UNIVERSIDAD SAN MARCOS

ESCUELA DE CIENCIAS ADMINISTRATIVAS

LICENCIATURA EN ADMINISTRACIÓN DE EMPRESAS

PROPUESTA DE ACCIONES PARA IMPULSAR LA CULTURA DE CIBERSEGURIDAD EN LA CAJA COSTARRICENSE DE SEGURO SOCIAL, DURANTE EL SEGUNDO SEMESTRE DEL 2023

TRABAJO FINAL DE GRADUACIÓN PRESENTADO PARA OPTAR POR EL GRADO DE LICENCIATURA EN ADMINISTRACIÓN DE EMPRESAS

POSTULANTE:

MARÍA ALEXANDRA SALAZAR RAMÍREZ

SAN JOSÉ, COSTA RICA

MAYO, 2023

UNIVERSIDAD SAN MARCOS

LICENCIATURA EN ADMINISTRACIÓN DE EMPRESAS

TRIBUNAL EXAMINADOR

_____

MBA. María Andrade González

Directora de la Carrera de Administración de Empresas

_____

MBA. Roger Mora Arias

Asesor Técnico y Metodólogo

Declaración Jurada

Yo, María Alexandra Salazar Ramírez, mayor, casada, estudiante de la Carrera de Administración de Empresas, de la Universidad San Marcos, domiciliado en Palmares, Alajuela, portadora de la cédula de identidad número 1-1395 0977, en este acto, debidamente apercibido y entendido de las penas y consecuencias con las que se castiga, en el Código Penal, el delito de perjurio y falso testimonio, ante quienes se constituyen en el Tribunal Examinador de nuestro Trabajo Final de Graduación para optar por el grado académico de Licenciatura en Administración de Empresas, juro solemnemente que este trabajo de investigación denominado: Propuesta de acciones para impulsar la cultura de ciberseguridad en la Caja Costarricense de Seguro Social, durante el segundo semestre del 2023., durante el primer semestre del 2023, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derechos de Autor y Derechos Conexos, número 6 683, del 14 de octubre de 1982 y sus reformas, publicada en La Gaceta número 226, del 25 de noviembre de 1982, incluyendo el numeral 70 de dicha ley que advierte: artículo 70º: Es permitido citar a un autor transcribiendo los pasajes pertinentes siempre que estos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor y de la obra original. Asimismo, quedó advertido que la Universidad San Marcos se reserva del derecho de protocolizar este documento ante Notario Público. En fe de lo anterior firmo en la ciudad de San José, el 12 de mayo del año dos mil veintitrés.

María Alexandra Salazar Ramírez

Cédula 1-1395 0977

Índice de contenidos

Índice de Gráficos

Índice de tablas

Índice de ilustraciones

Resumen ejecutivo

La Caja Costarricense de Seguro Social es la institución gubernamental encargada de la seguridad social en Costa Rica. A través de ella se proporcionan servicios de salud y pensiones a los costarricenses, esto de acuerdo con legislación vigente.

Como es bien conocido, las tecnologías actualmente se encuentran inmersas en todos los procesos de las instituciones, y en la Caja Costarricense del Seguro Social no es la excepción. El aumento de los procesos y la necesidad de automatización de los mismos, ha provocado que la institución migre hacia la digitalización, un ejemplo de ello, es el Sistema Expediente Digital Único en Salud (EDUS), el cual se utiliza para prestar servicios de salud a la población.

Ahora bien, con el fin de realizar todo este proceso tan fuerte de digitalización, asimismo, ser el proveedor de servicios tecnológicos, se tiene la Dirección de Tecnologías de Información y Comunicaciones, la cual es la unidad que se encarga de asumir la prestación de servicios tecnológicos.

A raíz de este auge en las tecnologías que si bien es cierto ha sido de gran aprovechamiento y mejora en la prestación de servicios, se encuentran riesgos, uno de ellos son los ciberataques o las fugas de información a personas no autorizadas. En ese sentido, ha surgido la gran necesidad de fortalecer las plataformas tecnológicas con el fin de asegurar el parque tecnológico y de esta manera evitar que los ciber delincuentes afecten a la institución.

Aunado a lo anterior, y tomando en cuenta que la ciberseguridad no solo se extiende al ámbito de plataforma tecnológica, sino también a las acciones que realizan las personas detrás de los dispositivos electrónicos, se hace necesaria una transformación cultural que permita concientizar a las personas en el uso correcto de las tecnologías y el manejo de la información.

El propósito de este proyecto de graduación es analizar la cultura de ciberseguridad en los usuarios internos de los servicios de tecnologías de información y comunicaciones de la Caja Costarricense de Seguro Social, y de esta manera sugerir una propuesta para fomentar un cambio de mentalidad para el uso seguro de las TIC.

Agradecimiento y dedicatoria

Dedico el presente proyecto de graduación a Dios, quién me da dado las fuerzas, salud y recursos para llevar adelante este proyecto y segunda carrera universitaria.

Un agradecimiento muy especial a mi esposo Steve Rojas Zúñiga por impulsarme a estudiar una segunda carrera, creer en mí y mantenerme en el camino a pesar de todo, sin él esto no hubiera sido posible.

Finalmente, a mis papás quienes han estado siempre a mi lado dándome su amor incondicional.

Capítulo I Introductorio

En virtud de la acelerada digitalización de los procesos en las empresas, se ha visualizado en los últimos años la importancia de tomar medidas de protección con el fin de evitar un ataque cibernético. En ese sentido, podemos observar que en los últimos años se tiene conocimiento de violaciones a la seguridad de dispositivos personales, así como de grandes ciberataques. Estos hechos han preocupado a las instituciones y empresas lo cual ha traído consigo un aumento en las prioridades de una cultura de ciberseguridad; así como la confianza digital de los usuarios internos y externos.

De acuerdo con el Consejo de la Unión Europea, los ciberataques y la ciberdelincuencia cada día aumentan más en el continente Europeo, asimismo, estos ataques cada vez se realizan de manera más especializada. Se estima que esto se seguirá agravando a futuro, esto en virtud de que se calcula que 41 000 millones de dispositivos en todo el mundo estarán conectados a la internet de las cosas de aquí a 2025. Consejo de la Unión Europea. (11 de enero de 2023). Ciberseguridad: cómo combate la UE las amenazas cibernéticas. Recuperado de: https://www.consilium.europa.eu/es/policies/cybersecurity/ .

Siendo que muchos de los ciberataques han sido exitosos debido a algún descuido o desconocimiento humano, ya sea por brindar contraseñas a extraños, atender llamadas desconocidas y dar información personal, se puede analizar que algunas amenazas a la ciberseguridad guardan relación con el comportamiento humano, en consecuencia, aunque existan robustos controles tecnológicos, siempre será necesario educar en ciberseguridad a las personas.

Por lo antes expuesto, es de suma importancia para toda empresa no perder de vista que la transformación digital también supone una transformación en las personas hacia una

cultura de ciberseguridad. Se requiere la generación de un plan de transformación cultural para que el talento humano se haga personal e individualmente responsables de la ciberseguridad, siendo que esta sea parte integral del trabajo, sus hábitos y comportamientos diarios.

Antecedentes

El día 31 de mayo de 2022 en horas de la madrugada la plataforma tecnológica de la Caja Costarricense de Seguro Social se vio afectada por un ataque cibernético, por lo cual se deshabilitaron de manera preventiva los sistemas informáticos, con el fin de proteger la plataforma institucional y la información contenida en las bases de datos, siendo algunos datos considerados como sensibles.

Dicho ciberataque no fue un evento aislado, en los últimos años se ha presentado un incremento exponencial de las ciber amenazas. Este riesgo latente, ha traído consigo que haya un aumento en la necesidad de implementar una cultura de ciberseguridad; así como la confianza digital de los usuarios internos y externos

En virtud de lo anterior, existe una necesidad de realizar una propuesta para el desarrollo de una cultura de ciberseguridad en la Caja Costarricense de Seguro Social, con el fin de reducir los riesgos y ciber amenazas. Lo anterior, tomando en cuenta que los usuarios de las tecnologías en una empresa tienen un rol fundamental en garantizar el éxito de las estrategias de ciberseguridad al cumplir con las prácticas recomendadas de seguridad.

Por medio de la presente investigación se conoce que posterior al ciberataque dicha Dirección ha venido realizando importantes esfuerzos en la aplicación de mejoras y

recomendaciones tanto de entes externos como de nuestra Auditoría Interna para fortalecer la seguridad informática, con los elementos y recursos disponibles hasta este momento.

