios a los locales protegidos de manera adecuada?
- Se utilidades externas adecuadamente protegidos?
- Son materiales peligrosos, que podrían ser valiosos para grupos hostiles, almacenados en el sitio?
- Un gran número de personas (incluyendo el público en general) utilizando la ubicación?
- ¿Alguno de los empleados tienen motivos para sentirse descontentos signos o mostrar la insatisfacción?
- Son mecanismos de auditoría interna independiente?
- Tienen un papel clave sido ocupadas por el personal durante muchos años con poca supervisión?

Para la organización:

- ¿Estamos bajo la propiedad extranjera de las naciones implicadas en el conflicto internacional?
- ¿Tenemos una celebridad de alto perfil o el director ejecutivo o propietario?
- ¿Tenemos una reputación de tener vínculos significativos, clientes, proveedores, etc., con regiones inestables del mundo?
- Nuestras marcas son objeto de controversia por algunos?
- Es lo que nuestros clientes o suministrar a los clientes de alto perfil o eventos?
- Es la organización que participan en el comercio de controversia?
- Han competidores comerciales sido acusados de espionaje o sabotaje?

En los sistemas de información:

- ¿Tiene medios de comunicación social Chatter sugieren que podríamos ser el blanco de la intrusión digital?
- Son nuestros sistemas de control de supervisión y adquisición de datos (SCADA) y otra de control también utilizados por otras organizaciones que podrían ser los principales objetivos?

El examen de las respuestas a estas preguntas puede dar una comprensión de los efectos de un ataque exitoso y la probabilidad de que tenga lugar. Esto informa requiere un juicio sobre el nivel proporcional de protección.

6.2 Identificación de vulnerabilidades

***NOTA** En esta sección EMA, la contaminación intencionada y ataque cibernético se utilizan como ejemplos de enfoques para la evaluación de la vulnerabilidad.*

6.2.1 Generalidades

Las distintas organizaciones tienen diferentes necesidades de negocio y operan en diferentes contextos. El equipo TACCP puede juzgar cuál es el enfoque y las preguntas son apropiadas y proporcionadas a las amenazas que identifican.

6.2.2 adulteración Económicamente motivado (EMA)

Una característica típica de EMA (ver 3.2) es la sustitución de un elemento de bajo coste en lugar de un relativamente alto componente de costo / ingrediente. El equipo TACCP necesita estar alerta a la disponibilidad de tales alternativas. Un ejemplo en el que esto puede ocurrir es cuando se afirma valor añadido,

por ejemplo, orgánico, no-GM, cultivado localmente, gama libre o con denominación de origen protegida. El atacante puede tener acceso inmediato a bajar equivalentes de valor, que son casi indistinguibles.

***NOTA** Más orientación sobre fuentes de información e inteligencia sobre la probabilidad de fraude alimentario se proporciona en el Anexo B.*

El equipo TACCP tiene que estar seguro de que sus propias operaciones y las de sus proveedores están en manos de confianza. Esto se puede lograr mediante el asesoramiento oficial sobre la seguridad personal. de 26)

Las preguntas que el equipo TACCP podría hacer incluyen:

- ¿Usted confía en gerentes y sus proveedores de sus proveedores gerentes?
- Hacen los principales proveedores utilizan prácticas de seguridad personal?
- ¿Los proveedores piensan que hacemos un seguimiento de su funcionamiento y analizar sus productos?
- Que los proveedores no son auditados de forma rutinaria?
- ¿Estamos suministrada a través de control remoto, cadenas oscuros?
- ¿De qué manera los proveedores disponen de cantidades excesivas de materiales de desecho?
- ¿Somos conscientes de accesos directos para el proceso que nos podría afectar?
- Son nuestro personal y los de los proveedores animó a las preocupaciones de informes (whistleblowing)?
- Son registros de acreditación, los certificados de conformidad y análisis de informes independientes?

6.2.3 contaminación malicioso

Las preguntas que el equipo TACCP podría pedir tanto de sus propias operaciones y la de sus proveedores incluyen:

- Se realizan auditorías de seguridad alimentaria rigurosa y actualizada?
- Son los procedimientos de seguridad personal en el uso?
- ¿El acceso al producto restringido a aquellos con una necesidad de negocio?
- No tienen recipientes de almacenamiento sellos-Sello de Seguridad?
- ¿Hay oportunidades para el acceso por parte de simpatizantes de los grupos individuales de emisión?
- ¿Alguno de los empleados tienen un resentimiento contra la organización?
- El aburrimiento es el personal, la disciplina, el reclutamiento es un problema?

6.2.4 ataques cibernéticos

Las preguntas que el equipo TACCP puede hacer incluyen:

- Tiene la Junta aprobó el NCSC de *10 pasos a la seguridad cibernética [*27] y se establecieron procedimientos adecuados? (Ver Anexo D)
- Son todos TI / SI proyectos objeto de una evaluación del riesgo de intrusión electrónica?
- Se colegas propensos a tener en cuenta y que informen de comunicaciones electrónicas sospechosas (por ejemplo, correos electrónicos, SMS)?
- Es un material altamente sensible a cabo el separada, soportar los sistemas informáticos por sí solos?
- Se utilizan contraseñas de forma segura, y de acuerdo con la orientación NCSC? 27)
- Son las condiciones relacionadas con el manejo de las cuentas electrónicas cuando un miembro del personal se une, movimientos u hojas de empleo eficaz?
- Son cualquier localidad enlaces Wi-Fi sin cifrar o accesibles por los usuarios externos?
- Son de fabricación u otros sistemas operativos interconectados con los sistemas de tecnología de la información?
- Están habilitados para Internet procesos seguros? Por ejemplo, podría procesar parámetros pueden cambiar sin la debida autorización? Basada en la nube podría estar dañados los registros?
- Son los procedimientos de copia de seguridad de datos efectiva?
- Están operadores notificados y consciente de los cambios en la producción o de otra configuración de funcionamiento, por ejemplo, a formulaciones de productos?
- Se puede acceder de forma remota los sistemas de producción?
- Son sistemas de operaciones esenciales separados de la red corporativa de la compañía y de la Internet?
- Es de origen externo de datos (desde el correo electrónico, Internet o medios extraíbles) verificado en busca de malware antes de ser importados?
- ¿Tiene acceso remoto a los sistemas de la empresa requiere autenticación de múltiples factores y es el grado de acceso limitado?
- ¿Los sistemas computarizados esenciales han probado, copias de seguridad fuera de línea?
- Son la continuidad del negocio y recuperación de desastres para los planes de TI y sistemas de producción en su lugar y efectiva?

de 26) Para más información sobre la seguridad personal se puede encontrar en la página web del IREC en http://www.cpni.gov.uk/advice/Personnelsecurity1/ [26].

27) NCSC guía está disponible en: https://www.ncsc.gov.uk/ orientación / contraseña-guía-simplificando-su-enfoque [28].

6.3 Evaluación del riesgo

Las organizaciones necesitan entender las amenazas que enfrentan, sino que debe centrarse la atención en los más prioritarios. Para cada amenaza identificada equipo TACCP considera y da una puntuación de la probabilidad de cada suceso amenaza y por su impacto (ver Tabla 1).

tabla 1 - La evaluación de riesgos de puntuación

Probabilidad de que ocurra una amenaza	Puntuación	Impacto
Muy alta probabilidad	5	Catastrófico
Tienen muchas posibilidades	4	Mayor
algunos oportunidad	3	Significativo
Puede pasar	2	Algunos
Poco probable que suceda	1	Menor

NOTA 1 *Se trata de una matriz de puntuación ejemplo, las organizaciones pueden elegir su propio esquema de clasificación.*

NOTA 2 *Probabilidad de un suceso amenaza podría ser juzgada, por ejemplo, durante un período de 5 años.*

NOTA 3 *Impacto podría considerar la muerte o lesiones, costo, daño a la reputación y / o pública y las percepciones de los medios de estas consecuencias.*

La probabilidad de un suceso amenaza puede ser evaluado teniendo en cuenta:

- si un atacante podría lograr sus objetivos si tiene éxito;
- si un atacante podría tener acceso al producto o proceso;
- si un atacante sería disuadido por las medidas de protección;
- si un atacante preferiría otros objetivos; y
- si un ataque se detecta antes de que tuviera ningún impacto.

El impacto podría ser evaluado en términos financieros como en términos de la antigüedad del personal necesario para tratar con él.

La puntuación de riesgo presentado por cada amenaza se puede mostrar en un gráfico simple. Una matriz de puntuación de riesgo ejemplo se presenta en la Figura 3.

informes 6.4 TACCP

Cuatro estudios de casos ficticios que muestran cómo el proceso TACCP puede ser aplicado y adaptado para satisfacer mejor las necesidades de una empresa individual se dan en el Anexo A. Se presentan como los registros formales de la investigación TACCP y pueden ser utilizados para demostrar que el negocio ha tomado todas las medidas razonables precauciones que deben ser víctimas de un ataque.

figura 3 - matriz de puntuación de riesgo

Impacto	5				Una amenaza	
	4		amenaza C			
	3					amenaza B
	2	amenaza E				
	1			amenaza D		
		1	2	3	4	5
	Probabilidad					

Riesgo muy alto	Una amenaza
Alto riesgo	amenaza B
Riesgo moderado	amenaza C
Riesgo bajo	amenaza D
riesgo insignificante	amenaza E

NOTA *Esta es una matriz de puntuación de riesgo ejemplo, las organizaciones pueden elegir diferentes criterios para las diferentes categorías de riesgo.*

7 controles críticos

NOTA *Tablas 2, 3 y 4 no están destinados a ser exhaustiva de todos los controles que pueden ser considerados relevantes o proporcionada para reducir un riesgo.*

7.1 Control de Acceso

Si un atacante potencial no tiene acceso a su objetivo, luego de que el ataque no puede tener lugar. No es posible o deseable para evitar cualquier acceso, pero las medidas físicas puede limitar el acceso a ciertos individuos y los que tienen una necesidad legítima. Algunos enfoques para la reducción del riesgo de que el equipo TACCP puede sentir son proporcionadas y relevante para su negocio se enumeran en la Tabla 2.

Tabla 2 - Enfoques para la reducción del riesgo

Acceso a los locales		**¿Pertinente? ¿Proporcionado?**
1	El acceso a las personas en viaje de negocios solamente	
2	Vehículo perímetro de aparcamiento en el exterior	
3	Locales dividen en zonas para restringir el acceso a las personas con una necesidad de negocio	
4	cerco perimetral visible e integral	
5	sistema de alarma perimétrica	
6	monitoreo CCTV / grabación de las vulnerabilidades del perímetro	
El acceso a los vehículos		**¿Pertinente? ¿Proporcionado?**
7 puntos de acceso monitoreados		
8	vías de acceso trafficcalmed	
9	entregas programadas	
10 documentación comprueba	antes de su ingreso	
11 entregas perdidas investigados		
El acceso a las personas		**¿Pertinente? ¿Proporcionado?**
12 control de acceso Chip y PIN		
13 Los vestuarios, separada	ropa personal de ropa de trabajo	
El acceso a los sistemas electrónicos		**¿Pertinente? ¿Proporcionado?**
14 El control de rutina y	aplicación de las directrices NCSC [28]	
15 Pruebas de penetración por	profesionales externos	
dieciséis entrenamiento de rutina en cibernética	principios de seguridad (por ejemplo cibernético esenciales [29] o BS ISO 27000 series)	
La detección de los visitantes		**¿Pertinente? ¿Proporcionado?**
17 Solo por cita		
18 Prueba de identidad requiere		
19 acompañado a lo largo		
20 La identificación positiva del personal	y visitantes	
21 monitoreo CCTV / grabación	de las zonas sensibles	
Otros aspectos		**¿Pertinente? ¿Proporcionado?**
22 manejo seguro del correo		
23 Restricciones sobre portátil	equipos electrónicos y la cámara	
24 Limitaciones en el acceso a	los servicios de red	

7.2 Detección de manipulación

almacenamiento mucho materia prima, algunos de almacenamiento del producto, la mayoría de los vehículos de distribución y todos los alimentos envasados pueden ser de manipulación evidente. En caso de que un atacante obtener acceso, una prueba de manipulación da una posibilidad de que el ataque puede ser detectada a tiempo para evitar el impacto.

