2020

Informe de recomendación, marco colaborativo de trabajo Israel - Costa Rica

MICITT-DGD-INF-023-2020

Departamento de Respuesta a Incidentes de Seguridad Informática

MICITT-DGD-INF-023-2020

	Elaborado	**Elaborado**	**Supervisado y Autorizado**
Nombre	Elder Briceño Mendoza	Edgar Mora Reyes	Jorge Mora Flores
Puesto	Analista de Ciberseguridad	Analista de Ciberseguridad	Director de Gobernanza Digital
Firma	ELDER ALONSO BRICEÑO MENDOZA (FIRMA) Firmado digitalmente por ELDER ALONSO BRICEÑO MENDOZA (FIRMA) Fecha: 2020.04.20 12:04:48 -06'00'		MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES Firmado digitalmente por JORGE EMILIO MORA FLORES (FIRMA) Motivo: Aprobación y visto bueno del informe Fecha: 2020.04.27 17:30:23 -06'00'

Firmado por EDGAR MORA REYES (FIRMA)
PERSONA FISICA, CPF-01-0878-0675. Fecha declarada: 20/04/2020 12:08 p. m.
Esta representación visual no es una fuente de confianza, valide siempre la firma.

Departamento de Respuesta a Incidentes de Seguridad Informática
CSIRT-CR
csirt@micitt.go.cr
Teléfono 2211-1251

Tabla de contenido

Qué es la Ciberseguridad 3
Alcances y competencias del CSIRT-CR 4
Impacto de la Ciberseguridad en las instituciones y los países. 7
Amenazas comunes a las que se enfrenta el país. 11
Realidad de Costa Rica 15
Caso de Israel y su posicionamiento en el tema 17
Beneficios del trabajo en conjunto con Israel para el MICITT y Costa Rica. 20
Bibliografía 22

Qué es la Ciberseguridad

De acuerdo con la UIT (Unión Internacional de Telecomunicaciones) la Ciberseguridad se define como:

"*El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber entorno. Las propiedades de seguridad incluyen una o más de las siguientes:*

- *Disponibilidad;*
- *Integridad, que puede incluir la autenticidad y el no repudio;*
- *Confidencialidad."*

Actualmente las instituciones tanto gubernamentales como empresas privadas necesitan tener sistemas digitales, por lo que el tema de ciberseguridad se vuelve crucial para el manejo y protección de la información ante amenazas.

No solo se necesita contar en el hardware adecuado, también es necesario contar con las políticas y protocolos a seguir para asegurar de manera integral todo el entorno organizacional y proteger a los usuarios.

Alcances y competencias del CSIRT-CR

El Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR es creado mediante el decreto Nº 37052-MICIT en el cual por medio del artículo 2º se definen los objetivos del CSIRT-CR:

- Promover a nivel nacional la cultura de la seguridad cibernética e informática.
- Coordinar, a nivel nacional acciones que permitan el mejoramiento general de la seguridad cibernética e informática.
- Apoyar a las autoridades administrativas y judiciales en los casos que corresponda para la investigación y procesamiento de perpetradores de delitos cibernéticos e informáticos.
- Coordinar con el Comité Interamericano contra el terrorismo (CICTE), y otras entidades nacionales e internacionales sobre el diseño y aplicación de políticas, estrategias y lineamientos en la adquisición de bienes y servicios en materia de la seguridad de las tecnologías de la información y la comunicación, con los estándares que observen las normativas vigentes internacionales para la implementación y/o aplicación en el sector público.
- Incentivar, orientar y promover las iniciativas públicas y privadas conducentes a lograr un adecuado desarrollo del país en el campo de la seguridad de las tecnologías de la información y la comunicación, esfuerzos orientados a lograr una mayor protección del ciudadano.
- Promover la adopción de políticas públicas que promuevan la mayor eficiencia y eficacia en los recursos informáticos de las entidades públicas.

- Promover y velar por el establecimiento de planes de contingencia en materia de seguridad de las tecnologías de la información y la comunicación en el sector público.
- Proponer las guías para la evaluación de los programas interinstitucionales en materia de seguridad de tecnologías de la información y la comunicación.
- Asesorar y proponer a la Presidencia de la República la normativa en materia de seguridad de las tecnologías de la información y la comunicación, que se requiera para el cumplimiento de las políticas públicas en la materia.
- Promover proyectos y actividades de investigación, capacitación y difusión en materia de seguridad de tecnologías de la información y la comunicación.
- Impulsar entre las entidades públicas y privadas el desarrollo y ejecución de políticas y estrategias nacionales en el campo de la seguridad de las tecnologías de la información y la comunicación.