Por otro lado, la Dirección de Tecnologías de Información y Comunicaciones (DTIC) en conjunto con una firma consultora y como parte del proyecto de diseño e implementación de un Modelo Meta de Gobierno de Tecnologías de Información y Comunicaciones y Gobierno de la Seguridad de la Información, estableció una iniciativa tendiente a desarrollar un Plan Táctico de Ciberseguridad, y a raíz del ciberataque sufrido el 31 de mayo del 2022, esta Dirección consideró conveniente valorar y revisar los esfuerzos que se estaban realizando en esta materia con el objetivo de robustecer el marco de ciberseguridad institucional y mitigar los riesgos para que una situación como la acontecida tenga el menor impacto posible en la prestación de servicios institucionales

Justificación

La la ciberseguridad se compone por tecnología, procesos y personas. (Alan Calder, 2017, sección de ciberseguridad). Es por ello, que es de suma importancia no dejar de lado el componente “persona” para fortalecer la ciberseguridad en cualquier institución. Siendo que la Caja Costarricense de Seguro Social atravesó un año 2022 muy complicado en temas de ciberseguridad y en virtud de mejorar este punto, es de gran importancia que exista una cultura de ciberseguridad en la institución que venga a minimizar este riesgo.

A través del análisis sobre la importancia de una cultura de ciberseguridad en la Caja Costarricense de Seguro Social, se plantea un esfuerzo en aras de lograr la protección de la información ante amenazas y ataques realizados por personas y/o empresas, cuya intención es provocar daños o favorecerse mediante la extracción de datos confidenciales.

Siendo que realizar cambios en cualquier organización tiende a ser una tarea un poco compleja, y en virtud de que establecer esta cultura de ciberseguridad supone un cambio, es necesario el establecimiento de una propuesta que genere una cultura de ciberseguridad en la institución alineada con un manejo adecuado de las resistencias a través del uso de la gestión del cambio organizacional.

Planteamiento del problema

En virtud del ciberataque sufrido por la Caja Costarricense de Seguro Social, el día 31 de mayo de 2022, es necesario realizar una serie de acciones para ordenar y articular los esfuerzos en aras de robustecer el marco de ciberseguridad institucional y mitigar los riesgos de afectar la prestación de servicios institucionales a la población.

En ese sentido, y tomando en cuenta que la ciberseguridad se compone por tecnología, procesos y personas, es importante no solamente robustecer la plataforma tecnológica institucional, sino también que los funcionarios se hagan responsables de la ciberseguridad desde su campo de acción a través de sus hábitos y comportamientos diarios.

De acuerdo con lo anterior, el desarrollo de este proyecto de investigación pretende resolver la problemática planteada en la siguiente interrogante.

¿Cuál es la importancia de una cultura de ciberseguridad en los funcionarios de la Caja Costarricense de Seguro Social y su incidencia en la seguridad informática?

Objetivo general

Analizar la importancia de una cultura de ciberseguridad en los usuarios internos de los servicios de tecnologías de información y comunicaciones de la Caja Costarricense de Seguro

Social, con el fin de sugerir una propuesta de acciones para impulsar la cultura de ciberseguridad en la institución.

Objetivos específicos

- Conocer la importancia de una cultura de ciberseguridad en los usuarios internos de servicios informáticos en la Caja Costarricense de Seguro Social.
- Identificar cuáles son las actividades que se llevan a cabo actualmente en la Caja Costarricense de Seguro Social para fomentar una cultura de ciberseguridad en los usuarios internos de los servicios informáticos.
- Valorar elementos que permitan llevar a cabo una cultura de ciberseguridad en la Caja Costarricense de Seguro Social.
- Proponer un plan de trabajo para el desarrollo de una cultura de ciberseguridad en usuarios internos de los servicios TIC de la Caja Costarricense de Seguro Social, durante el segundo semestre del 2023.

Alcances y limitaciones

La Dirección de Tecnologías de Información y Comunicaciones, es el órgano rector en materia tecnológica de la Caja Costarricense de Seguro Social, está conformada por un despacho el cual tiene adscritas 3 subáreas y cuatro áreas. En ese sentido, es quien debe generar la normativa y directrices en materia de ciberseguridad en la institución.

Siendo que la Caja Costarricense de Seguro Social es una institución que tiene alcance nacional y múltiples sedes de prestación de servicios de salud y pensiones, requiere en el ámbito tecnológico de igual manera un alcance a lo largo y ancho del país, por lo cual se

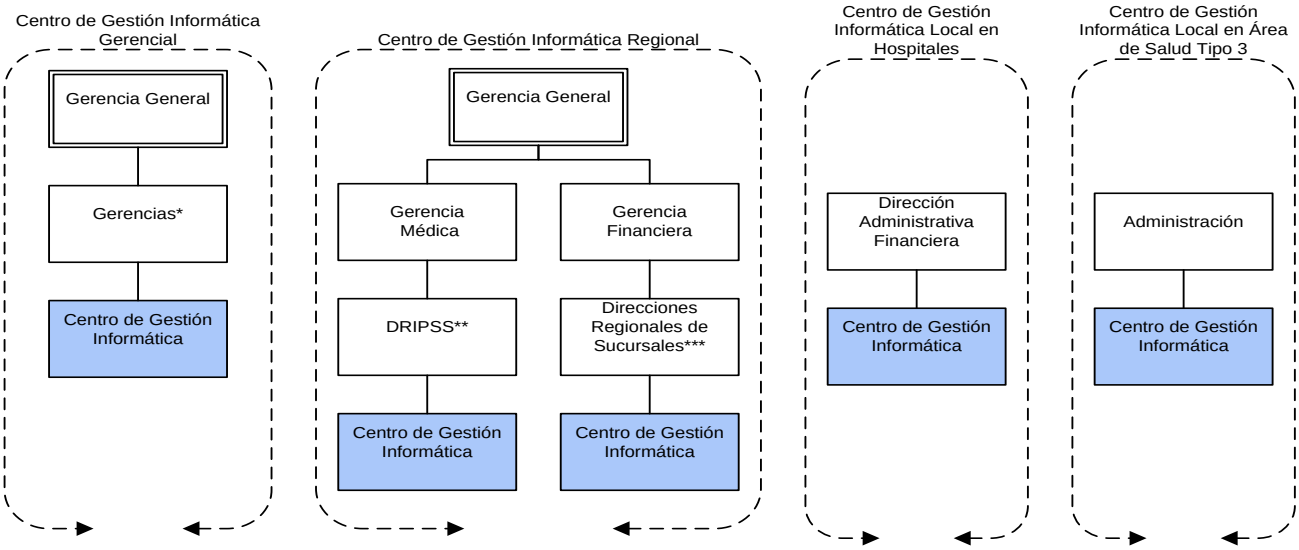
crearon los Centros de Gestión Informática (CGI), por la Junta Directiva en la sesión 7130, artículo 26, celebrada el 27 de mayo de 1997, en la cual textualmente se indicó:

> "Artículo 26: por tanto, con base en las consideraciones precedentes y la recomendación del señor Gerente de la División Administrativa, se acuerda aprobar el Manual de Políticas Institucionales de Desarrollo en Sistemas de Información y el documento Centros de Gestión Informática, según los términos de los documentos que quedan formando parte del expediente original de esta acta".

Según el Modelo de Organización de los Centros de Gestión Informática, los CGI como unidades organizacionales formales están presentes en el ámbito central y se les denomina "Centro de Gestión Informática Gerencial". A nivel regional se encuentran establecidos en las Direcciones de Red Integradas de Prestación de Servicios de Salud y en las Direcciones Regionales de Sucursales. Finalmente, en un ámbito local, se conformaron en los hospitales de la CCSS y las Áreas de Salud Tipo 3. En las Áreas de Salud tipo 1 y 2, se constituyen en actividades sustantivas adscritas a la Administración y no como unidades formales.

Al respecto, los CGI tienen la siguiente estructura organizacional:

Ilustración 1 Estructura Organizacional Centros de Gestión Informática



* Gerencia:Médica, Administrativa, Infraestructura y Tecnologias, Financiera, Logistica y Pensiones
**DRIPSS: Dirección de Red Integrada de Prestación de Servicios de Salud:Central Norte,Central Sur Chorotega,Huetar Norte,Huetar Atlántica,Pacífico Central, Brunca
***Dirección Regional de Sucursales: Atlántica, Brunca, Central, Huetar Norte, Chorotega

Fuente: Caja Costarricense de Seguro Social, Gerencia Administrativa, Dirección de Desarrollo Organizacional. (Octubre 2013). Modelo de Organización de los Centros de Gestión Informática (segunda actualización)

Tomando en cuenta lo antes descrito, la complejidad, el nivel de responsabilidad, de autoridad, los recursos asignados, la afinidad, la interrelación e interdependencia de los procesos, son variables fundamentales que orientan la definición del estatus de los niveles organizacionales.