Algunas aproximaciones a los aspectos de evidencia de manipulación que el equipo TACCP puede sentir son proporcionadas y relevante para su negocio se enumeran en la Tabla 3.

Tabla 3 - Alterar evidencia

La detección de manipulación		¿Pertinente? ¿Proporcionado?
1	sellos numerados en silos de almacenamiento a granel	
2	sellos numerados en tiendas de etiquetas y paquetes etiquetados	
3	sellos eficaces en los paquetes de venta al por menor	
4	sellos numerados en materiales peligrosos	
5	Cerrar el control de existencias de materiales clave	
6	Grabación de números de precinto en los vehículos de reparto	
7	nombres de usuario y contraseñas seguras para el acceso electrónico	
8	La comunicación de acceso no autorizado de los sistemas cibernéticos	

7.3 garantizar la seguridad del personal

orientación al personal de seguridad se utiliza para mitigar las amenazas internas a la organización. Sus principios también pueden ser utilizados por las empresas alimentarias para juzgar si el personal clave dentro de las organizaciones que suministran bienes y servicios se puede confiar para cumplir con las especificaciones y procedimientos, y para el trabajo en el mejor interés de ambos el proveedor y el cliente. Algunos enfoques para garantizar la seguridad del personal que el equipo TACCP puede sentir son proporcionadas y relevante para su negocio se enumeran en la Tabla 4.

***NOTA** Otras orientaciones sobre la seguridad personal y la población se encuentra disponible en: http://www.cpni.gov.uk/ consejos / Personal-seguridad1 / [26]. En particular, las empresas alimentarias pueden hacer uso de la publicación del IREC, Gestión Integral del Riesgo Empleado (Homer) [30].*

Tabla 4 - Personal de Seguridad

Las comprobaciones previas de empleo		¿Pertinente? ¿Proporcionado?
1	Prueba de identidad	
2	La prueba de las cualificaciones	
3	La verificación de los contratistas	
4 papeles más sensibles	identificado con el reclutamiento adecuado	
En curso de seguridad personal		**¿Pertinente? ¿Proporcionado?**
5	El personal de papeles críticos motivado y supervisado	
6 La denuncia de irregularidades	preparativos	
7	El personal temporal supervisado	
8	Las personas capaces de trabajar solo	
9	cultura de seguridad favorable [28)]	
Fin de acuerdos contractuales		**¿Pertinente? ¿Proporcionado?**
10 tarjetas y claves de acceso e ID	recuperado	
11 Las cuentas cerradas ordenador o	suspendido	
12 entrevista de despido	evalúa implicaciones de seguridad	

[28)] Para más información sobre la cultura de seguridad está disponible a partir de: IREC en https://www.cpni.gov.uk/developing-security-culture [31].

8 Respuesta a un incidente

8.1 Gestión de una crisis de protección de los alimentos

protección de los alimentos y los procedimientos de defensa tienen por objeto reducir el riesgo de un ataque, pero no puede eliminarlo, por lo que la respuesta a emergencias y protocolos de continuidad de negocio son esenciales.

protección de los alimentos puede sentarse dentro del sistema de gestión de crisis de una empresa (véase BS 11200), y es probable que compartan sus objetivos generales:

- para reducir al mínimo los daños físicos y financieros a los consumidores, clientes, empleados y otros;
- colaborar con las autoridades de investigación y ejecución (por ejemplo, la Unidad Nacional de Alimentación del crimen en el Reino Unido);
- para ganar el apoyo público a la organización;
- para reducir al mínimo el costo - financiera, la reputación y el personal - del suceso;
- para prevenir la re-ocurrencia; y
- para identificar a los delincuentes.

Donde la contaminación es implícita, cuarentena y tal vez retirada y recuperación de producto podría esperarse.

En los casos que implican la acción penal, policías de las unidades de delitos graves deben estar involucrados en la primera oportunidad para evitar cualquier pérdida de pruebas.

***NOTA** Algunos ejemplos de los contactos con la policía son la Agencia Nacional del crimen y la unidad antisecuestro y extorsión; otros también se proporcionan en el Anexo B.*

En general, el mejor momento para aprender cómo gestionar una crisis no está en la crisis, por lo que la planificación avanzada y el ensayo de los procedimientos es esencial.

8.2 Gestión de un ciberataque

La velocidad de respuesta puede influir en gran medida el daño causado por un ataque cibernético por lo que el mantenimiento de la conciencia colega puede ser crucial. La complejidad y variedad de ataques pueden ser tan grandes que la selección de un contratista especializado (por adelantado del incidente) puede beneficiar a muchas organizaciones.

Pensamientos acerca de la respuesta a incidentes cibernéticos están disponibles de CREST (Consejo de Ética registrados probadores de seguridad) [32]. El apoyo también puede estar disponible en calidad de miembro de la seguridad cibernética Asociación de Intercambio de Información (CISP) [33].

8.3 La planificación de contingencia para la recuperación de los ataques

principios de gestión de continuidad de negocio dan buena resistencia a reaccionar y recuperarse de un ataque. Consejos sobre la mejor manera de desarrollar y poner en práctica la recuperación de su organización en respuesta a un incidente perturbador se proporciona en BS ISO 22313.

9 Examen de las disposiciones de protección de alimentos

Cualquier cambio que pueda afectar a la evaluación, tales como TACCP infracciones y posibles infracciones de seguridad o autenticidad, debe ser reportado inmediatamente a la líder del equipo TACCP quien decide si se necesita una revisión completa.

El equipo TACCP debe supervisar los sitios web oficiales de actualizaciones en las evaluaciones nacionales de amenazas y de información sobre los riesgos emergentes (véase el anexo B). La situación local puede ser revisada con frecuencia y brevemente contra los cambios en las condiciones relativas a los locales.

Un informe conciso de la revisión debe tener solamente una circulación limitada.

El equipo TACCP debe revisar periódicamente las disposiciones de protección de alimentos en línea con otras políticas de la empresa.

***NOTA** El informe TACCP y cualquier documento de revisión son comercialmente sensible y confidencial. De confianza altos directivos con una 'necesidad de saber' y los agentes requieren acceso. Las organizaciones pueden considerar publicación de una descripción genérica para uso interno y / o para presentar a los auditores externos. Tal evita descripción del detalle que podría ser de valor para un atacante. Los auditores externos deben respetar la naturaleza sensible del proceso TACCP.*

Estudios Anexo A (informativo)
TACCP de casos

NOTA *Estos estudios de casos son completamente ficticios y cualquier parecido con las organizaciones reales es pura coincidencia.*

A.1 Generalidades

Esto presenta anexo cuatro estudios de casos para ilustrar cómo el proceso TACCP se puede adaptar, operado y reportado por diferentes organizaciones para reflejar su situación de negocios. Se escriben como registros formales de la evaluación de riesgos y no intentan cualquier contexto documentación de la empresa.

Un estudio de caso es una cadena nacional de comida rápida, y el estudio de caso B es una pequeña empresa con un propietario / gerente que se encarga de todos los asuntos estratégicos y operativos personalmente.

Estudio de caso C y D estudio de caso se pretende que los problemas de seguridad más destacado cibernéticos que enfrentan las empresas alimentarias innovadoras. Estudio de caso C es una iniciativa de alimentos por un Internet establecida, pero no a los alimentos, operador. Estudio de caso D es una empresa profesional de alimentos con el objetivo de aprovechar las oportunidades digitales.

En todos los casos el proceso TACCP ha cambiado deliberadamente de la descrita en la cláusula 5 para animar a los usuarios de esta PAS a adoptar un enfoque de mente abierta.

Un estudio A.2 Caso

Un estudio de caso presenta un ejemplo de informe siguiendo el trabajo de investigación del equipo de TACCP en Burgers4U, una cadena nacional de comida rápida. Los supuestos realizados son los siguientes:

- Burgers4U es una cadena de comida rápida ficticia con la propuesta única de venta (USP) que elabora sus propias hamburguesas. A nivel nacional es un importante operador pero no tiene ningún negocio internacional;
- la hamburguesa estándar se considera que es típico de la gama: estándar, jumbo, de vegetales, queso, y chile;
- el Director de Operaciones de Burgers4U conduce Comité de Planificación de Emergencia y la continuidad del negocio de la compañía;
- el Jefe de Auditoría Interna tiene la responsabilidad delegada para la seguridad y prevención de fraude;
- el equipo TACCP también recibió contribuciones de otros administradores en temas especializados; y
- Este caso hace estudiar el uso de la información en el informe del grupo consultivo de expertos: Las lecciones que pueden aprenderse de la carne de caballo incidente 2013 [34].

TACCP Un estudio de caso

Empresa: BURGERS4U

Ubicación: Todos los puntos de venta de la calle

Producto: hamburguesa de comida para llevar Estándar

TACCP equipo: Contratación Director de Operaciones (Presidente) Director de Recursos Humanos Jefe Director Técnico Director de Auditoría Interna

Tabla A.1 - Información de la amenaza

No hay	amenazas a la empresa y info-sistemas de:	método de operación posible	comentarios
UN	derechos de los animales	El vandalismo o sabotaje	Poca evidencia de actividad actual
si	hacktivistas	denegación de servicio distribuido ataque (DDoS) en el sitio web	El desarrollo de perfil de la empresa pueden provocar ataques
C	los compradores de la compañía	Fraude; colusión con los proveedores	Establecido equipo que trabaja de forma autónoma
re	Los criminales	falsificación; apropiación indebida de los envases	El aumento del riesgo como fortalece la marca
No hay	**amenazas a las poblaciones de:**	**método de operación posible**	**comentarios**
mi	Los partidarios de las empresas locales	Publicidad adversa; 'La culpa por asociación' con la comida rápida	Algunos lugares reportan altos niveles de interés de la prensa
F	personal de la empresa con exceso de trabajo, el desencanto podría conducir a la alianza con los extremistas (por ejemplo, los terroristas)	contaminación Petty; posible contaminación intencionada grave	Algunos escasez de personal donde hay poca educación post-18; y en lugares con una reputación extremista
sol	grupos monotemáticos	infestación deliberada de Locales	Algunos precedentes recientes
H	Personal de primera línea	Robo; connivencia con los clientes	rigurosa auditoría en su lugar; gestores Outlet digno de confianza (Personal controles de seguridad)
No hay	**Amenazas a producto de:**	**método de operación posible**	**comentarios**
yo	Proveedores de carne	EMA - proteína no animal, o carnes nonbeef, carne sustitución	Carne de vacuno se especifica y se espera que, a pesar de que no se reivindica en la publicidad
J	Personal de primera línea	la cocción insuficiente deliberada de Patty	Rotas minimizar la posibilidad de colusión
K	Personal de primera línea	La venta de hamburguesa demasiado tiempo después de envolver	
L	grupo ideológicamente motivado	contaminación malicioso del componente	nivel oficial amenaza sin cambios
NOTA *Los informes de prensa de preocupaciones acerca de la autenticidad de alimentos son pertinentes.*			