Además, en el artículo 5º-Serán funciones del CSIRT-CR:

- Asesorar al Consejo Director del CSIRT- CR en el diseño de políticas, estrategias y acciones en materia de seguridad cibernética e informática, así como elaborar programas nacionales en materia de seguridad de tecnologías de la información y la comunicación.
- Promover la implementación de políticas y estrategias de seguridad cibernética de las instituciones gubernamentales, tomando en cuenta los estándares internacionales.

- Elaborar un plan de trabajo anual con las prioridades y actividades a desarrollar en materia de seguridad cibernética e informática para las instituciones gubernamentales.
- Elaborar informes de incidentes para las diferentes instituciones gubernamentales que lo soliciten.
- Promover y ejecutar acciones de capacitación en materia de seguridad cibernética e informática con expertos nacionales e internacionales.

Actualmente el CSIRT nacional de Costa Rica se encuentra constituido por 4 profesionales que atienden y desarrollan actividades para el sector de gobierno central principalmente.

Durante la ejecución de sus labores ha visto la necesidad de formar vías de comunicación como una primera actividad, para permitir una comunicación más fluida y directas con las entidades de gobierno y el Departamento de Respuesta a Incidentes de Informática (DRII o CSIRT)

Es así como el CSIRT-CR se ha trabajado proactivamente para crear la primera red de enlaces de ciberseguridad que ha logrado generar una importante vía de comunicación para mejorar la protección de las instituciones de gobierno central, permitiendo importantes canales directos para el envío de información importante para la protección, como las alertas técnicas, convocatorias para capacitación de funcionarios o alguna otra noticia importante relacionada con el tema de la ciberseguridad.

Impacto de la Ciberseguridad en las instituciones y los países.

Tanto Costa Rica, como los países de la zona están experimentando un crecimiento económico y cada vez hacen más uso de las tecnologías para, por un lado, desarrollar sus negocios y acercarse a una mayor cantidad de demandantes de productos y servicios y por otro, para disminuir costos en sus procesos productivos y volverse más competitivos en los actuales mercados.

Las organizaciones estatales, son otro tipo de organización que, aunque no se dedique a la rentabilidad de sus procesos como lo puede hacer el sector productivo, requiere de la tecnología como una herramienta para ejecutar sus funciones y cumplir con las necesidades de los habitantes para el bienestar de todos y dichas tecnologías tienen la posibilidad de agrupar a las organizaciones para ir en búsqueda de soluciones integradoras, para cumplir con los objetivos del estado digitalizado, para la gobernanza digital y para ofrecer trámites simplificados para los usuarios.

En todo el mundo se viene dando la digitalización de la economía, lo que hacer ver comportamientos como los anteriormente mencionados.

El Foro Económico Mundial en una de sus publicaciones realiza una muestra del estado de la tecnología para varios países, incluido Costa Rica. En dicha publicación denota el crecimiento de la tecnología a pesar de las adversas condiciones económicas del país y se indica que el sector de telefonía móvil ha demostrado en el tiempo un gran crecimiento sobre la telefonía fija, aunque con un menor rendimiento en cuanto a datos, pero es una solución más asequible por parte de la población. Esto

deja entrever la necesidad de servicios digitales y la necesidad de inversión en plataforma tecnológica con costos más competitivos, en caso contrario, el desarrollo del país se verá frenado.

Todo este crecimiento demostrado, lleva a su vez a una nueva conclusión: A mayor cobertura tecnológica, mayor exposición a ataques cibernéticos. Como lo afirma el Foro Económico mundial “Con todos estos acontecimientos, los riesgos cibernéticos son cada vez más preocupantes y se están convirtiendo en un factor de mayores consideraciones en seguridad y formulación de políticas económicas.” (OEA & BID, 2016, p.26)

Se hace evidente el deber de los Estados por proteger su desarrollo tecnológico, sus plataformas, infraestructuras de telecomunicaciones y sistemas de información en todos los sectores públicos y productivos de cada país.

Lo anterior demuestra el rumbo que los países deben tomar para su progreso, la inversión en tecnología y su mantenimiento.

Un tipo de inversión en seguridad cibernética que se puede hacer es el de la generación de alianzas en entre países y la transferencia de tecnologías de ciberseguridad que se pueda lograr de dichas alianzas.