El análisis se limita al estudio de las importancia de una cultura de ciberseguridad partiendo de información externada por parte de las jefaturas de la Dirección de Tecnologías de Información y Comunicaciones (ente rector) y no a los Centros de Gestión Informática dada la amplia cantidad de personal y ubicación geográfica.

Por otro lado, el órgano rector, asimismo, capacitado en estrategia en materia de ciberseguridad corresponde a las jefaturas de la Dirección de Tecnologías de Información y Comunicaciones, es por ello, que la presente investigación se enfoca en este nivel jerárquico.

Finalmente, es importante hacer mención que dado que la temática de esta investigación tiene que ver con temas de ciberseguridad, no se puede tener acceso y publicar cierto tipo de información de la institución dado su grado de sensibilidad, por lo que la misma la maneja con un tratamiento confidencial y restringido.

Alcances

Los alcances de esta investigación corresponden específicamente a la Dirección de Tecnologías de Información y Comunicaciones, la cual es el ente encargado de apoyar la gestión de los usuarios mediante el desarrollo de las tecnologías de información y las comunicaciones, la formulación de la regulación, la normativa técnica, las políticas y las estrategias globales, con la participación de los diversos niveles de la organización, para lograr la prestación efectiva de los servicios de salud y de pensiones.

Tomando en cuenta lo anterior y dado que esta unidad es el ente rector en materia de tecnologías de la institución , la estrategia para implementar la cultura de ciberseguridad es un elemento que debe gestarse desde esta unidad, por lo que el alcance se delimita a la Dirección de Tecnologías de Información y Comunicaciones.

Delimitaciones

Espaciales.

La investigación se encuentra delimitada espacialmente para desarrollarse el diseño de la propuesta será efectuada en la provincia de San José.

Temporales.

El estudio será únicamente en el periodo comprendido en los meses de febrero a mayo de 2023.

Legales.

No se ahonda información relacionada con proveedores, compras y otros datos de ciberseguridad ya que puede colocar a la Caja Costarricense de Seguro Social en una situación vulnerable, ya que si estos datos son publicados, facilitaría a un eventual perpetrador (hacker) a infiltrarse y efectuar la sustracción de información sensible en los servicios de misión crítica.

En esta misma línea es importante mencionar que las contrataciones administrativas se realizan por seguridades calificadas, esto según la Ley de Contratación Administrativa N. 7494 del 02 de mayo de 1995, corrida su numeración por el artículo 2., del decreto ejecutivo N. 40124 del 10 de octubre del 2016, lo que traspasó del antiguo inciso 131 h al inciso139 h.

> ‘‘Articulo 139. – Objetos de naturaleza o circunstancia concurrente incompatibles con el concurso.
>
> La Administración, podrá contratar de forma directa los siguientes bienes o servicios que, por su naturaleza o circunstancias concurrentes, no pueden o no conviene adquirirse por medio de un concurso, así como los habilite la Contraloría General de La República.
>
> h) Objetos que requieren seguridades calificadas: Los casos en los que para elaborar las ofertas se requeriría revelar información calificada y confidencial se podrá contratar de forma directa”.

En estos supuestos, la Administración deberá realizar un sondeo del mercado, sin revelar los elementos del objeto que comprometen la seguridad que justifica el procedimiento. Concluido el sondeo de mercado, la entidad procederá a seleccionar a la empresa que considera es la más apta para la satisfacción de su necesidad. La Administración podría negociar con la empresa seleccionada las condiciones de precio. En todo caso, la Administración deberá acreditar que el precio reconocido es razonable, con relación en prestaciones similares o en función de las aplicaciones y tecnología.

No es aplicable esta causal de excepción en los supuestos en los que sea posible realizar un concurso abierto y determinar la idoneidad de un contratista sin tener que revelar esa información, reservándola únicamente para el contratista”.

Capítulo II Marco conceptual

Marco contextual

La Dirección de Tecnologías de Información y Comunicaciones se encuentra adscrita a la Gerencia General de la Caja Costarricense de Seguro Social, actualmente es la encargada de apoyar la gestión de los usuarios mediante el desarrollo de las tecnologías de información y las comunicaciones, la formulación de la regulación, la normativa técnica, las políticas y las estrategias globales, con la participación de los diversos niveles de la organización, para lograr la prestación efectiva de los servicios de salud y de pensiones.

Durante ya hace muchas décadas la Caja Costarricense de Seguro Social ha venido aportando y evolucionando con recursos TIC a lo largo y ancho de toda la organización, siempre buscando beneficios para la población que atiende los servicios de salud y la eficiencia de los procesos partir de la participación de la infraestructura social interna.

Detrás de toda esta infraestructura y equipamiento se encuentra un gran grupo de personas dedicadas a asegurar que todas las soluciones estén bajo el desarrollo de aplicativos con las más estrictas normativas de ingeniera de software, con redes de datos amplias y locales con capacidad de transporte 24/7, bajo una gestión de aseguramiento de la disponibilidad de los servicios, de su seguridad y de su calidad, integrado con las distintas plataformas de hardware bajo tendencias internacionales.

El aporte de cada uno de los colaboradores de las Áreas y Subáreas de la Dirección de Tecnologías de Información y Comunicaciones, en conjunto con el trabajo intenso de los Centros de Gestión Informática, tanto en nivel de Gerencia, en el ámbito Regional y local en cada Hospital y Área de Salud de esta compleja organización; ha sido para acompañar, apoyar, gestionar y contribuir con los compañeros y compañeras de la primera línea de atención.

A continuación, se muestra la misión y visión de esta Dirección según lo indicado en el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones:

Misión

Somos el órgano responsable de promover, impulsar y facilitar el desarrollo de las tecnologías de información y las comunicaciones, con base en los requerimientos institucionales y la participación activa de los usuarios, para lograr una prestación efectiva de los servicios de salud y de pensiones.

Para el cumplimiento de la misión, la organización se compromete a desarrollar los siguientes valores y compromisos:

Excelencia.

Promovemos la excelencia en el desarrollo de la gestión, en beneficio de la sociedad y de los usuarios de los servicios.

Tolerancia.

Respetamos las ideas y opiniones de los demás, no obstante sean diferentes a las nuestras.

Respeto a las personas.

Apoyamos y valoramos a las personas que trabajan y aportan soluciones para el bienestar de la organización y de la Institución.

Responsabilidad social.

Contribuimos significativamente al desarrollo institucional y del país, privilegiando la eficiencia, la calidad y la oportunidad en la prestación de los servicios que otorga la Institución.

Humanismo.

Valoramos y promovemos la formación integral de nuestros funcionarios, resaltando los valores humanos de dignidad, honestidad, transparencia, entre otros.

Cooperación.

Apoyamos las relaciones que fomentan la cooperación inter y extra institucional, para desarrollar con oportunidad las acciones en salud, pensiones y prestaciones sociales.

Compromiso.

Se desarrollarán acciones para cumplir con la obligación contraída, lograr la oportunidad en la ejecución del trabajo, promover el desarrollo de la cultura organizacional y mantener un análisis permanente de la organización y del entorno, con el propósito de orientar la toma de decisiones.

Integridad.

La ética y la moral serán las bases de nuestra actuación y los elementos fundamentales que orienten la toma de decisiones.

Transparencia.

Las actuaciones de los funcionarios en los asuntos de carácter institucional y de cualquier orden, se deben tratar con ética, honestidad, lealtad, claridad, sin ambigüedad y con altos valores morales.

Visión

Visualiza a la organización en el mediano y largo plazo, lo cual es importante para establecer los procesos de planificación estratégica interna y favorecer la competitividad de la unidad de trabajo. La visión definida para esta unidad de trabajo es la siguiente:

"Nos constituiremos en el motor del desarrollo y el facilitador técnico que promueve en coordinación con los usuarios el desarrollo efectivo de las tecnologías de información y las comunicaciones institucionales." (Manual de Organización Dirección de Tecnologías, octubre 2013, 26ágs.. 13-16)

El Manual de Organización Dirección de Tecnologías. (2013), describe los objetivos de esta Dirección a fin de conocer y poner en contexto la labor que realiza para la Caja Costarricense de Seguro Social, así como para los asegurados. A continuación, se destacan estos objetivos tomados de igual manera del Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones.