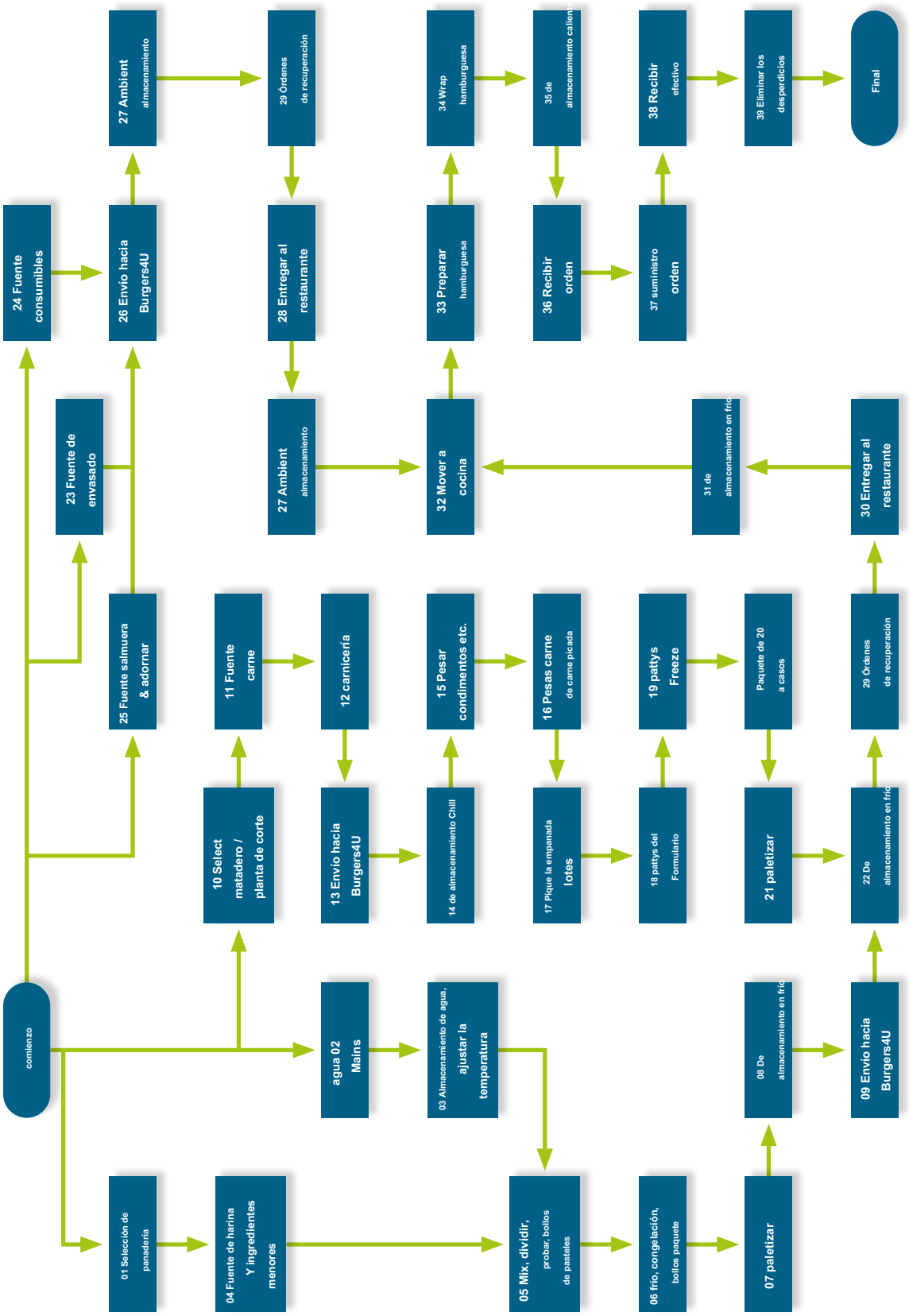


Figura A.1 - la identificación de amenazas

Tabla A.2 - la identificación de amenazas

Paso No	Paso de proceso	Amenaza	Acceso vulnerabilidad		Mitigación	Mezcla; Contaminación	Impacto del proceso de	QA / QC	Probabilidad	Impacto
01A	Seleccionar panadería	Varios	personal eventual	Staff de producción	Contratos requieren protocolos de seguridad personal	-	-	-	-	-
01B	Seleccione panadería	Fraude	Colusión	Los compradores	Pequeño	-	-	-	2	3
02	Agua de la red	contaminación malicioso	depósitos de almacenamiento a granel	Los ingenieros de servicios	El control efectivo del acceso	toxinas solubles	Puede inhibir la levadura; puede afectar a la masa de manipulación	Puede fallar pruebas sensoriales	1	1
03	Almacenar agua; ajustar temperatura	Como anteriormente	depósitos de almacenamiento de lotes	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriormente	1	1
04	harina de fuente + menor ingredientes	sustitución fraudulenta	Poco ventaja de costos a defraudador	-	-	-	-	-	-	-
05	Mezcla, dividir, probar los bollos, pasteles	contaminación malicioso	operación de mezclado por lotes	operativa mezclador especializada	El personal capacitado y con experiencia	la toxina en polvo	Puede inhibir la levadura; puede afectar a la masa de manipulación	Puede fallar pruebas sensoriales	1	1
06	Fresco, congelado, bollos paquete	-	-	-	-	-	-	-	-	-
07	paletizar	-	-	-	-	-	-	-	-	-
08	Almacenamiento en frio	-	-	-	-	-	-	-	-	-
09	Entregar a Burgers4U	-	-	-	-	-	-	-	-	-

Tabla A.2 - la identificación de amenazas (*continuado)*

Paso No	Paso de proceso	Amenaza	Acceso vulnerabilidad		Mitigación	Mezcla; Contaminación	Impacto del proceso de	QA / QC	Probabilidad	Impacto
10A	Seleccionar matadero / de despiece	Fraude	Colusión	Los compradores	Pequeño	-	-	-	3	5
10B	Seleccionar matadero planta / corte	sustitución fraudulenta	La mala segregación de las especies	Los conductores de reparto; el personal de proceso	identificación animal única registró	La carne de fuentes más baratas	Despreciable	pruebas aleatorias pueden detectar a menos que la colusión	2	3
11	fuente carne	sustitución fraudulenta	La mala segregación de las especies	La gestión de procesos y el personal		La carne de fuentes más baratas	Despreciable	pruebas aleatorias pueden detectar a menos que la colusión	4	3
12	Carnicería	sustitución fraudulenta	La mala segregación de las especies	dirección y personal proceso de		La carne de fuentes más baratas	Despreciable	pruebas aleatorias pueden detectar a menos que la colusión	2	3
13	Entregar a Burgers4U	El secuestro de envío	la responsabilidad del proveedor	-	-	-	-	-	-	-
14	almacenamiento refrigerado	-	-	-	-	-	-	-	-	-
15	Pesar condimentos, etc.	contaminación malicioso	Manual de operación	dirección y personal proceso de	rigurosas normas de higiene	toxinas en polvo	Puede no despreciable	pruebas sensoriales	1	3
dieciséis	Pesar carne para carne picada	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriomente	Como arriba	Como arriba	Como anteriormente
17	lotes empanada de carne picada	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriomente	Como arriba	Como arriba	Como anteriormente

Tabla A.2 - la identificación de amenazas (*continuado)*

Paso No	Paso de proceso	Amenaza	Acceso vulnerabilidad		Mitigación	Mezcla; Contaminación	Impacto del proceso de	QA / QC	Probabilidad	Impacto
18	pattys del formulario	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriormente	Como anteriormente	Como arriba	Como arriba	Como anteriormente
19	pattys congelación	-	-	-	-	-	-	-	-	-
20	Empacar para casos	-	-	-	-	-	-	-	-	-
21	paletizar	-	-	-	-	-	-	-	-	-
22	Almacenamiento en frio	-	-	-	-	-	-	-	-	-
23	Fuente embalaje	Malversación; falsificación	la seguridad del depósito con proveedor	conductores de la entrega de la agencia	Pequeño	-	-	-	2	4
24	Fuente consumibles	-	-	-	-	-	-	-	-	-
25	guarnición de pepinillos + Fuente	la sustitución de ingredientes	-	-	marcas establecidas; contratos fiables	-	-	-	-	-
26	Entregar a Burgers4U	-	-	-	-	-	-	-	-	-
27	Ambiente de almacenamiento -		-	-	-	-	-	-	-	-
28	Entregar al restaurante	-	-	-	-	-	-	-	-	-
29	recoger pedidos	-	-	-	-	-	-	-	-	-
30	Entregar al restaurante	-	-	-	-	-	-	-	-	-
31	Almacenamiento en frio	-	-	-	-	-	-	-	-	-
32	Mover a la cocina malicioso	sustitución	Fuera de las horas; sin supervisión	storestaff noche	Tamper casos evidentes	pattys 'pinchos'	Pequeño	Ninguna	1	3

Tabla A.2 - la identificación de amenazas (*continuado)*

Paso No	Paso de proceso	Amenaza	Acceso vulnerabilidad		Mitigación	Mezcla; Contaminación	Impacto del proceso de	QA / QC	Probabilidad	Impacto
33	preparar hamburguesas	la cocción insuficiente deliberada	trabajador solitario	El personal del restaurante	fabricación seguridad alimentaria rigurosa	-	-	Ninguna	1	2
34	hamburguesa envoltura	-	-	-	-	-	-	-	-	-
35	almacenamiento en caliente	-	-	-	-	-	-	-	-	-
36	Orden recibida	-	-	-	-	-	-	-	-	-
37	para la oferta	Vendiendo demasiado tiempo después de envolver	El director del restaurante bajo presión desperdicio	-	procedimientos de seguridad personal	-	-	-	2	2
38	recibir efectivo	Robo	El personal del restaurante	Contador personal	Automatizado cajas registradoras; rigurosa auditoría	-	-	-	4	1
39	Eliminar los residuos	apropiación indebida; falsificación	contenedores externos desbloqueados	Público	la eliminación diaria	-	-	-	1	2
NOTA *El símbolo '-' indica 'no aplicable' o 'no significativo'.*										

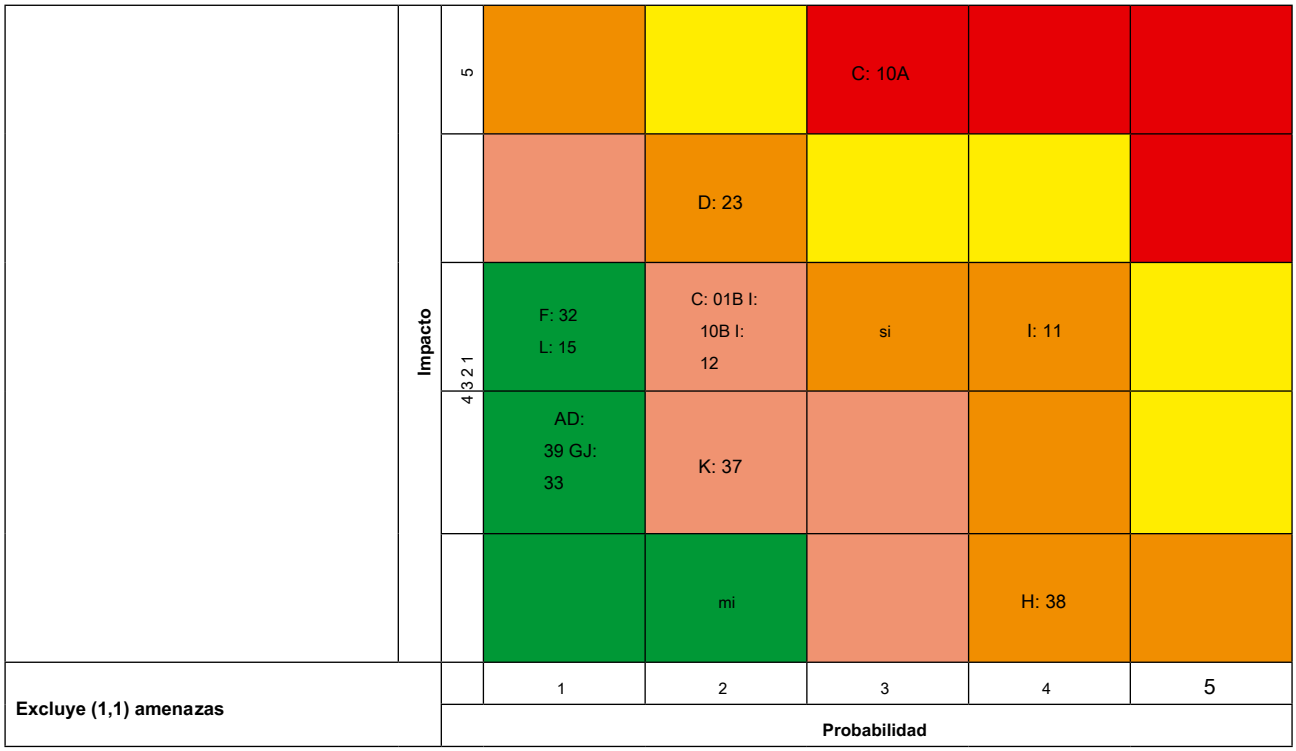
Tabla A.3 - Evaluación de amenazas

Amenaza	Descripción	paso vulnerables	Probabilidad	Impacto	acción protectora
UN	El vandalismo o sabotaje	todas las localizaciones	1	2	mantener la vigilancia
si	Ataque DDoS en el sitio web	Márketing	3	3	Garantizar una práctica buena seguridad cibernética
C: 01B	Fraude; colusión con los proveedores	Seleccione panadería	2	3	rotación en el trabajo <5 años
C: 10A		Seleccionar matadero planta / corte	3	5	Auditoría interna