Así, Israel se presenta como un aliado importante, por su nivel de desarrollo en la protección cibernética y cuenta con una amplia trayectoria en el desarrollo de sistemas

y de estrategias de ciberseguridad para proteger a esta nación de amenazas tanto locales como extranjeras.

Han desarrollado un plan de manera integral que cubre sectores militares, productivos, gubernamentales y civiles del país, lo que implica todo un compendio de conocimientos, técnicas y herramientas que podrán ser un ejemplo a seguir en nuestro país. Por lo que, un convenio para trabajo colaborativo entre Israel y nuestro país puede significar una oportunidad importante de transferencia de conocimiento y tecnología que nos podrá posicionar como un país desarrollado en ciberseguridad y atractivo para la inversión y el desarrollo por su dedicación a la protección de las facilidades necesarias para el desarrollo de las actividades productivas nacionales.

Uno de los puntos importantes para el desarrollo de la resiliencia cibernética de los países es la educación y la concienciación en ciberseguridad, como lo reitera el Foro Económico Mundial: “Una tendencia en seguridad cibernética hoy es la idea de mejorar la higiene cibernética” (OEA & BID, 2016, p.28)

Los países de la zona, incluyendo el nuestro debe de realizar importantes inversiones y esfuerzo continuado en la formación de los habitantes en el tema de ciberseguridad. Es necesario educar a los habitantes y a los usuarios de sistemas, particularmente de gobierno para que sean conscientes de las amenazas que se presentan día a día y de su complejidad creciente para que actúen en consecuencia y sean una de las respuestas ante ciberataques de primera línea.

Igualmente, en el tema de la capacitación, Israel puede ser un ejemplo con sus programas de formación y replicar su experiencia de manera local.

Toda la inversión en ciberseguridad que se pueda ejecutar a nivel nacional será beneficiosa para desarrollar capacidades cibernéticas y una menor propensión a ver afectados los sectores de la nación por los ataques cibernéticos.

En consecuencia, para todos los países del área, la inversión, la transferencia de conocimiento y desarrollo de capacidades y el fortalecimiento de las infraestructuras tecnológicas será un factor clave para su desarrollo y su bienestar.

Amenazas comunes a las que se enfrenta el país.

Las amenazas actualmente vienen en aumento y en diversificación. Se están volviendo más complejas de detectar y combatir.

Todas estas amenazas buscan explotar las distintas vulnerabilidades existentes en las plataformas tecnológicas desarrolladas, poniendo en riesgo las operaciones y la integridad de la información.

Tanto buscan afectar la información, como la disponibilidad de la misma, incluso, afectar los servicios prestados por organizaciones, lo que viene a generar una serie de trastornos importantes en el medio:

- Robo de información
- Afectación de sistemas y hardware
- Pérdida de productividad y competitividad
- Afectación a los usuarios de los servicios

Siendo muy diversos lo daños provocados por la actividad ciberdelincuente, se procede a hacer una clasificación general de las amenazas más comunes en nuestro medio.

Para esto, instituciones como el Instituto Nacional de Ciberseguridad de España (INCIBE) o empresas dedicadas al tema de los antivirus y soluciones de protección de sistemas como Kaspersky, se han dedicado a recolectar y analizar diversas

amenazas y han generado catálogos y descripciones detalladas de distintos ataques informáticos, clasificados entre otros:

Contenido abusivo

- SPAM, corresponde a correos no solicitados que son enviados de forma masiva, con objetivos variados, publicidad, ventas o estafas.
- Ciberacoso
- Contenidos inadecuados, corresponde a material relativo a la violencia, pornografía, xenofobia, etc.

Contenido dañino

- Rootkits, es un tipo de amenaza que es difícil de detectar y que se aloja en partes del sistema operativo, afectando el comportamiento del sistema, desactivando antivirus o robando información.
- Botnets, redes de computadoras creados a partir de software malicioso instalado en los mismos, que pueden ser utilizadas para ataques del tipo DoS o DDoS.
- Troyanos, tipo de malware o amenaza que se instala en equipos y que una vez instalado, habilita otro tipo de amenazas como spam o software no autorizado.
- Downloaders, amenazas que se instalan en el equipo y permiten la instalación de aplicaciones dañinas o peligrosas.

Obtención de información

- Escaneo de redes, es una actividad de sondeo de los equipos de la red para buscar equipos desprotegidos y explotar sus posibles vulnerabilidades.

- Análisis de paquetes, es la interceptación de paquetes de datos en redes de equipos para revisar y obtener su contenido.