Objetivo general Dirección de Tecnologías de Información y Comunicaciones

Apoyar la gestión de los usuarios mediante el desarrollo de las tecnologías de información y las comunicaciones, la formulación de la regulación, la normativa técnica, las políticas y las estrategias globales, con la participación de los diversos

niveles de la organización, para lograr la prestación efectiva de los servicios de salud y de pensiones.

Objetivos específicos de la Dirección de Tecnologías de Información y Comunicaciones

- Desarrollar en forma oportuna y con efectividad, las actividades estratégicas, técnicas, logísticas y administrativas, necesarias para facilitar el cumplimiento efectivo de las competencias asignadas.
- Establecer, en coordinación con los usuarios, la regulación, la normativa técnica, las políticas, las estrategias, en tecnologías de información y comunicaciones, para lograr el desarrollo efectivo de la organización y agilizar la prestación de los servicios de salud y de pensiones.
- Desarrollar sistemas de información efectivos, que respondan a los requerimientos de los usuarios, agilicen los procesos de trabajo, la prestación de los servicios, retroalimenten la toma de decisiones de los niveles superiores, contribuyan al cumplimento de los objetivos y las metas institucionales.
- Mantener mecanismos de coordinación efectivos para apoyar la gestión que desarrollan los Centros de Gestión Informática en los diferentes niveles de la organización, con el propósito de facilitar el desempeño funcional y promover el cumplimiento de la regulación y la normativa técnica establecida en materia de tecnologías de información y comunicaciones.
- Administrar el desarrollo de los diferentes proyectos informáticos para garantizar su efectiva implementación en la Institución.
- Contar con sistemas de comunicación inalámbricos que permitan mantener los sistemas de información funcionando en forma eficaz.
- Administrar las frecuencias de radio para fortalecer los medios de comunicación

institucionales.

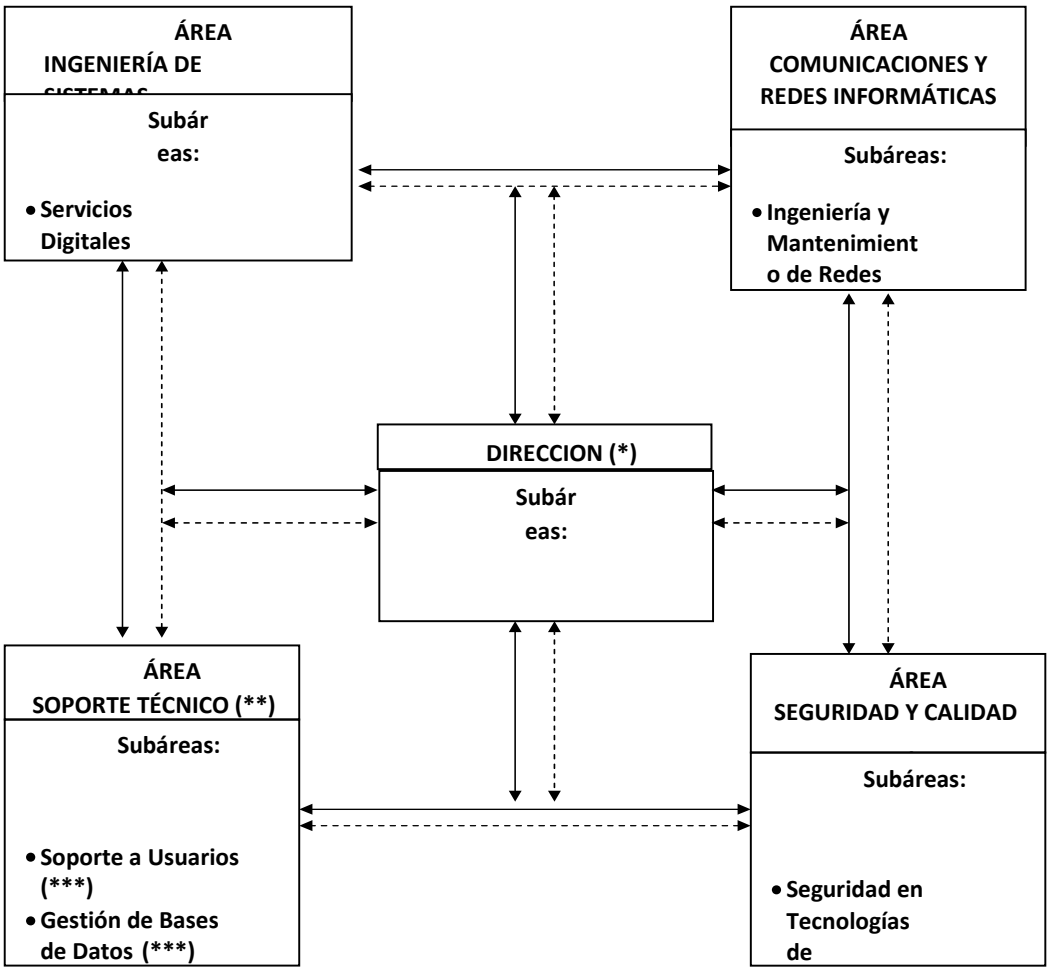
- Garantizar la continuidad de la gestión en Tecnologías de Información y Comunicaciones en situaciones de emergencia o desastres, mediante la administración e implementación de procesos alternos de trabajo, planes de contingencia, de recuperación de la información y de la capacidad operativa. (Manual de Organización Dirección de Tecnologías, octubre 2013, p16)

Las políticas de funcionamiento son guías básicas y escritas, que orientan la dirección, la acción administrativa y logística de una unidad organizacional y señalan los límites generales dentro de los cuales se deben realizar las actividades. A continuación, se presenta la política de funcionamiento de la unidad de trabajo en relación con el servicio según su manual de organización.

Política de servicio al usuario

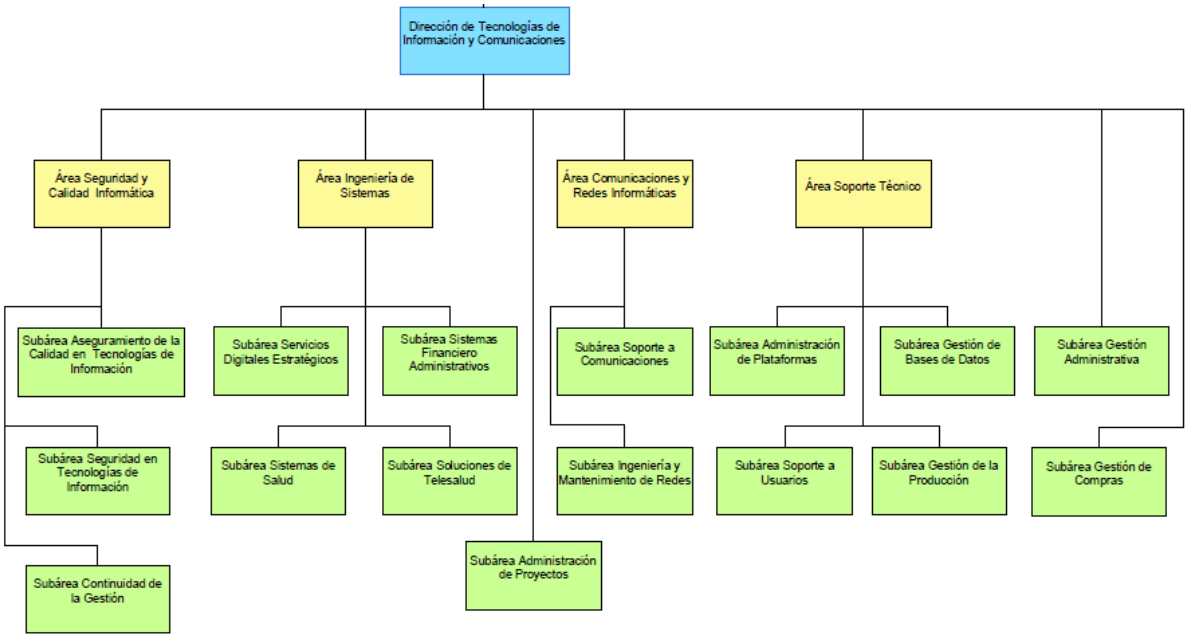
- Se fortalecerá la cultura organizacional de servicio al usuario, para lograr una atención humanizada, oportuna y de calidad.
- La organización se orientará a satisfacer la demanda de los usuarios de los servicios, de acuerdo con las políticas y estrategias institucionales. (Manual de Organización Dirección de Tecnologías, octubre 2013, 28ágs.. 17-18)