Tabla A.3 - Evaluación de amenazas (*continuado)*

Amenaza	Descripción	paso vulnerables	Probabilidad	Impacto	acción protectora
D: 23	falsificación; apropiación indebida de los envases	fuente envases	2	4	requerimiento al proveedor; nuevo proveedor si no hay mejoría en la seguridad después de 6 meses
D: 39		Eliminar los residuos	1	2	Ninguna otra acción
mi	La publicidad adversa: 'La culpa por asociación' con la 'comida rápida'	Corporativo	2	1	Revisión de la estrategia de relaciones públicas
F: 32	contaminación Petty; Posible contaminación intencionada grave	Mover a la cocina	1	3	Parte utilizada casos a ser la seguridad sellada por el gerente
sol	infestación deliberada de Locales	restaurantes	1	2	mantener la vigilancia
H: 38	Robo: la colusión con los clientes	recibir efectivo	4	1	Ninguna otra acción
I: 10B	EMA - proteína no animal, o carnes nonbeef, carne sustitución	Seleccionar matadero planta / corte	2	3	gestión más fuerte de proveedor: auditoría técnica, muestreo regular / pruebas ad hoc, facilitan la denuncia de irregularidades
I: 11		fuente carne	4	3	
I: 12		Carnicería	2	3	
J: 33	la cocción insuficiente deliberada de Patty	preparar hamburguesas	1	2	Ninguna otra acción
K: 37	La venta de hamburguesas demasiado tiempo después de envolver	para la oferta	2	2	Ninguna otra acción
L: 02	contaminación malicioso del componente	Agua de la red	1	1	Ninguna otra acción
L: 03		Almacenar agua; ajustar la temperatura	1	1	
L: 05		Mezcla, dividir, probar los bollos, pasteles	1	1	
L: 15		Pesar condimentos, etc.	1	3	El personal clave de seguridad personal cumpla con las normas

Figura A.2 - priorización de amenazas



Conclusiones A.3

TACCP dio un registro amenaza de amenazas, 19, 9 de ellas bajo control satisfactorio.

Fraude en la selección de la planta matadero / corte es la mayor amenaza para Burgers4U. En marcha penas de costes y daños a la reputación significativa que pudiera resultar. Estrechamente vinculadas son las amenazas de especies o sustitución proteína no carne. Dentro del equipo TACCP, el Gestor Técnico se encarga de la aplicación de medidas de protección con el objetivo de reducir la amenaza a (2,3) dentro de los 12 meses. Esta acción es probable que también mitigar otras amenazas de abastecimiento.

Como marca con una creciente reputación por la calidad y la integridad, la amenaza de los aumentos de los productos falsificados. El proveedor tradicional de material de embalaje impresa no reconocer esto y tiene medidas de seguridad físicas inadecuadas en su lugar. Como socio de otra manera fiable, el Gerente de Compras se encarga de desafiar el proveedor para remediar la situación o encontrar una alternativa. Esta amenaza se debe evaluar como (1,3) o mejor dentro de los 6 meses.

La página web Burgers4U no es un instrumento de venta principal, pero juega un papel importante la comercialización. El Jefe de Auditoría Interna se encarga de lidiar con el Departamento de Sistemas de negocios para asegurar la adecuada financiación de los procedimientos de seguridad informática en general, y en contra de ataques de denegación de servicio en particular. Consejos y ofertas para servicios de respuesta cibernéticos pueden buscarse (por ejemplo, de CREST aprobó proveedores). Se prevé ninguna reducción en la evaluación (3,3).

El Director Técnico es monitorear las fuentes oficiales y de la industria de información e inteligencia sobre los riesgos emergentes y decidir con el presidente del equipo TACCP si se debe convocar al grupo antes de su programada 6 reunión de rutina mensual.

A.4 Estudio de caso B

Caso B estudio presenta un ejemplo de informe de evaluación de amenazas de Bridgeshire Cheese Company. Fue preparado, solos en ausencia de otros colegas ejecutivos, por
A. Bridgeshire el socio gerente, y resume su evaluación individual de las amenazas que enfrenta. Bridgeshire Cheese Company es una pequeña familyfarm ficticia de propiedad y operación orgánica venta productora de queso a tiendas especializadas y empresas de servicios de alimentos.

Tabla A.4 representa un ejemplo de informe de evaluación de amenazas. Figura A.3 representa un diagrama de flujo evaluación de la vulnerabilidad.

Tabla A.4 - Informe de Evaluación de amenazas 20170602

Amenaza No	Desde	Amenaza	Vulnerabilidad [UN]	Mitigación	Consecuencia	Impacto	La acción protectora probabilidad
1	proveedores	suministro no orgánico	'Top-up' de la leche; Comprado-en terneros; semen [SI]	Todos los productos de los proveedores acreditados	Pérdida de la condición orgánica	5	2 Requerir certificado de conformidad para todas las compras especiales
2	Vecinos sobre-reaccionar a 'efluentes molestia'	enfermedades del ganado generalizada	Derechos de paso a través de la granja	Bioseguridad cumple con las mejores prácticas	La pérdida de la manada y / o cobertura de seguro	3	2 Instalar depósito para evitar la descarga de efluente cuando el viento desde el SW
3	El personal BCC	contaminación malicioso	Las operaciones manuales, sin supervisión (proceso en gran medida selfcontrolling)	Todo el personal son miembros de la familia o socios de confianza a largo plazo; Todos los lotes se prueban el sabor	enfermedad localizada posible	2	1 Ninguna otra acción
4	granjas adyacentes Ensayos de GM cultivos		Perímetro pastos	campaña de organización de acreditación	Pérdida de la condición orgánica	4	3 La acción cooperativa con la asociación comercial para funcionarios elegidos vestíbulo
5	criminales oportunistas	El robo de distribución del producto, vehículo menudo no tripulado y desbloqueado		Pequeño	Valor de los bienes; La pérdida de la reputación de fiabilidad	2	3 Reemplazar con vehículo más moderno en primera oportunidad
6	Los delincuentes cibernéticos ataque remoto	Nube en proceso de producción controlado	La manipulación de la 'de la clavija' sistema SCADA para reducir el tiempo de pasteurización / temperatura	Proveedor es tranquilizador	de peligrosidad del producto de debajo de procesamiento	5	1 Mantener el análisis de control de calidad por separado seguir el consejo NCSC

[UN] Ver Figura A.3 para la evaluación completa proceso de vulnerabilidad.

[SI] Otros productos se obtienen habitualmente a partir de empresas acreditadas de larga data.