Intento de intrusión

- Explotación de vulnerabilidades en hardware/software, usando bases de datos de errores o vulnerabilidades para atacar sistemas o equipos
- Ataques de día cero, es la explotación de fallos que no han sido detectados en dispositivos antes de su liberación.

Intrusión

- Compromiso de cuentas de sistemas, ataque en el se ha conseguido acceso a sistemas mediante cuentas que pueden tener o no privilegios de acceso, que permitirán hacer otros tipos de ataque, como el de obtención de información.
- Inyección SQL, consiste en una intrusión aprovechando deficiencias en la validación de las entradas de los sistemas y ingresar código para evadir la seguridad y acceder a la información para destrucción o robo

Disponibilidad

- Ataques de denegación de servicio DoS, consiste en la saturación de los servicios de información hasta el punto en el que el servicio no es capaz de resolver el volumen de peticiones y queda fuera de servicio.
- Ataques de denegación de servicio distribuido DDoS, corresponde a un ataque del mismo tipo que el DoS, pero de una capacidad mayor.

- Sabotaje, es una amenaza que corresponde a daños intencionales en los sistemas o equipos, como destrucción de hardware o datos para interrumpir servicios a usuarios.

Compromiso de la información

- Robo de credenciales, es el uso de credenciales no autorizadas para el acceso a equipos o a la información.
- Pérdida o daño de la información, esta situación es una amenaza que se puede dar por el daño de dispositivos de almacenamiento o de respaldos de información.
- Ransomware, es una amenaza que corresponde a un software creado para el secuestro de información mediante el cifrado de la misma a cambio de sumas de dinero para la recuperación de la información.

Fraude

- Phishing, es una amenaza común en la que se busca robar la información de usuarios mediante engaños o simulaciones de sitios a los que el usuario tiene acceso.
- Pharming, técnica para la recolección masiva de datos personales o credenciales de usuarios mediante la redirección a sitios falsos.
- Violación de derechos de autor, es la copia ilegal de software para usos no permitidos sin el pago de los debidos costos y derechos.

Realidad de Costa Rica

Actualmente Costa Rica cuenta con:

➔ Decreto ejecutivo 37052-MICITT

En el cual se establece la creación del CSIRT-CR

➔ Ley N° 8968

Protección de la persona frente al tratamiento de sus datos personales

➔ Prodhab

Agencia de protección de datos de los habitantes

➔ Ley N° 9048- reforma de varios artículos

Delitos informáticos y contextos

➔ Contraloría General de la República

Normas técnicas para la gestión y control de las TIC’s

➔ Estrategia Nacional de Ciberseguridad

Desarrollada con ayuda de la OEA en el año 2017

➔ MoU’s y Cooperación internacional

Corea del sur

OEA

CSIRT-Americas

Estonia

Caso de Israel y su posicionamiento en el tema

Israel ha generado una larga trayectoria en el tema de la seguridad física o territorial y en la ciberseguridad. Su situación geográfica lo ha impulsado a generar sistemas para su protección como estado.

Por otro lado, con la adopción y desarrollo de tecnologías para todos sus sectores productivos y sociales viene la necesidad de proteger este otro tipo de infraestructuras. La misma necesidad de protección la tienen el resto de los países, incluido Costa Rica.

Israel, durante el año 2018 hizo una fuerte inversión en tecnología y ha estado trabajando en el desarrollo de un ecosistema tecnológico que incluye a la ciberseguridad como componente esencial.

Según publicación digital de El Economista: “En Israel, operan 400 empresas de ciberseguridad en donde trabajan 13,000 empleados en esta materia. Para Raviv, este es un ecosistema que incluye al gobierno y al ejército israelíes, a la academia y a la iniciativa privada, además de organizaciones internacionales.” (El Economista, 2019)

Dicha inversión implica varios miles de millones de dólares que potencian el desarrollo de tecnologías y la atracción de empresariado tecnológico relacionado con la ciberseguridad.

El anterior extracto demuestra las dimensiones en las que la ciberseguridad se visualiza en Israel y lo anterior, lo hace un modelo de seguridad importante a seguir y replicar en todas sus posibilidades en nuestro país. De ahí la importancia de recibir recursos y conocimiento de parte de este gran aliado que tiene el país.

¿Cómo es posible concentrar en un parque tecnológico de tipo “Sillicon Valley” ubicado en Israel, una cantidad aproximada de 400 empresas dedicadas a la ciberseguridad?

La pregunta se responde en su actitud de desarrollo y apoyo a los emprendimientos locales, a su inversión en la empresa y a su Estrategia Nacional de Ciberdefensa.