Ilustración 2 Niveles Organizacional



Fuente: Caja Costarricense de Seguro Social, Gerencia Administrativa, Dirección de Desarrollo Organizacional, (Octubre 2013). Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones (segunda actualización)

Ilustración 3 Estructura Organizacional de la Dirección de Tecnologías de Información y Comunicaciones



Fuente: Caja Costarricense de Seguro Social, Gerencia Administrativa, Dirección de Desarrollo Organizacional, (Octubre 2013). Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones (segunda actualización)

Tabla N° 1

PLAZAS CON PERFIL INFORMÁTICO FUERA DE LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES A SETIEMBRE DE 2022

Perfil de plazas	Gerencia Medica	Gerencia Administrativa	Gerencia Logística	Gerencia Pensiones	Gerencia Financiera	Gerencia General	Gerencia Infraestruct.	Total general
Técnico (no profesional)	184	6	18	11	30	9	1	259
Profesional	203	6	6	14	46	8	14	297

Fuente: Dirección de Tecnologías de Información y Comunicaciones (marzo 2023)

De la tabla anterior, se desprende que existe un total de 297 plazas con perfil profesional, correspondientes a Analistas de Sistemas 2,3,4 y puestos de Jefaturas, en diversas gerencias, de las cuales el 68% correspondiente a 203 plazas profesionales se encuentran adscritas a la Gerencia Médica, mientras que el 32% restante se ubican en las restantes gerencias.

Tabla N° 2

RECURSO HUMANO ADSCRITO A LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES A MAYO DE 2023

Unidad	Cantidad
Despacho Direccion Tecnologías de Inf Comunicaciones	11
Subdirección	2
Subarea Administracion Proyectos	7
Subarea Gestion Administrativa	12
Subarea Gestion de Compras	0
Area Comunicaciones y Redes	1
Subarea Ingenieria y Mantenimiento de Redes	19
Subarea Soporte a Comunicaciones	6
Area de Seguridad y Calidad Informática	1
Subarea Seguridad en TIC	5
Subarea Aseguramiento de Calidad en TIC	4
Subarea Continuidad de la Gestion	1
Area Ingeniería de Sistemas	11
Subarea Servicios Digitales Estratégicos	6
Subarea Sistema Financiero Administrativo	37
Subarea Sistemas de Salud	31
Subarea Videocomunicaciones	5
Area de Soporte Técnico	8
Subarea Administracion de Plataforma	7
Sub Area Gestión de Base Datos	7
Subarea Gestión de la Producción	2
Subarea Soporte a Usuarios	14

Fuente: Dirección de Tecnologías de Información y Comunicaciones (marzo 2023)

De la tabla anterior, se desprende que para la gestión institucional correspondiente al desarrollo de las tecnologías de información y las comunicaciones, la formulación de la regulación, la normativa técnica, las políticas y las estrategias globales, con la participación de los diversos

niveles de la organización, para lograr la prestación efectiva de los servicios de salud y de pensiones, se tienen adscritas 197 recursos humanos con perfil no profesional, administrativo, técnico e informático.

2.2 Marco teórico

Koontz -Weiheich y Cannice (2014) en el libro “Administración, una perspectiva global y empresarial”, la administración es un proceso en el que se crea y mantiene un ambiente en el que las personas cumplen con las metas que se establecen de manera correcta. Para ello, no solamente se deben considerar los elementos internos de la empresa, esto ya que existen factores también externos que deben ser considerados, esto no solo para brindar el bien o servicio propio de la organización, sino para coexistir y mantener sinergia con el entorno.

En ese sentido, los administradores, deben tomar en cuenta elementos sociales, ecológicos, tecnológicos, político – legales, económicos y éticos para poder llevar a cabo su gestión y de esta manera cumplir con las metas organizacionales. Teniendo esto en consideración, el presente proyecto de investigación se encuentra enfocado en el ámbito tecnológico, uno de los elementos antes mencionados que giran en torno a la administración.

Bajo esta premisa se presenta definición del entorno tecnológico:

> El término tecnología se refiere a la suma total del conocimiento que poseemos sobre cómo hacer las cosas, incluidos los inventos, las técnicas y el amplio cúmulo de conocimiento organizado acerca de todo, de la aerodinámica a la zoología; pero su principal influencia está en la forma de hacer las cosas, es decir, en cómo diseñamos,

producimos, distribuimos y vendemos bienes y servicios. (Koontz -Weiheich y Cannice, 2014 p. 70)

Tomando como referencia que la administración contempla y tiene dentro de su entorno las tecnologías de información y comunicaciones el presente proyecto de investigación se enfoca en el ámbito de la ciberseguridad y la cultura que debe existir entorno a ella con el fin de proteger la plataforma tecnológica y la información que se resguarda en ella, misma que es elemento fundamental para la administración de la empresa.

La ciberseguridad tiene varias aristas, entre ellas la protección de soluciones tecnológicas, aplicativos, sistemas, redes y programas de ataques digitales; en ese sentido, los ciberataques significan el acceder, modificar o destruir la información incluyendo la confidencial, o bien, extorsionar a los usuarios y administradores de datos o interrumpir la continuidad del negocio.

Según la teoría la ciberseguridad tiene distintas capas de protección que se encuentran en computadoras, redes, programas o datos, por tanto, en una organización las personas, los procesos y la tecnología deben complementarse para crear una defensa eficaz contra los ciberataques.

Tomando en cuenta lo anterior, y como parte del objetivo del presente proyecto, las personas deben comprender y cumplir con los principios básicos de seguridad de datos, como elegir contraseñas seguras, no brindar contraseñas a nadie, no dejar guardadas contraseñas en dispositivos que no son los de uso exclusivo, hacer copias de seguridad de datos, cerrar sesión al no utilizar el computador, entre otros temas que son de conocimiento general y que vemos día a día en los noticieros y campañas publicitarias pero muchas veces no les damos importancia.

Ahora bien, todo es un complemento para formar esta capa de seguridad, es por ello que las empresas tienen una estructura para manejar los ciberataques, con procesos definidos que permitan guiar y explicar cómo se pueden identificar ataques, proteger sistemas, detectar y responder a amenazas, así como recuperarse de ataques exitosos, mas sin embargo, no solamente estos temas de infraestructura tecnológica son los que establecerán la defensa en la empresa, sino también esa cultura de ciberseguridad y protección de la información y los equipos desde el usuario.

Existen instituciones a nivel internacional así como estándares dirigidos a la seguridad de la información, entre ellos podemos encontrar la norma ISO 270001, e instituciones como el NIST(Instituto Nacional de Estándares y Tecnología).

Ciberseguridad

Con el fin de definir el concepto de ciberseguridad desde un punto de vista técnico, a continuación, se detalla definición según la empresa internacional CISCO:

> La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio.
>
> Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos. (CISCO, 2023, sección seguridad)

Ahora bien, (CISCO, 2023, sección seguridad), indica que la ciberseguridad tiene muchas capas de protección, mismas que se encuentran repartidas entre las computadoras, redes,

programas o datos que se deben mantener a salvo. En razón de lo anterior, indican que en una organización, las personas, procesos y tecnología deben complementarse para crear una defensa eficaz contra los ciberataques. Asimismo, se indica que un sistema unificado de gestión de amenazas puede automatizar las integraciones entre productos selectos de seguridad de Cisco y acelerar las funciones de operaciones de seguridad claves: detección, investigación y corrección. A continuación, se detallan las capas de protección que deben ser tomadas en cuenta para velar por la ciberseguridad según la empresa tecnológica CISCO:

Personas.

Los usuarios deben comprender y cumplir con los principios básicos de seguridad de datos, como elegir contraseñas seguras, ser cautelosos con los archivos adjuntos de los correos electrónicos y hacer copias de seguridad de datos. Obtenga más información sobre los principios básicos de ciberseguridad.

Procesos.

Las organizaciones deben tener una estructura para manejar los ciberataques tentativos y sospechosos. Una estructura de buena reputación puede guiarlo y explicar cómo puede identificar ataques, proteger sistemas, detectar y responder a amenazas, y recuperarse de ataques exitosos.

Tecnología.