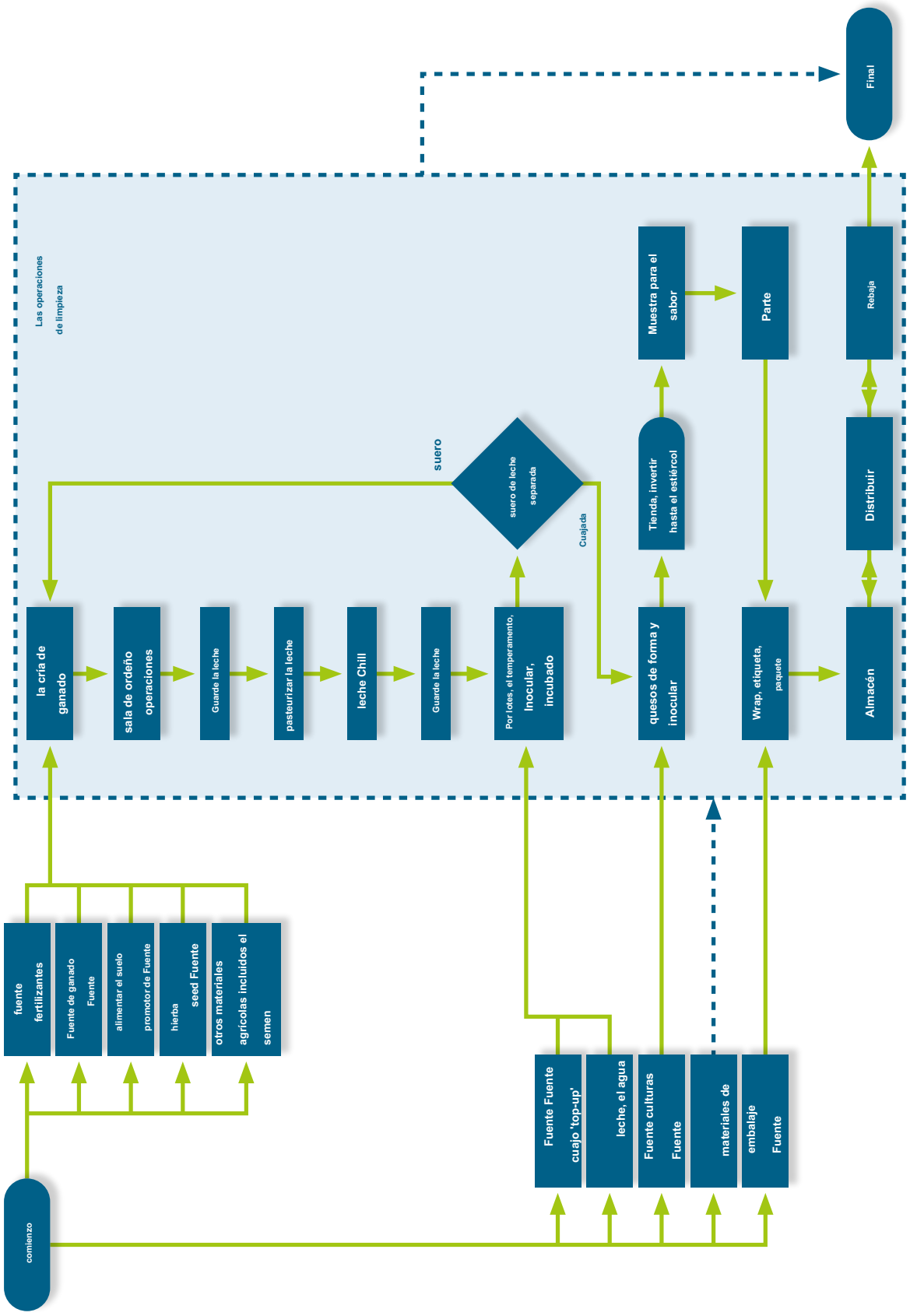


Figura A.3 - Evaluación de vulnerabilidad

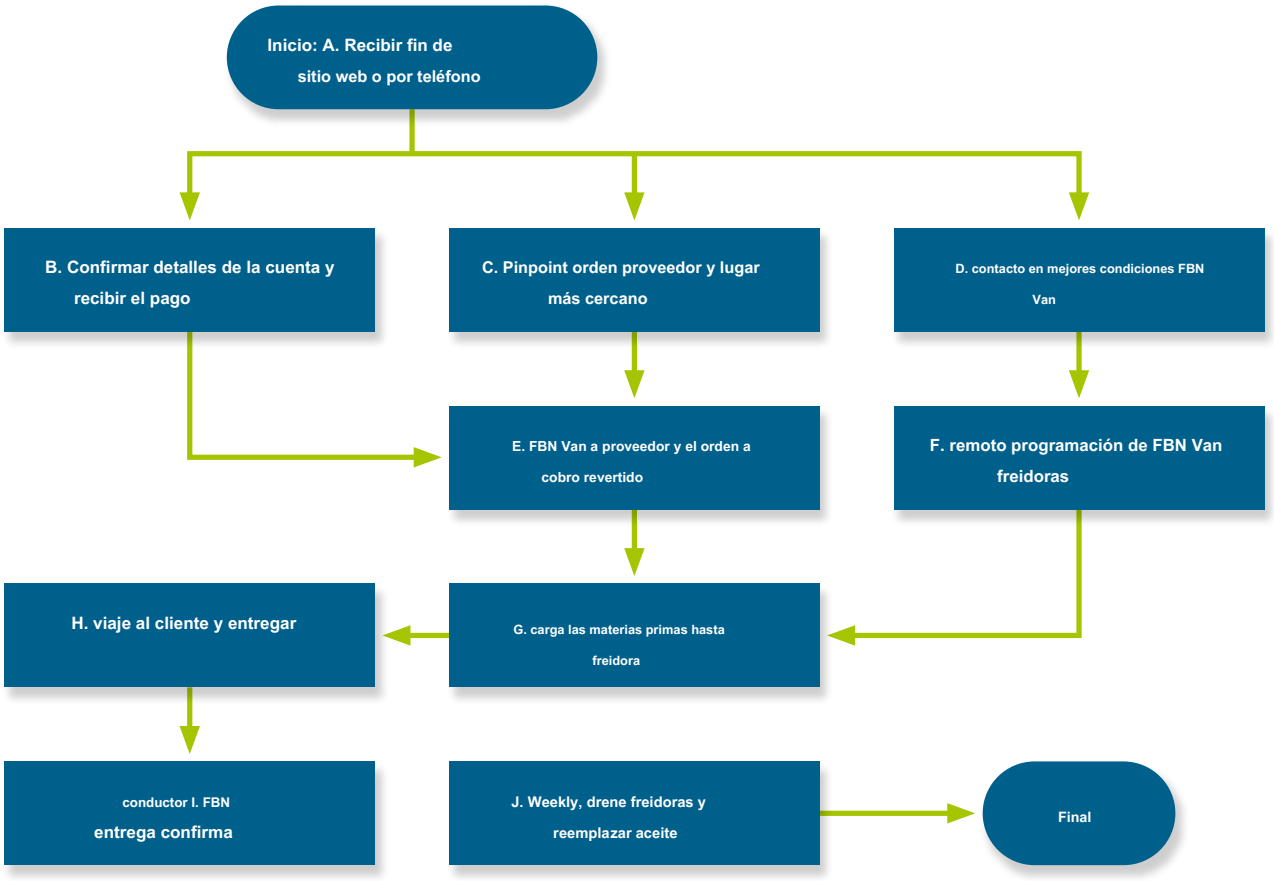
A.5 Estudio de caso C

FryByNite es una nueva empresa, el servicio nacional de entrega de comida caliente de una importante compañía de comercio general basado en Internet. La compañía es líder mundial en su campo de software y gestión de la logística, pero es nuevo en las operaciones comerciales de alimentos. Se reconoce su debilidad en los alimentos y tiene un especialista en alimentos consultor en el contrato por la duración de la puesta en marcha y consolidación de las fases de FryByNite.

FryByNite tiene como objetivo ofrecer comida caliente recién hecha a la puerta de los clientes dentro de los 30 minutos de recibir una orden web o teléfono. El producto estándar es de pescado y patatas, con cada vehículo de salida que lleva freidoras programables. El producto crudo se ordena través de Internet desde una red de puntos de venta de comida rápida contratados. Estos preparan la comida y cargarlo en las cestas de fritura usados por el vehículo de suministro. Un sistema de posicionamiento global (GPS) estima el tiempo a las instalaciones de los clientes e iniciados el proceso de fritura. Cuando esté listo, las cestas de fritura se retiran de forma automática y la comida se envasa y se mantiene caliente para que el cliente recibe comida caliente recién hecha en mejores condiciones que si hubieran visitado la salida de sí mismos. (Ver Figura A.4)

Ejemplo producto: pescado frito y patatas fritas para la entrega a domicilio (como típica del menú)

Figura A.4 - FryByNite flujo de trabajo



TACCP Equipo: Director de Recursos Humanos (Presidente)
Director de Sistemas de Información
alimentos Consultor técnico jefe de seguridad

información de la amenaza

NOTA *Como una nueva 'marca' FryByNite está cubierto por la celebración de los procedimientos de gestión de riesgos de la empresa y de planificación de contingencia. Por tanto, el TACCP aborda los aspectos operativos de la nueva empresa.*

Cuadro A.5 - Información de la amenaza

No hay	actores de amenazas	Las amenazas a la empresa de:	método de operación posible	comentarios
1	hacktivistas	El fallo de sistema de pedidos basado en la web	ataque DDoS	Protegidos por los sistemas de toda la compañía y la experiencia
2	Estados nacionales	La pérdida de la navegación basada en GPS	El exceso de compromiso y / o mantenimiento inadecuado por los operadores de satélites.	No hay control sobre los actores amenaza, sino una fuerte protección contractual con los operadores
3	extorsionistas	Exfiltración de datos sensibles	Los mensajes de phishing para el personal	Ransomware fácilmente disponibles
4	Insiders	El robo de IP	El acceso no autorizado a los privilegios administrativos	
		Las amenazas a la del producto:		
5	proveedores agraviadas	Comida envenenada	manejo inadecuado de producto	
6	Competidores	Comida envenenada	El fallo de la cocción van régimen	De corte de energía, o la subversión de los controles de los procesos
7	El personal perjudicada	Comida envenenada	contaminación malicioso	la seguridad personal de inspección en el lugar
		Las amenazas a las operaciones de:		
8	Los criminales	Ataque en el vehículo / conductor	Atraco por dinero en efectivo	Signos: “No hay dinero que tuvo lugar en este vehículo” en su sitio
9	vándalos	daño Petty al vehículo	el oportunismo no planificada al azar	las zonas de mayor riesgo en el sistema de navegación vía satélite observaron
10	Los defraudadores	Pérdida de ingreso	El uso de los datos personales robados para crear una cuenta falsa	

Tabla A.6 - Evaluación de amenazas

amenaza	paso	Amenaza nº	Vulnerabilidad	Mitigación	Adulterante / Contaminante	Comentario	Probabilidad	Impacto
UN	DDoS (**1**)	A1	Alta - sitio público	sistemas corporativos dan la alerta temprana	-	Molestia; pérdida de ventas; clientes molestos	4	2
UN	insuficiencia interbancaria (**2**)	A2	sistema de transferencia electrónica de fondos es un objetivo primordial cibernética, pero bien protegido	Mantener estrechos vínculos con los operadores de sistemas	-	Pequeña posibilidad de pérdida importante	2	4
si	cuenta fraudulenta (**10**)	B1	punto de entrega ficticio	Consultar nuevas cuentas en la configuración	-	Derrochador de tiempo	1	1
C	Proveedor no disponible	C1	Bases de datos de retraso	Estrecha colaboración con los proveedores	-		1	1
C	Producto contaminación (**5**) (**6**) (**7**)	C2	Batter puede ser objetivo	Proveedores examinados para la operación de HACCP	Químicos tóxicos; bacterias formadores de esporas	Proveedor no conoce la identidad del cliente, a menos que la colaboración	1	4
C	Producto sustitución (**5**)	C3	fraude alimentario oportunista	Como C2	Intercambio de especies	La reputación y la regulación	3	2
re	insuficiencia GPS	D1	Señal debil	Enlace con los proveedores de telecomunicaciones	-	planes de contingencia	1	1
F	La corrupción del sistema de control con malware (**1**) (**4**)	F1	La nueva tecnología: engancha probable	Las pruebas han revelado la capacidad de recuperación	-	Incendio o mal cocinado de alimentos posible	3	5
sol	la cocción insuficiente	G1	filetes de gran tamaño	Los límites de tamaño	-	producto comestible	1	1

Tabla A.6 - Evaluación de amenazas (*continuado)*

amenaza paso		Amenaza nº	Vulnerabilidad	Mitigación	Adulterante / Contaminante	Comentario	Probabilidad	Impacto
sol	Producto contaminación (**4)**	G2	operación manual sin supervisión	selección de personal	Químicos tóxicos; bacterias formadores de esporas		2	4
H	Los retrasos en la ruta	H1	el tráfico inesperado o obras viales	Las actualizaciones automáticas de navegación vía satélite	-	Compensación si no comestible comida	3	1
H	**Asalto en el personal (8) H2**		Algunos clientes difíciles y áreas.	La formación del personal en la prevención de conflictos	-	Una de las principales preocupaciones en algunas áreas	2	5
H	Daños al vehículo (**9)**	H3	Vehículo sin supervisión durante el parto	las zonas de mayor riesgo en el sistema de navegación vía satélite observaron	-	en gran medida las molestias	1	2
J	una eliminación inadecuada de **los aceites usados (7)**	J1	El personal bajo presión en busca de atajos	Sustitución 'nuevo por viejo'	-	daños a la reputación	1	2
J	El uso de aceite incorrecto	J2	El personal bajo presión en busca de accesos directos o errores que cubren	Sustitución 'nuevo por viejo'	Otros aceites comestibles Aceites minerales químicos orgánicos tóxicos	Temas: el etiquetado; alergia; integridad; toxicidad; seguridad contra incendios	1	4

Figura A.5 - priorización de amenazas

Probabilidad						
	5					
	4		A1			
	3	H1	C3			F1
	2				G2 A2	H2
	1	B1 C1 D1 G1	J1 H3		C2 J2	
		1	2	3	4	5
	Impacto					

Cuadro A.7 - Registro de Amenazas

Amenaza	Valoración (L, I)	Descripción	Además acción defensiva	Responsabilidad	Comentario
F1	(3,5)	La corrupción de sistema de control de proceso para las freidoras	Revisión diaria por fases puesta en marcha y consolidación. Construir el contacto con el proveedor de software.	Director de Info Tech	Objetivo (2,3) dentro de un año.
A1	(4,2)	DDoS - sitio web	Construir contacto NCSC. Realizar un seguimiento de la charla medios de comunicación social.	Director de Info Tech	En marcha. riesgo de amenaza poco probable que cambie.
H2	(2,5)	Asalto en el personal	Evaluar el uso de cámaras corporales	Director de Info Tech	Con el Director de Recursos Humanos
C3	(3,2)	la sustitución de productos fraudulentos	Introducir bajo nivel abierta muestreo del producto	Consultor de tecnología de los alimentos	Target (1,2)
A2	(2,4)	el fracaso de transferencia de fondos entre bancos	Continuar los protocolos actuales.	Director de Info Tech	Seguro de cobertura adecuada.
G2	(2,4)	la contaminación del producto malicioso	Introducir rutinas de seguridad de personal en curso.	Director de Recursos Humanos	Target (1,4)
H1	(3,1)	Los retrasos en la ruta	Continuar los protocolos actuales.		Bajo el control proporcional.
J1	(1,2)	una eliminación inadecuada de los aceites usados	Revisión y promover 'nuevo por viejo' modelo.	Director de Recursos Humanos	Target (1,1) dentro de un año.
H3	(1,2)	Daños al vehículo	Continuar los protocolos actuales.		Bajo el control proporcional.

Cuadro A.7 - Registro de Amenazas (*continuado)*

Amenaza	Valoración (L, I)	Descripción	Además acción defensiva	Responsabilidad	Comentario
C2	(1,4)	la contaminación del producto malicioso	Incluir el manejo de productos químicos no alimentarios en la homologación de proveedores.	Consultor de tecnología de los alimentos	riesgo de amenaza poco probable que cambie.
J2	(1,4)	El uso de aceite incorrecto	La tecnología de construcción en la formación de inducción.	Director de Recursos Humanos	riesgo de amenaza poco probable que cambie.
B1	(1,1)	cuenta fraudulenta	No se requieren mas acciones.	-	Bajo el control proporcional.
C1	(1,1)	Proveedor no disponible	la formación de la opinión del administrador de base de datos.	Director de Recursos Humanos	-
D1	(1,1)	insuficiencia GPS	No se requieren mas acciones.	-	Bajo el control proporcional.
G1	(1,1)	productos poco cocinados	No se requieren mas acciones.	-	Bajo el control proporcional.

Comentario

1. Como un nuevo desarrollo de los planes del equipo TACCP a reunirse mensualmente para revisar los desarrollos.
2. En todo el equipo ha identificado 15 amenazas de las que siete requieren una acción protectora sustantiva.
3. El control remoto de la operación de freír crea la oportunidad para las nuevas amenazas (F1) que recibirían la atención de alto nivel y prioridad de la organización.
4. Las precauciones, es decir, una formación adecuada, desde el lanzamiento de la iniciativa han mantenido la probabilidad de asalto a la baja del personal, pero es necesario seguir trabajando.
5. altos directivos de la empresa matriz continúan su política de evitar una imagen pública de alto perfil que ayuda a reducir la posibilidad de FBN ser un objetivo.

A.6 Caso de estudio D

F. Armer y hijas Ltd es una compañía agrícola establecida con una reputación envidiable de 'buenas prácticas'. El negocio ha evolucionado y crecido desde sus orígenes como una granja familiar mixto suministro de su población local con productos de temporada a través de su arancel hortícola amplio presente. La actividad principal es 'fresco como puede ser fresca' de suministro de verduras para la venta al por menor. Algunos cereales de frutas y especialistas complementan la producción de hortalizas. Existe un interés creciente en el suministro a las operaciones de servicio de alimentos.