El Ministerio de Economía de Israel hace la siguiente referencia que refleja la direcció de Israel en el tema de la tecnología y la ciberseguridad: ““Israel es el centro global para la innovación, ingrediente indispensable de la iniciativa empresarial”, dijo el Netanyahu el jueves en su discurso en el Foro Económico Mundial en Davos, Suiza.” (Min. de Industria y Economía de Israel, 2014)

De lo anterior se puede observar claramente que la fuerza en el tema de ciberseguridad del Estado de Israel se debe al apoyo de las iniciativas de sus profesionales (emprendimientos o *start-ups*) para lograr desarrollar un proyecto y convertirlo en una empresa desarrolladora de productos que dinamizarán su economía. Esto de fijo es una inversión en sus propios habitantes y en su nación. Costa Rica puede tomar con atención este ejemplo para aplicarlo, no solo a la seguridad cibernética sino también a todas las demás actividades productivas.

El posicionamiento de Israel en ciberseguridad no solo se hace evidente en la promoción de iniciativas locales, sino también, en la generación de tecnologías que un uso inmediato y no son simples ideas o prototipos, como lo demuestra la siguiente publicación digital: “El gigante de computadoras HP está instalando ciber seguridad Sure Sense de Israel en su última de la gama de EliteBook y ZBook.” (latamisrael, 2019)

Así, Israel ha desarrollado un inventario de soluciones de seguridad que cubre tanto sistemas de información para la ciberseguridad más tradicionales, como los sistemas complejos con técnicas de inteligencia artificial y aprendizaje profundo entre otros.

Es para nuestro país un asunto de interés estratégico mantener el trabajo en temas de ciberseguridad en colaboración con el estado de Israel por su alto nivel de desarrollo tecnológico gracias a su innovación, la búsqueda de nuevas soluciones que se adapten a las amenazas en cambio constante y por su sistema nacional de la promoción en ciberseguridad y ciberdefensa nacional.

Beneficios del trabajo en conjunto con Israel para el MICITT y Costa Rica.

El estado de Israel cuenta en la actualidad con uno de los mejores programas nacionales de ciberseguridad en el mundo, para proteger todos los sectores de su país, gobierno, empresa, salud, educación, etc. y ha sido desarrollado a través del tiempo para mejorarse y tomar en cuenta los nuevos tipos de amenazas que van surgiendo, por lo que, los programas y actividades de ciberdefensa de Israel están en constante evolución y generando gran cantidad de conocimiento en el área.

El trabajo conjunto con el Estado de Israel, a través de un memorando de entendimiento (MoU), será claramente será beneficioso para adoptar el conocimiento y buenas prácticas logradas a partir de un largo y complejo proceso y ajustarlo a la realidad nacional, con el objetivo de poder elevar el nivel de protección del ciberespacio costarricense en un mundo cada vez más dependiente de la tecnología y ampliamente expuesto a múltiples amenazas cibernéticas.

El tema de la seguridad de la información es un aspecto necesario para considerar, ya que el uso masivo de la tecnología implica el deber de proteger a nuestro país contra ataques cibernéticos sobre las infraestructuras y sistemas tecnológicos locales.

No se trata solamente de contar con tecnología para el beneficio nacional, sino también protegerla de amenazas tanto internas como externas.

La colaboración con Israel nos permitirá estar en contacto con sus metodologías de protección, en la que la preparación mediante procesos de defensa cíclicos es decisiva para una estructura nacional de ciberseguridad robusta y preparada.

La selección de Israel para establecer un convenio de colaboración corresponde con esa búsqueda de fuentes altamente especializadas en el tema de ciberseguridad, que permitirá potenciar nuestras capacidades de ciberdefensa para atender las propias necesidades de protección de sistemas vitales e infraestructuras críticas de Costa Rica.

Bibliografía

INCIBE, 2020, https://www.incibe-cert.es/taxonomia

Kaspersky, 2020, https://latam.kaspersky.com/blog/clasificacion-de-malwares/1608/

El Economista, 2019, https://www.eleconomista.com.mx/tecnologia/Israel-desarrolla-un-Silicon-Valley-de-ciberseguridad-en-Beerseba-20190623-0002.html

ITU, 2010, https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

Ministerio de Industria y Economía de Israel, 2014, https://itrade.gov.il/spain/israel-es-un-centro-mundial-de-innovacion-y-ciberseguridad/

Diario digital Latam Israel, 2019, https://latamisrael.com/las-computadoras-de-hp-vendran-con-seguridad-israeli-integrada-a-partir-de-ahora/