La tecnología es esencial para brindar a las organizaciones y los individuos las herramientas de seguridad informática necesarias para protegerse de ciberataques. Se deben proteger tres entidades importantes: los dispositivos Endpoints (como computadoras, dispositivos inteligentes y routers), las redes y la nube. La tecnología común que se usa para proteger estas entidades incluye firewalls de próxima generación, filtrado de DNS, protección contra malware, software antivirus y soluciones de seguridad de correo electrónico. (CISCO, 2023, sección seguridad)

Como antes se mencionó, existen distintos marcos de referencia y organizaciones que se refieren al tema de ciberseguridad con el fin de coadyubar con la lucha contra los criminales cibernéticos, que si bien es cierto en muchas ocasiones cometen crímenes contra empresas, estos vienen a afectar a sus usuarios; existe también el otro caso, que se refiere a ataques contra los usuarios en los cuales no se vulneran los sistemas de la empresa, sino que tal vez por simplemente entregar una contraseña, se pudieron acceder datos personales o información bancaria.

Como se puede observar, la ciberseguridad no se enfoca propiamente al robustecimiento de plataformas tecnológicas, sino también de procesos, personas, entre otros. En la actualidad existen marcos de referencia y tendencias hacia el establecimiento de Sistemas de Gestión de la Seguridad de la Información, entre los mas conocidos se encuentran: NIST, COBIT 5 e ISO 27001.

Importancia de la ciberseguridad

A continuación, se detalla la importancia de la ciberseguridad de acuerdo con (AWS, 2023, sección ciberseguridad) la cual es la empresa con la plataforma en la nube más amplia a nivel mundial, asimismo, brinda servicios de ciberseguridad a todo el mundo:

> En los negocios de varios sectores, como la energía, el transporte, el comercio al detalle y la fabricación, use sistemas digitales y conectividad de alta velocidad para proporcionar un servicio eficiente al cliente y ejecutar operaciones empresariales rentables. Igual que protegen los recursos físicos, deben proteger también los recursos digitales y los sistemas frente al acceso no intencionado. El evento no intencionado de incumplimiento y acceso no autorizado a un sistema informático, una red o recursos conectados se denomina ciberataque. El éxito de un ciberataque

produce la exposición, sustracción, eliminación o alteración de datos confidenciales. Las medidas de ciberseguridad defienden frente a ciberataques y proporcionan los siguientes beneficios:

Prevención o reducción del costo de las brechas.

Las organizaciones que implementan estrategias de ciberseguridad minimizan las consecuencias no deseadas de ciberataques que pueden afectar a la reputación empresarial, las capacidades financieras, las operaciones empresariales y la confianza del cliente. Por ejemplo, las compañías activan planes de recuperación de desastres para contener las posibles intrusiones y minimizar las interrupciones en las operaciones empresariales.

Mantenimiento de la conformidad normativa.

Las empresas de sectores y regiones específicos deben cumplir con los requisitos normativos para proteger los datos confidenciales frente a posibles riesgos cibernéticos. Por ejemplo, las empresas que operan en Europa deben cumplir el Reglamento General de Protección de Datos (GDPR), que espera que las organizaciones adopten las medidas de ciberseguridad adecuadas para garantizar la privacidad de los datos.

Mitigación de las ciberamenazas en desarrollo.

Los ciberataques evolucionan a la par que las tecnologías cambiantes. Los delincuentes utilizan nuevas herramientas y elaboran nuevas estrategias para el acceso no autorizado al sistema. Las organizaciones emplean y actualizan las medidas de ciberseguridad para mantenerse al día de estas tecnologías y herramientas de ataque digital nuevas y en desarrollo.” (AWS,2023 sección ciberseguridad)

ISO 27001

Según la Norma ISO 27701, este estándar establece todos los requisitos necesarios a la hora de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en cualquier tipo de empresa, asimismo se extrae textualmente sobre el mismo:

> La parte más importante de una empresa es la información. Evidentemente, la empresa contará con otro tipo de activos que también tendrán una destacada importancia, pero si la organización tiene algún problema en la Seguridad de la Información, ésta no podrá recuperarla. Esa es la principal razón por la que las empresas deben dedicar parte de su esfuerzo en garantizar la seguridad de la información corporativa.
>
> Habitualmente, la gestión de la Seguridad de la Información en una empresa se encuentra desorganizada, por lo que no cuenta con un criterio común, es decir, cada departamento de la organización cuenta con sus propios procedimientos y políticas, que han sido constituidas sin contar con las necesidades generales de la empresa e incluso podemos hablar de que se encuentran alejadas de los objetivos del negocio.
>
> Implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 es la manera más eficiente de poder conseguir la coordinación y gestión necesaria para alcanzar los objetivos de la organización y además puede conseguir que la organización salga mucho más reforzada.
>
> Un Sistema de Gestión de Seguridad de la Información según la ISO27001 genera una garantía con la que sabemos que poder realizar una adecuada gestión de la seguridad de la información en la organización. Para ello, se

debe realizar un tratamiento según los diferentes niveles de riesgos cosechados como consecuencia de considerar los distintos efectos que se pueden producir sobre la información de la organización.

El Sistema de Gestión de Seguridad de la Información según la norma ISO-27001 genera un proceso de mejora continua y de gran flexibilidad frente a los cambios que se pueden producir en la empresa refiriéndonos a los procesos de negocio y a la tecnología, ya que ésta avanza a una gran velocidad.

El SGSI se basa en tres pilares fundamentales:

- Confidencialidad: es la garantía de acceso a la información de los usuarios que se encuentran autorizados para tal fin.
- Integridad: es la preservación de la información completa y exacta.
- Disponibilidad: es la garantía de que el usuario accede a la información que necesita en ese preciso momento.

El Sistema de Gestión de Seguridad de la Información debe tener en cuenta los tres pilares fundamentales para realizar el tratamiento de los riesgos de la organización ya que la implementación de los controles de seguridad son los activos de la organización. (ISO 27001, 2005, sección pilares de un Sistema Gestión de Seguridad de Información)

El marco de la norma ISO 207001, se enfoca en tres principios de gestión, enfoque al cliente, liderazgo y participación de las personas. Bajo esta premisa podemos observar que la participación de las personas viene a ser un pilar fundamental en la ciberseguridad de una empresa , ya que es a través de las personas donde puede existir el no cumplimiento de las normas que se establezcan al implementar un sistema de gestión de seguridad de la información,

es por ello, la importancia de establecer la cultura de ciberseguridad que se viene comentando a lo largo de esta investigación.

Ahora bien, en el caso de la Caja Costarricense de Seguro Social, se tiene conocimiento que a través de la Dirección de Tecnologías de Información y Comunicaciones se viene implementando un Proyecto de Ciberseguridad, el cual tiene por objetivo prevenir y mitigar las vulnerabilidades y amenazas a la seguridad informática, desde una perspectiva táctica y operativa.

Para realizar dicho plan, en primera instancia se identificaron una serie de iniciativas que venían siendo ejecutadas por la Dirección, no obstante, el 31 de mayo del 2022, la Institución sufrió un ciberataque que obligó a la desconexión de los servicios y sistemas institucionales, razón por lo cual se reorientaron los esfuerzos que se estaban realizando en esta materia y la Dirección se enfocó en la habilitación de los servicios tecnológicos y a la protección de su infraestructura y plataformas.

Una vez realizado el levantamiento de los sistemas, y bajo la normalización de los servicios de tecnologías de la institución, esta Dirección continúa con la implementación de este plan de ciberseguridad, el cual permitirá robustecer en materia de seguridad informática la plataforma de la institución.

Ahora bien, teniendo este antecedente, y los datos antes expuestos en materia de ciberseguridad, es importante destacar que es necesario llevar adelante una estrategia que permita incorporar al recurso humano dentro del robustecimiento de la ciberseguridad institucional. Esto se expone bajo la luz de los datos emitidos anteriormente, en donde se indica que el componente humano puede generar riesgos en la ciberseguridad al no seguir los procedimientos de manera adecuada en materia tecnológica, o bien, como usuario de las

tecnologías utilizarlas sin tomar en cuenta parámetros importantes en cuanto al manejo de sistemas y de equipo tecnológico.