El negocio es administrado sobre una base del día a día a las nietas del fundador de la granja, el padre de la F. Armer que nombró a la empresa y sigue siendo su presidente. Emplea un pequeño equipo para ejecutar la fábrica de limpieza y el embalaje altamente mecanizada, sino que depende en gran medida de los contratistas agrícolas para el cultivo de trabajo, el uso de personal temporal a los períodos de mayor cobertura. Se ha comprometido a verificación externa de sus procesos y procedimientos y recibe informes a modo de ejemplo a partir de organismos de acreditación y múltiples clientes por igual. Estos procedimientos incluyen un método eficaz para la gestión de riesgos.

Ahora, la compañía ha llevado a cabo un movimiento masivo en la automatización y el control remoto de ambas operaciones de cultivo y el paquete interno. Se ha comprometido a la utilización de la vigilancia vehículo aéreo no tripulado (UAV) de los cultivos para mejorar la gestión del riego, aplicación de pesticidas, fertilizantes y otros tratamientos, y la cosecha. Se pretende integrar plenamente refrigeración, limpieza, limpieza y embalaje de los productos. Su objetivo es reducir significativamente aún más el tiempo del campo a la expedición.

Como parte de esta iniciativa y que no se detiene a cabo, los Administradores han contratado un especialista en seguridad de la información de consultoría para llevar a cabo un ejercicio de TACCP relacionada específicamente con los nuevos sistemas de información. La gestión de riesgos del negocio convencional está bien establecida. La intención es que tienen controles proporcionados en su lugar.

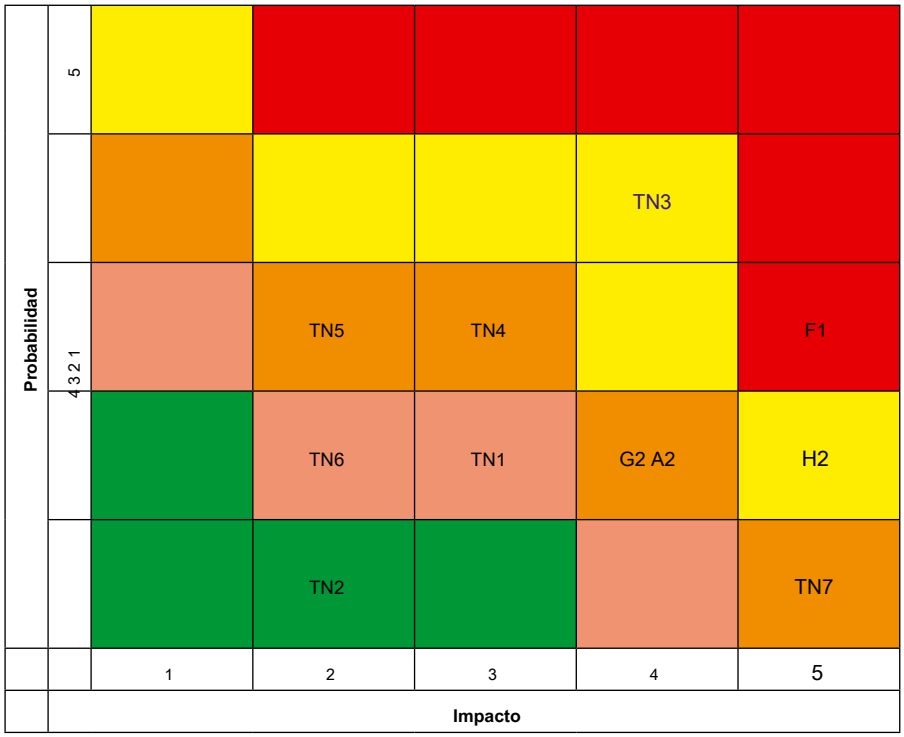
Tabla A.8 - Las posibles fuentes de actividad maliciosa que afectan F. Armer y hijas Ltd

Mayor amenaza de:	Moderar la amenaza de:	amenaza más bajo de:
hacktivistas	ex empleados alienados que buscan venganza	Competidores
El sabotaje de la infraestructura de soporte de TI	Los terroristas que buscan publicidad	defensores del medio ambiente
extorsionistas		Contratistas
Los delincuentes que roban IP innovadora		

Tabla A.9 - Evaluación de amenazas

Amenaza No.	Sistema	Amenaza	Vulnerabilidad	Mitigación	Comentario	Probabilidad	Impacto
TN1	Electrónico pedidos de los clientes	La falta de líneas telefónicas (si el tiempo, accidente, el sabotaje, la incompetencia)	La operación puede ser lento, pero no ha fallado en 5 años	arreglos personales fuertes con los compradores por lo que la llamada móvil es un recurso		2	3
TN2	Electrónico pedidos de los clientes	La corrupción de datos durante la transferencia	La intervención de personas no autorizadas	Grandes variaciones de los volúmenes planificados le pedirá confirmación		2	2
TN3	Levantamiento procesamiento de pedidos de paquete de la casa	Mal funcionamiento de la transferencia de datos	La interrupción de la operación de limpieza / embalaje que lleva a pérdida importante, la escasez de productos y el tiempo de inactividad	vivienda Secure, tamperevident para equipos	La entrada manual retrasará la operación de embalaje en un grado inaceptable	4	4
TN4	El aumento de la carga del vehículo y documentos de entrega	Corrupción de datos	Las principales sanciones escala de los envíos rechazados		transportistas contratados con pocas probabilidades de discrepancias nota	2	3
TN5	UAV monitoreo de los cultivos	Cámaras y sensores fallan en detectar problemas emergentes	El control remoto de dispositivo puede ser asumida por los actores maliciosos	actualizaciones de software instalados de rutina	Tanto daño causado y el robo del dispositivo podría ser incentivos para la negligencia	3	2
TN6	sistema de registros de finca equipo	Pública de adquisición de un rescate por parte de delincuentes	El acceso remoto por los directores a través de Internet ofrece oportunidades para los delincuentes	back-up diario independiente reduciría las pérdidas	Clave para la práctica operativa y acreditación externa	2	2
TN7	Sistemas de control industrial	Sabotaje de controles electrónicos	Alto costo instrumentos altamente sofisticados no se pueden duplicar, por lo que no funcionamiento = no productivo	Actualización y mantenimiento es riguroso	ingeniero de servicio contratado en la llamada 24/7	1	5

Figura A.6 - priorización de amenazas



Comentario

1. La empresa ha adoptado plenamente 'fabricación totalmente integrado' como su camino hacia la eficiencia y el servicio al cliente, pero todavía no es plenamente consciente de las vulnerabilidades que están implicados. La consultoría especialista en seguridad de la información se ha contraído más para completar la evaluación de amenazas y recomendar controles proporcionados.

2. Siempre que sea posible, los sistemas duplicados son para ser operado hasta la finalización de la evaluación.

3. Apoyo y asesoramiento de ncsc.gov.uk se utiliza para aumentar la conciencia entre los contratistas principales y personal de confianza.

4. Revisión que tendrá lugar en un mes.

Anexo B (informativo)

Las fuentes de información e inteligencia sobre riesgos emergentes al suministro de alimentos

B.1 Generalidades

La Organización Mundial de la Salud (a través de INFOSAN) y la Organización para la Agricultura y la Alimentación (a través de EMPRES y el SMIA) de las Naciones Unidas para coordinar los esfuerzos globales para identificar nuevos riesgos y las medidas de control Promulgar para minimizar su impacto.

Que difunden información a las organizaciones nacionales de alimentos como la Food Standards Agency en el Reino Unido. Estas organizaciones nacionales de alimentos pueden ponerlo a disposición de las empresas alimentarias, normalmente a través de asociaciones de comercio, pero en realidad es un proceso de 2 vías.

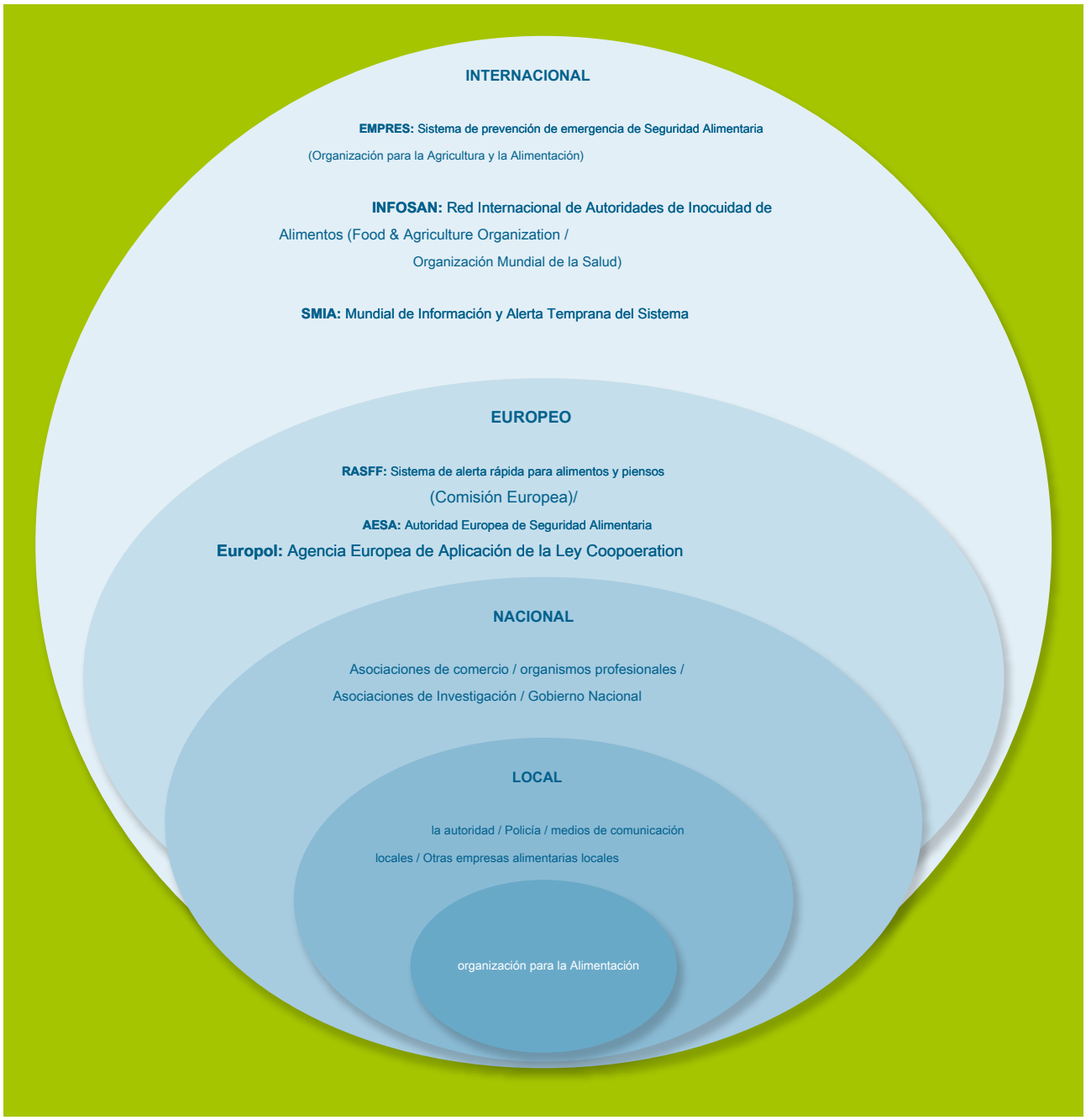
***NOTA** Los servicios de suscripción que proporcionan información útil también incluyen:*

- *HorizonScan que supervisa las cuestiones globales de integridad de los alimentos, ver: https://horizon-scan.fera.co.uk/;*
- *Fraude de alimentos de base de datos de la Convención de la Farmacopea de Estados Unidos, ver: https://www.foodfraud.org/;*
- *US-CERT - Estados Unidos ordenador Preparación del equipo ver https://www.us-cert.gov/.*

B.2 Información y los niveles de inteligencia

Figura B.1 ilustra la difusión mundial y el intercambio de información e inteligencia sobre los riesgos a los alimentos que pueden ser usados para actualizar las evaluaciones TACCP emergente. Cinco niveles se pueden utilizar para describir los diferentes niveles de intercambio de información, siendo 1 el más bajo y 5 el más alto: Nivel 1 - Organización para la Alimentación; Nivel 2 - Local; Nivel 3 - Nacional; Nivel 4 - Europeo; Nivel 5 - Internacional.