Tipos de ataque que se Intentan defender con la ciberseguridad

A continuación, se definen algunos tipos de ataque que se buscan contrarrestar al establecer un sistema de gestión de la seguridad en las tecnologías que a su vez contempla una cultura de ciberseguridad:

Malware: Se cataloga como un código malicioso compuesto por gusanos, worms, spyware, troyanos, virus o script malintencionados que tiene como propósito infiltrarse y dañar un computador o sistema de información sin el consentimiento de los propietarios. (Cañón Parada, 2023, sección malware)

Ramsomware: El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito. (malwarebytes, 2023, sección malware)

Ataque de intermediario: Un ataque de intermediario implica que una parte externa intenta acceder de forma no autorizada por una red durante un intercambio de datos. Dichos ataques aumentan los riesgos de seguridad de la información confidencial, como los datos financieros. (AWS, 2023, sección ciberseguridad)

Phishing: Su objetivo es intentar obtener datos como usuarios , contraseñas, información de cuentas bancarias , e identidad del usuario mediante correos electrónicos y llamadas telefónicas usando la técnica de suplantación de portales bancarios haciendo creer al usuario ,que se está conectando al sitio oficial del banco , sin saber que está siendo víctima de un portal falso donde luego utilizan la información con el fin de generar transacciones no autorizadas donde se genera hurto. (Cañón Parada, 2023, sección phishing)

DdoS*:* Es un ataque muy común donde su objetivo principal es denegar el funcionamiento de sitios web, donde se vulnera la disponibilidad del servicio ya que cuando un usuario trata de ingresar al sitio este se encuentra fuera de servicio cumpliendo con el objetivo propuesto. (Cañón Parada, 2023, sección DdoS)

Amenaza interna*:* Una amenaza interna es un riesgo de seguridad introducido por personal con malas intenciones dentro de una organización. El personal posee acceso de alto nivel a los sistemas informáticos y puede desestabilizar la seguridad de la infraestructura desde dentro. (AWS, 2023, sección ciberseguridad)

Ingeniería social: Es el arte de engañar a las personas, las amenazas de la ingeniería social son más peligrosas, ya que es más difícil protegerse frente a ellas, debido a que el objetivo principal no solamente el sistema si no la víctima.

Es una técnica de hackeo utilizada para extraer información a otras personas, teniendo como base la interacción social, donde la persona que está siendo atacada no se da cuenta cuando suministra información personal que puede terminar en manos de un atacante. (Cañón Parada, 2023, sección ingeniería social)

Tipos de ciberseguridad

Para los fines de la presente investigación, se hace referencia a los tipos de ciberseguridad con el fin de tener un panorama amplio sobre el cual analizar cual es el enfoque para la concientización en ciberseguridad, a continuación, se describen de acuerdo con (AWS, 2023, sección ciberseguridad), especialista en temas de ciberseguridad y almacenamiento en nube:

Ciberseguridad de la infraestructura crítica.

La infraestructura crítica hace referencia a sistemas digitales importantes para la sociedad, como la energía, la comunicación y el transporte. Las organizaciones requieren, en estas áreas, un enfoque sistemático de ciberseguridad debido a que la interrupción o la pérdida de datos pueden desestabilizar la sociedad.

Seguridad de la red.

La seguridad de la red es una protección de ciberseguridad para los equipos y dispositivos conectados a una red. Los equipos de TI utilizan las tecnologías de seguridad de red, como los firewalls y el control de acceso a la red para regular el acceso de usuarios y administrar los permisos para recursos digitales específicos.

Seguridad en la nube.

La seguridad en la nube describe las medidas que toma una organización para proteger los datos y las aplicaciones que se ejecutan en la nube. Es importante para reforzar la confianza del cliente, proteger las operaciones tolerantes a errores y cumplir con la normativa de la privacidad de datos en un entorno escalable. Una estrategia sólida de seguridad en la nube implica la responsabilidad compartida entre el proveedor de nube y la organización.

Seguridad de IoT.

El término Internet de las cosas (IoT) hace referencia a dispositivos electrónicos que funcionan remotamente en Internet. Por ejemplo, una alarma inteligente que envía actualizaciones periódicas al smartphone podría considerarse un dispositivo IoT. Estos dispositivos IoT presentan una capa adicional de riesgo en la seguridad debido a la constante conectividad y los errores ocultos del software. Por lo tanto, es esencial introducir políticas de seguridad en la infraestructura de red para evaluar y mitigar los posibles riesgos de los distintos dispositivos IoT.

Seguridad de los datos.

La seguridad de los datos protege los datos en tránsito y en reposo con un sistema sólido de almacenamiento y una transferencia de datos segura. Los desarrolladores usan medidas protectoras, como el cifrado y las copias de seguridad aisladas, para la resistencia operativa frente a posibles brechas de datos.

Seguridad de las aplicaciones

La seguridad de las aplicaciones es un trabajo coordinado para fortalecer la protección de una aplicación frente a la manipulación no autorizada durante las etapas de diseño, desarrollo y prueba. Los programadores de software escriben códigos seguros para evitar errores que puedan aumentar los riesgos de seguridad.

Seguridad de los puntos de conexión.

La seguridad de los puntos de conexión aborda los riesgos de seguridad que surgen cuando los usuarios acceden remotamente a la red de una organización. La protección de la seguridad de los puntos de conexión examina los archivos de dispositivos individuales y mitiga las amenazas al detectarlas.

Planificación de la recuperación de desastres y continuidad del negocio.

Describe los planes de contingencia que permiten a una organización responder de inmediato a incidentes de ciberseguridad mientras continúa funcionando con pocas o ninguna interrupción. Implementan políticas de recuperación de datos para responder positivamente a las pérdidas de datos.

Educación del usuario final.

Las personas de una organización representan un rol crucial para garantizar el éxito de las estrategias de ciberseguridad. La educación es clave para garantizar que los empleados se formen en las prácticas recomendadas de seguridad correctas, como la eliminación de correos electrónicos sospechosos y la detención de conexiones de dispositivos USB desconocidos. (AWS, 2023, sección ciberseguridad)

Cultura de ciberseguridad

Para comprender de este punto, se toma como referencia lo indicado por la Agencia para la Ciberseguridad de la Unión Europea (ENISA), que indica que la cultura de la ciberseguridad tiene que ver con los hábitos, normas, conocimientos y actitudes en relación con la ciberseguridad. Esta agencia refiere que la cultura viene a dirigirse hacia la forma en que las personas utilizan y se comportan de frente a las tecnologías.

ENISA se dedica a lograr un alto nivel común de ciberseguridad en toda Europa, entre las labores que desarrolla y en el caso que nos ocupa, la misma promueve la cultura de ciberseguridad de red y seguridad de la información para el beneficio de los ciudadanos, consumidores, empresas y organizaciones del sector público de la Unión Europea, esto lo realiza con el objetivo de mejorar el funcionamiento interno de la Unión Europea.

Tomando en cuenta lo anterior, la Unión Europea como parte del primer mundo, que significa haber logrado un alto grado de industrialización y estándares de tecnología, tiene dentro de sus principales actividades establecer una cultura de ciberseguridad, lo cual implica que este punto no es solamente alguna teoría sin fundamento, sino un parámetro y un tema de gran relevancia que debe ser tomado en cuenta al momento de querer fortalecer la ciberseguridad. (ENISA, 2023, sección about ENISA)

La cultura de ciberseguridad establece la necesidad de aumentar la participación de los funcionarios de una organización a través de normas y políticas que los mismos deberán seguir. Para llegar a ello, es fundamental una comunicación y capacitación eficaz que venga en cascada, o sea desde la dirección, ya que esto permitirá a los colaboradores entender que el tema es crucial para la organización, y además generará reflexión.

Para reforzar lo antes indicado, se extrae el siguiente párrafo de la página web ISO TOOLS la cual es una organización comprometida con la Seguridad de la Información y los Sistemas de Gestión especialmente diseñados y aplicables a las TIC´s, que indica:

> La seguridad de los datos no es solo responsabilidad del área de TI. Como ya se ha comentado con anterioridad, los mayores riesgos para la privacidad y la seguridad de la información se encuentran bajo las acciones de los empleados y empleadas. Un trabajador bien intencionado pero desinformado puede causar una infracción al caer en una estafa de phishing, descargar malware sin darse cuenta o hacer clic en un enlace malicioso. Es por ello que cualquier capacitación debe ser amplia y tomada por todos los estamentos de la organización. (ISOTOOLS, 2022, sección cultura de ciberseguridad)

¿Cómo crear una cultura de ciberseguridad?

Crear una cultura de ciberseguridad no es un principio estándar para toda organización, ya que todas las organizaciones tienen distintas maneras de gestión interna, y especialmente a

nivel de las TIC, habría que determinar el nivel de madurez e importancia que se les brinde. En ese sentido, es importante tener en cuenta que no solamente es importante considerar una gestión del cambio desde su teoría, sino también estudiar y analizar si en la empresa ya se está haciendo algún tipo de gestión con el fin de educar y sensibilizar a los colaboradores, para tomar esto como punto de partida al momento de saber qué y cómo hacerlo.