Figura B.1 - difusión mundial de información e inteligencia sobre los riesgos a la alimentación emergente que puede ser utilizado para las evaluaciones de actualización TACCP



***NOTA** Para más información sobre estas fuentes internacionales se puede encontrar en la siguiente: INFOSAN http: // www. who.int/foodsafety/areas_work/infosan/en/ [35], EMPRES http://www.fao.org/foodchain/empres-prevention-andearly-warning/en/ [36] y GIEWS http: // www. fao.org/giews/english/index.htm [37].*

Anexo C (informativo)

Enfoques complementarios a la protección de alimentos y bebidas

C.1 CARVER + Amortiguación

CARVER + Shock es una herramienta de priorización ofensiva que ha sido adaptado para su uso en el sector de la comida americana. Al igual que TACCP, Carver + choque implica una organización de juego 'Equipo Rojo', donde los miembros del equipo se ponen en el lugar del atacante potencial y preguntar:

Si quería causar daño, o hacer más dinero, o publicidad de ganancia, o tomar ventaja de la situación de otra manera:

- ¿Que debería hacer?
- Cuando lo haría?
- Cuando lo haría?

En efecto utilizan los militares herramienta para juzgar la orientación debilidades mediante la evaluación de sus:

C riticality

UN ccesibilidad

R ecognizability

V ulnerabilidad

mi fecto

R ecoverability

Más información sobre CARVER + Shock es disponible de Carver + Primer Choque [38].

plan de acción de 5 puntos C.2 UE

En respuesta al fraude de la carne de caballo en 2013, la Comisión Europea estableció en su lugar el plan siguiente punto 5 [39].

1) Desarrollar sinergias entre las fuerzas
   autoridades, garantizan un rápido intercambio de información sobre violaciónes intencionales de las reglas de la cadena alimentaria, promover la participación de Europol en las investigaciones.

2) Asegúrese de que las normas sobre pasaportes para caballos se hacen cumplir
   correctamente, que los pasaportes se entregan sólo por las autoridades competentes y que las bases de datos nacionales se crean.

3) Exigir que las sanciones financieras por intencional
   violaciónes de las normas de la cadena alimentaria se establecerán a niveles suficientemente disuasorias, y que los planes de control de los Estados miembros incluyen controles sin previo aviso.

4) Adoptar normas de etiquetado de origen obligatorio de la carne
   (Oveja, cabra, cerdo, aves de corral, caballo, conejo, etc.) y entregar un informe en el otoño de 2013 sobre la posible ampliación de etiquetado de origen obligatorio a todo tipo de carne utilizada como ingrediente en los alimentos.

5) Presente y evaluar los resultados de los controles
   Actualmente lleva a cabo en los países de la UE.

C.3 Reino Unido Alimentos y bebidas Federación

El Reino Unido Alimentos y bebidas (FDF) Guía de Federación el 'autenticidad Alimentación: cinco pasos para ayudar a proteger su negocio de fraude alimentario [40], la continuación de la guía del FDF 'Sostenible Sourcing: cinco medidas para la gestión de riesgos de la cadena de suministro'[32] y proporciona información sobre:

1) mapeo de la cadena de suministro;
2) la identificación de impactos, riesgos y oportunidades;
3) evaluación y priorización de sus hallazgos;
4) la creación de un plan de acción; y
5) la implementación, el seguimiento, la revisión y la comunicación.

Anexo D (informativo)

10 pasos a la seguridad cibernética: Un responsabilidad a nivel directivo [29)]

NOTA *En este anexo se desarrolló a partir de material fuente proporcionado por el Centro Nacional de Seguridad Cibernética (NSCS).*

D.1 preguntas clave para los CEOs y las juntas

Protección de los activos de información D.1.1 clave es crítica

1) ¿Qué tan seguro estamos de que la mayor parte de nuestra empresa información importante se gestiona y está a salvo de las amenazas informáticas?

2) ¿Está claro que la Junta probable que sea la llave son objetivos?

3) Por qué tenemos una imagen completa y precisa de:

- el impacto en la reputación, la acción de nuestra empresa o de la existencia sensible si la información interna o cliente en poder de la empresa fueron a perderse o ser robado?
- el impacto en el negocio si nuestros servicios en línea fueron interrumpidas por un período corto o sostenido?

D.1.2 La exploración que podrían comprometer nuestra información y por qué

1) ¿Recibimos la inteligencia ordinaria del Jefe Oficial de Información / Jefe de Seguridad sobre quién puede ser la orientación de nuestra empresa, sus métodos y sus motivaciones?

2) Cómo animamos a nuestro personal técnico para entrar en el intercambio de información compartidos con otras empresas de nuestro sector y / oa través de la economía con el fin de punto de referencia, aprender de otros y ayuda a identificar las amenazas emergentes?

D.1.3 gestión proactiva del riesgo cibernético a nivel de la Junta es crítica

1) El valor de impacto del riesgo de cuota de la seguridad cibernética, fusiones, fijación de precios, de reputación, cultura, personal, información, control de procesos, la marca, la tecnología y las finanzas. Estamos seguros de que:

- hemos identificado nuestros activos de información clave y evaluado a fondo su vulnerabilidad al ataque?
- la responsabilidad por el riesgo cibernético se ha asignado de manera adecuada? Es en el registro de riesgos?
- tenemos una política de seguridad de la información escrita en el lugar, que está defendido por nosotros y apoyado a través de la formación del personal regular? Estamos seguros de toda la plantilla entiende y lo sigue?

29) Para más información sobre la seguridad cibernética, véase: https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility [42].

Bibliografía

publicaciones Normas

Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición del documento de referencia (incluyendo cualquier modificación).

Gestión de riesgos

BIP 2153, *La gestión de riesgos de la manera ISO 31000*

BS 31100, *La gestión del riesgo - Código de prácticas y orientaciones para la aplicación de la norma ISO 31000 BS*

BS EN 31010, *La gestión del riesgo - las técnicas de evaluación de riesgos*

BS ISO 31000, *gestión de riesgos - Principios y directrices*

PD ISO / TR 31004, *La gestión de riesgos - Orientación para la implementación de la norma ISO 31000*

Gestión de crisis

BS 11200, *Gestión de crisis - Orientación y buenas prácticas*

Business Continuity Management

BS ISO 22301, *sistemas de gestión de continuidad de negocio - Los requisitos y directrices*

BS ISO 22313, *La sociedad de seguridad - sistemas de gestión de la continuidad del negocio - Orientación*

Cadena de Suministro de Seguridad

BS ISO 28000, *Especificación para sistemas de gestión de seguridad para la cadena de suministro*

BS ISO 28002, *sistemas de seguridad para la gestión de la cadena de suministro - Desarrollo de la capacidad de recuperación en la cadena de suministro - Requisitos con orientación para su uso*

PD CEN / TR 16412, *seguridad de la cadena de suministro (SCS) - Guía de buenas prácticas para los operadores de pequeñas y medianas empresas*

Seguridad de información

BS ISO / IEC 27000, *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción y vocabulario*

BS ISO / IEC 27001, *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos*

otras Normas

BS 10501, *Guía para la implementación de controles de fraude de compras*

BS EN ISO 22000, *sistemas de gestión de la seguridad de los alimentos - Requisitos para cualquier organización en la cadena alimentaria*

Otras publicaciones y sitios web

[1] Codex Alimentarius. *CODEX CAC / RCP 1-1969: Principios generales de higiene de los alimentos.* Roma: Codex Alimentarius, 2003.

[2] CENTRO DE SEGURIDAD National Cyber. Glosario. Disponible a partir de: https://www.ncsc.gov.uk/glossary [vista de julio de 2017].

[3] Food Standards Agency. Disponible en: https: // www.food.gov.uk/enforcement/the-national-foodcrime-unit/what-is-food-crime-and-food- [vista de julio de 2017].

[4] Base de Datos de Fraude de Alimentos de los Estados Unidos Convención de la Farmacopea. Disponible a partir de: http://www.foodfraud.org/ [vista de julio de 2017].

[5] BBC. ' *plástica del arroz' secuestrado en Nigeria.* BBC, 2016. Disponible en: http://www.bbc.co.uk/news/worldafrica-38391998 [vista de julio de 2017].

[6] OLIVA TIMES aceite. *Italia 33 detenciones acusados de fraude aceite de oliva.* Aceite de Oliva Times, 2017. Disponible en: https: // www.oliveoiltimes.com/olive-oil-business/italy-arrests33-accused-olive-oil-fraud/55364 [vista de julio de 2017].

[7] OLIVA TIMES aceite. *Brasil revela el fraude generalizado aceite de oliva.* Aceite de Oliva Times, 2017. Disponible en: https: // www.oliveoiltimes.com/olive-oil-business/brazil-revealswidespread-olive-oil-fraud/56395 [vista de julio de 2017].

[8] EURO WEEKLY NEWS. *Policía destape importante fraude alimentario carne de vacuno en España.* Noticias Euro Weekly, 2017. Disponible en: https://www.euroweeklynews.com/3.0.15/news/ de euros a la semana-noticias / España-noticias-en-Inglés / 144405-

policía-destape-importante-beef-comida-fraude-en-España [vista de julio de 2017].

[9] ANTONY Gitonga. *Naivasha vendedores ambulantes que utilizan formol para conservar la leche.* Estándar de papel. Disponible a partir de: http://www.standardmedia.co.ke/ artículo / 2000107380 / Naivasha-vendedores-usando-formalina topreserve leche [vista de julio de 2017].

[10] ORGANIZACIÓN MUNDIAL DE LA SALUD Y ORGANIZACIÓN DE LA ALIMENTACIÓN Y LA AGRICULTURA las Naciones Unidas. *aspectos toxicológicos de la melamina y ácido cianúrico: Informe de una reunión de expertos en colaboración con la FAO.* La OMS y la FAO, 2009. Disponible en: http://www.who.int/foodsafety/fs_management/ Exec_Summary_melamine.pdf, [vista de julio de 2017].

[11] de la Convención de la Farmacopea de los Estados Unidos. *fraude alimentario base de datos versión 2.0.* Disponible mediante suscripción en: http://www.foodfraud.org/#/food-fraud-databaseversion-20, [vista de julio de 2017].

[12] Food Standards Agency. *Actualización sobre la manipulación maliciosa con pan Kingsmill.* Food Standards Agency, 2006. Disponible en: http: // webarchive. nationalarchives.gov.uk/20120206100416/http://food. gov.uk/news/newsarchive/2006/dec/kingsmill [vista de julio de 2017].

[13] TOROK, THOMAS J. MD, Tauxe, ROBERT V. MD, MPH, WISE, ROBERT P. MD, MPH; Livengood, JOHN R MD, SOKOLOW, ROBERT, MAUVAIS, STEVEN, BIRKNESS, Kristen A, Skeels, MICHAEL R PhD, MPH, Horan, MPH JOHN M MD, Foster, LAURENCE R, MD, MPH.
Un gran brote en la comunidad de salmonelosis causada por la contaminación intencional de las barras de ensaladas restaurante.
American Medical Association, 1997. Disponible en: http://www.cdc.gov/phlp/docs/forensic_epidemiology/% 20Materials adicionales / Artículos / Torok% 20et% 20al.pdf [vista de julio de 2017].

[14] Q LOS ALIMENTOS. *La manipulación de alimentos: [1989] cristal en alimentos para bebés.* Alemania. Disponible en: http: //www.qfood. eu / 2014/03/1989-vidrio-en-alimentos para bebés / [vista de julio de 2017].

[15] ORR, James. *Chantajista encarcelado por amenazas de bomba Tesco.* The Guardian, 2008. Disponible en: http: // www.theguardian.com/uk/2008/jan/28/ukcrime [vista de julio de 2017].

[16] MURRAY, KEVIN D. *escuchas electrónicas y espionaje industrial.* Nueva York: Murray Associates. Disponible en: https: // contraespionaje. worldsecuresystems.com/tscm-the-missing-businessschool-course.html [vista de julio de 2017].

[17] Gillam, CAREY. *Mujer china arrestado en complot para robar la tecnología de maíz de Estados Unidos.* Kansas City: Grainews. Disponible a partir de: http://www.grainews.ca/daily/chinesewoman-arrested-in-plot-to-steal-us-corn-technology [vista de julio de 2017].

[18] INFORME La falsificación. *Cómo identificar los vodkas de falsificación de Glen.* Alejandría, 2014. Disponible en: http://thecounterfeitreport.com/product/322/ [vista de julio de 2017].

[19] NewsCore. *incursiones en alta mar aparecen los vinos de la cala falsa australiano Jacob.* Australia, 2011. Disponible en: http://www.news.com.au/finance/offshoreraids-turn-up-fake-aussie-jacobs-creek-wines/storye6frfm1i- [vista de julio de 2017].

[20] El fraude financiero ACCIÓN Reino Unido. *Restaurantes y comensales dirigidos en la nueva estafa.* Londres. Disponible a partir de: http://www.financialfraudaction.org.uk/cms/assets/1/ estafa% 20alert% 20-% 20restaurants% 20web% 20% 20doc.pdf enlace [vista de julio de 2017].

[21] Nacional de Fraude AUTORIDAD. *indicador de fraude anual.* Autoridad Nacional de Fraude, 2013. Disponible en: https://www.gov.uk/government/uploads/system/ uploads / attachment_data / archivo / 206552 / NFA-anual-fraudindicator-2013.pdf [vista de julio de 2017].

[22] SMITH, MATT. *Ciber criminales usan hackeado Deliveroo cuentas para pedir comida en las tarjetas de las víctimas.* Daily Telegraph, 2016. Disponible en: https://businessreporter.co.uk/2016/11/23/cyber-criminals-use-hackeddeliveroo-accounts-order-foo [Julio 2017].

[23] Associated Press. *con sede en Michigan Biggby café informa incumplimiento de base de datos, es posible robo de información de los clientes.* Empresa canadiense, 2015. Disponible en: http://www.canadianbusiness.com/business-news/-Biggby-menaje para informes basados en Michigan databasebreach-posible-robo-de-cliente-información [vista de julio de 2017].

[24] FEDERAL Oficina de Investigación CYBER división. *PIN Número 160331-001 Smart Farming Puede Aumentar cibernético se dirigen específicamente al de Estados Unidos Agricultura y la Alimentación Sector 3* 1. marzo de 2016. Disponible en: https://info.publicintelligence.net/FBISmartFarmHacking.pdf [vista de julio de 2017].

[25] CENTRO NACIONAL CIBERSEGURIDAD y nacionales ORGANISMO crimen. *La amenaza cibernética a Reino Unido Empresas.* Disponible a partir de: https://www.ncsc.gov.uk/news/ NCSC-y-NCA-amenaza-informe-provee de profundidad analysisevolving-amenaza [vista de julio de 2017].

[26] Centro para la Protección de la infraestructura nacional. *Personal de Seguridad.* Londres: IREC. Disponible a partir de: http://www.cpni.gov.uk/advice/ Personal-seguridad1 / [vista de julio de 2017].

[27] CENTRO DE SEGURIDAD National Cyber. *10 Pasos para la seguridad cibernética.* NCSC, 2016. Disponible en: https: // www.ncsc.gov.uk/guidance/10-steps-cyber-security [vista de julio de 2017].

[28] CENTRO DE SEGURIDAD National Cyber. *Contraseña Orientación: La simplificación de su enfoque.* Disponible a partir de: https://www.ncsc.gov.uk/guidance/password-guidancesimplifying-your-approach [vista de julio de 2017].

[29] Gobierno de SM. *Fundamentos cibernéticos - Proteja su empresa contra las amenazas informáticas.* Disponible en: https: // www.cyberaware.gov.uk/cyberessentials/ [vista de julio de 2017].

[30] Centro para la Protección de la infraestructura nacional. *gestión integral de riesgos de trabajo (Homero).* Londres: IREC, 2012. Disponible en: http://www.cpni.gov.uk/advice/Personnel-security1/ cuadrangular / [vista de julio de 2017].

[31] Centro para la Protección de la infraestructura nacional. El desarrollo de una cultura de seguridad de Londres: IREC https://www.cpni.gov.uk/developingsecurity-culture [vista de julio de 2017].

[32] CREST. Disponible en: http: //www.crest-approved. org / [vista de julio de 2017].

[33] Información de Seguridad de asociación para compartir cibernético (CISP) Disponible a partir https://www.ncsc.gov.uk/cisp [vista de agosto de 2017].

[34] SCOTTISH Gobierno y FOOD Standards Agency. *Peritaje grupo asesor de las lecciones que se pueden aprender del incidente 2.013 carne de caballo.* 2013. Disponible en: http://www.scotland.gov.uk/ Recursos / 0043 / 00437268.pdf [vista de julio de 2017].

[35] World Health Organization. *Red Internacional de Autoridades de Inocuidad de Alimentos (INFOSAN).* Disponible de: http://www.who.int/foodsafety/areas_work/ INFOSAN / es / [Vista de julio de 2017].

[36] ORGANIZACIÓN AGRICULTURA Y LA ALIMENTACIÓN DE las Naciones Unidas. *Sistema de prevención de emergencia (EMPRES).* Disponible de: http://www.fao.org/ foodchain / empres-prevención-y-alerta temprana / es / [Vista de julio de 2017].

[37] INFORMACIÓN GLOBAL sistema de advertencia y (SMIA). Disponible de: http://www.fao.org/ SMIA / Inglés / index.htm [Vista de julio de 2017].

[38] Food and Drug Administration. *Carver + choque Primer - Una visión general del método de Carver, más de choque para las evaluaciones de vulnerabilidad del sector alimentario.* FDA, 2009. Disponible a partir de: http://www.fda.gov/downloads/ Alimentos / FoodDefense / FoodDefensePrograms / UCM376929. pdf [vista de julio de 2017].

[39] ALIMENTOS Y BEBIDAS FEDERACIÓN. *autenticidad de los alimentos: Cinco pasos para ayudar a proteger su empresa contra el fraude alimentario.* Londres: FDF, 2013. Disponible en: https: // www. fdf.org.uk/food-authenticity.aspx [vista de julio de 2017].

[40] ALIMENTACIÓN Y BEBIDA federación. *abastecimiento sostenible: cinco medidas para la gestión de riesgo de la cadena de suministro.* Londres: Londres: FDF, 2014. Disponible en: http: // www.fdf.org.uk/sustainable-sourcing.aspx [vista de julio de 2017].

[41] CENTRO DE SEGURIDAD National Cyber. *10 Pasos: Una responsabilidad a nivel directivo.* Disponible en: https: // www. ncsc.gov.uk/guidance/10-steps-board-level-responsibility [vista de julio de 2017].

[42] CENTRO DE SEGURIDAD National Cyber. *10 pasos: a nivel de placa responsabilidad.* NCSC, 2016. Disponible en: https://www.ncsc.gov.uk/guidance/10-steps-board-levelresponsibility [vista de julio de 2017].

Otras lecturas

BRC Norma Mundial de Seguridad Alimentaria. Consorcio Británico de venta al público.

British Retail Consortium (BRC). *Cyber Security Toolkit: Una guía para los minoristas.* Disponible en: https: // final.pdf brc.org.uk/media/120731/brc-cyber-security-toolkit_ [vista de julio de 2017].

Centro para la Protección de la infraestructura nacional. *Productos y servicios.* Disponible a partir de: http://www.cpni.gov.uk/advice/ [vista de julio de 2017].

COMISIÓN EUROPEA. http://ec.europa.eu/ DGS / health_consumer / Dyna / consumervoice / create_ cv.cfm? cv_id = 891

Food Standards Agency. *Principios para la prevención y respuesta a incidentes de alimentos.* FSA, 2007. Disponible en: http://multimedia.food.gov.uk/multimedia/pdfs/ taskforcefactsheet23mar07.pdf [vista de julio de 2017].

INSTITUTO DE ALIMENTOS ciencia y tecnología. *Buenas prácticas de fabricación: Una guía para su gestión responsable.* Wiley-Blackwell, 2013.

El servicio de seguridad MI5. *nivel de amenaza actual en el Reino Unido.* Disponible a partir de: www.mi5.gov.uk [vista de julio de 2017].

CENTRO NACIONAL CIBERSEGURIDAD. *Guia.* Disponible a partir de: https://www.ncsc.gov.uk/guidance [vista de julio de 2017].

ORGANIZACIÓN MUNDIAL DE LA SALUD. *amenazas terroristas a la alimentación. Directrices para el establecimiento y fortalecimiento de los sistemas de prevención y respuesta.* Cuestiones de Seguridad Alimentaria (OMS), 2008.

INTERPOL. *Operación opson.* Disponible en: http: // www.interpol.int/Crime-areas/Trafficking-in-illicitgoods-and-counterfeiting/Operations/Operations/ Operación-opson [vista de julio de 2017].

EUROPAL y la INTERPOL. *Operación opson III 2013: Orientación de los productos alimenticios falsificados y de baja calidad.* Disponible a partir de: http://www.ipo.gov.uk/ipenforce-opson. pdf [vista de julio de 2017].

CIO de IDG (International Data Group - Global) 5 pasos para responder a una violación de la seguridad. Disponible a partir de: https://www.cio.com.au/article/580908/5-steps-respondsecurity-breach/ [vista de agosto de 2017].

CampdenBRI Directriz 72 TACCP (Evaluación de amenazas y Puntos Críticos de Control) - Una guía práctica.

British Standards Institution (BSI)

BSI es el organismo nacional independiente responsable de la preparación de las normas británicas y otras publicaciones relacionadas con las normas, información y servicios. Presenta la vista del Reino Unido sobre las normas en Europa y en el ámbito internacional.

BSI se incorpora por la carta real. British Standards y otros productos de normalización son publicados por BSI Normas Limited.

Las revisiones

British Standards y pasar se actualizan periódicamente mediante revisión o modificación. Los usuarios de British Standards y pase deberán asegurarse de que poseen las últimas modificaciones o ediciones.

Es el objetivo constante de BSI para mejorar la calidad de nuestros productos y servicios. Agradeceríamos si alguien encontrar una imprecisión o ambigüedad durante el uso de los estándares británicos informaría al secretario del comité técnico responsable, la identidad de los que se puede encontrar en la cubierta interior delantera. Del mismo modo para pasar, por favor notifique a las partidas del balance de Servicio al Cliente.

Tel: +44 (0) 845 086 9001

BSI ofrece a los miembros BSI Participantes permanentemente un servicio de actualización individuo llamado PLUS que garantiza que los suscriptores reciben automáticamente las últimas ediciones de las normas británicas y aprobar.

Tel: +44 (0) 845 086 9001 E-mail: plus@bsigroup.com

normas de compra

Usted puede comprar versiones PDF y copia impresa de las normas directamente utilizando una tarjeta de crédito de la tienda de BSI en el sitio web **www.bsigroup.com/shop.** Además todos los pedidos de publicaciones estándares BSI, internacionales y extranjeras pueden dirigirse a las partidas del balance de Servicio al Cliente.

Tel: +44 (0) 845 086 9001 E-mail: orders@bsigroup.com

En respuesta a los pedidos de los estándares internacionales, BSI suministrará la implementación estándar británico de la norma internacional pertinente, a menos que se solicite lo contrario.

Información sobre las normas

BSI ofrece una amplia gama de información sobre las normas nacionales, europeas e internacionales a través de su Centro de Conocimiento.

Tel: +44 (0) 20 8996 7004 Correo electrónico: knowledgecentre@bsigroup.com

BSI miembros suscriptores se mantienen al día con la evolución de las normas y recibir importantes descuentos en el precio de compra de las normas. Para más detalles de estos y otros beneficios de contactos de Administración de miembro.

Tel: +44 (0) 845 086 9001 E-mail: membership@bsigroup.com

Información sobre el acceso en línea a los estándares británicos y pasar a través de British Standards Online se puede encontrar en **http://shop.bsigroup.com/bsol**

Más información sobre British Standards está disponible en la web de BSI en **www.bsigroup.com/standards**

Derechos de autor

Tel: +44 (0) 20 8996 7070 Correo electrónico: copyright@bsigroup.com

BSI, 389 Chiswick High Road
Londres W4 4AL Reino Unido

www.bsigroup.com

ISBN 978-0-580-98099-2