Dentro del desarrollo de esta investigación se puede observar en muchos recursos puntos específicos como madurez de la organización, gestión del cambio, capacitación, comunicación. En ese sentido, se destacan los siguientes elementos de (ISOTOOLS, 2022, sección cultura de ciberseguridad), la cual basada en la norma ISO 27001, la cual es la encargada de establecer marcos de ciberseguridad, se refieren a cinco elementos a través de los cuales crear una cultura de ciberseguridad en las empresas:

Rutina de capacitación regular y personalizada.

La formación constante ayuda a mejorar la moral de las personas de la organización, fomenta la calidad en los resultados y permite la puesta en marcha de soluciones más rápidas. Sin embargo, la mayoría de los motivos por los que un empleado rehúsa de la capacitación en ciberseguridad es por la carga de trabajo. Si los trabajadores cuentan con una gran carga, pedirles que empleen una cantidad de tiempo en capacitación en ciberseguridad puede provocar un mayor agotamiento o la total desconexión durante la formación.

Por su parte, un líder en ciberseguridad o CISO debe ayudar a reforzar el valor de la capacitación y demostrar la efectividad de la misma. La disponibilidad de diferentes formas de tomar la capacitación también fomenta la participación. Habrá

que ofrecer las posibilidades que mejor se ajusten a las preferencias de los empleados y empleadas.

Alinear al equipo con la ciberseguridad.

Un elemento fundamental en la construcción de una cultura de ciberseguridad es alinear los diferentes equipos de trabajo que componen la organización y con las disciplinas de seguridad. Para ello, será fundamental fomentar la comunicación interna, dando especial visibilidad a los aspectos relacionados con la ciberseguridad.

El objetivo es estar presente y ser transparente con toda la compañía. Buscando que todo el mundo se encuentre alineado para proteger la organización, habrá que informar acerca de esta materia y mantener al equipo tanto.

Observar las tendencias de la organización.

La única forma de evitar las amenazas en materia de ciberseguridad es estando al tanto de todos los posibles puntos de entrada. Esto se consigue mediante la observación de las diferentes tendencias que sigue la organización. La información al respecto tendrá que estar disponible para quien la precise.

En este sentido, no se trata únicamente de desarrollar planes y protocolos de contingencia frente a amenazas, sino que habrá que mantenerlos actualizados en todo momento. Para ello habrá que actualizar la documentación de manera regular y ponerla a disposición de todo el equipo, así como de la organización en general. Esto ayudará a minimizar los ataques si es que llegan a ocurrir.

Colaborar con los socios y clientes.

La colaboración y la comunicación con socios y clientes de manera regular, compartiendo tendencias, estrategias y novedades, les brindará una idea de cómo se

mantienen seguros. La educación y la comunicación ayudan a crear una comunidad con conciencia cibernética.

Enfoque permanente.

Un elemento clave para la creación de una cultura de ciberseguridad, y al que deben prestar especial atención los CISO, es permanecer enfocado en todo momento en estar preparado ante cualquier posible amenaza. Tener planes para combatir los ataques es, en último término, la mejor forma posible de utilizar los recursos de la organización. Incluir a toda la fuerza laboral en este proceso de construcción de la cultura de ciberseguridad, y permanecer transparente, tendrá óptimos resultados para el conjunto de la organización. .(ISOTOOLS, 2022, sección cultura de ciberseguridad)

Bajo esta línea, la cultura de ciberseguridad se puede entender como “educación” por lo que deben generarse actividades que hagan que las personas aprendan los principios de seguridad y se sensibilicen ante su importancia para resguardar la información y garantizar el uso correcto de las tecnologías. A continuación se indican algunas medidas para mejorar la cultura según (Nueva ISO 450001, 2020, sección seguridad) :

- Impartir cursos de formación
- Concienciar a los trabajadores de por qué es importante seguir con los procedimientos y adoptar buenas prácticas.
- Proporcionar el material adecuado: maquinaría, herramientas, procedimientos de trabajo, guías técnicas, etc.
- Difundir los aspectos clave y comportamientos esperados por medio de posters, boletines, etc.
- Premiar las buenas prácticas.
- Dar ejemplo por parte de la dirección, jefes y coordinadores.

- Controlar los procesos clave y buscar formas de minimizar dificultades, riesgos y puntos negros.
- Fomentar la comunicación, participación y cooperación entre los empleados.

Componentes de estrategia de ciberseguridad

Dada la importancia de establecer un marco que permita proteger a las empresas de un ciberataque o robo de información, es importante tener en cuenta los componentes que se deben integrar al momento de establecer un plan de ciberseguridad, en ese sentido, a continuación se describen los componentes para dicha estrategia de acuerdo con (AWS, 2023, sección ciberseguridad), especialista en temas de ciberseguridad y almacenamiento en nube:

Personas.

La mayoría de los empleados no conocen las amenazas y las prácticas recomendadas de seguridad más recientes para proteger sus dispositivos, red y servidor. La formación y educación de los empleados con respecto a los principios de ciberseguridad reduce los riesgos de descuidos que pueden dar lugar a incidencias no deseadas.

Procesamiento.

El equipo de seguridad de TI desarrolla un marco de seguridad sólido para el monitoreo e informe continuado de las vulnerabilidades conocidas en la infraestructura informática de la organización. El marco es un plan táctico que garantiza que la organización va a responder y recuperar de inmediato las posibles incidencias de seguridad.

Tecnología.

Las organizaciones utilizan tecnologías de ciberseguridad para proteger los dispositivos conectados, los servidores, las redes y los datos frente a posibles amenazas. Por ejemplo, las empresas utilizan firewalls, software de antivirus, programas de detección

> de malware y filtrado DNS para detectar e impedir automáticamente el acceso no autorizado al sistema interno. Algunas organizaciones usan tecnologías que aplican la seguridad de confianza cero para reforzar más la ciberseguridad.

Gestión del cambio organizacional

El componente de gestión de cambio, es un elemento esencial para el éxito en la implementación de proyectos, ya que permite anticiparse de manera oportuna al cambio y apoyar a las organizaciones en el involucramiento del personal dentro de la nueva manera de hacer las cosas. El manejo adecuado de las resistencias permite aumentar las probabilidades de éxito en tiempo, costo y calidad.

Para comprender mejor este tema a continuación se define gestión del cambio organizacional según (Licari,2022, sección marketing):

> La gestión de cambio es una metodología con la que una empresa busca facilitar la implementación y transformación de procesos de forma ágil y eficaz. Esta se aplica de manera estructurada con el apoyo de herramientas, a fin de involucrar a todos los miembros de una organización.
>
> En otras palabras, la gestión de cambio se enfoca en ayudar a las personas que laboran en una empresa a participar, adoptar y utilizar un cambio a su favor en las actividades diarias. Los cambios más comunes que contempla esta metodología son los tecnológicos, de modelo de negocio y organizacionales, entre otros.

Con base en la anterior definición, la gestión del cambio organizacional es un elemento que viene a generar la implantación de un mejoramiento en los distintos aspectos que se

requieran dentro de una empresa. Este componente se visualiza como de gran relevancia ya que analiza los aspectos por mejorar y establece las pautas para llevar a cabo dichas mejoras, contemplando diversos aspectos que sean los factores de éxito.

Existen diversos modelos de gestión del cambio, no se puede decir que alguno sea mejor que otro, en esencia debe analizarse el proyecto que requiera esa gestión de cambio y determinar cual modelo podría ser más favorecedor. A continuación, se menciona el nombre de los cinco modelos más conocidos, a saber:

1. Modelo de Lewin
2. Modelo ADKAR
3. Modelo del empujón
4. Modelo de Transición de Bridges
5. Modelo de Kotter

Para efectos de implementar una cultura de ciberseguridad en una organización, es necesario valerse de herramientas como lo son la gestión del cambio organizacional, para asegurar el éxito en la implementación, en ese sentido, la presente investigación se enfocará en comprender el modelo ADKAR.

Modelo ADKAR

A continuación, se describe que es el modelo ADKAR según Hiatt, el cual es un modelo para gestionar el cambio organizacional:

> ADKAR es un acrónimo que representa los cinco hitos o resultados que un individuo debe lograr para que el cambio se realice con éxito: awareness (conciencia), desire (deseo),

knowledge (conocimiento), ability (habilidad) y reinforcement (refuerzo). Cuando se aplica al cambio organizacional, este modelo permite que los líderes y los equipos de gestión de cambio enfoquen sus actividades en lo que impulsará el cambio individual y producirá resultados organizacionales colectivamente.

Los objetivos o resultados definidos por ADKAR son secuenciales y acumulativos. Deben lograrse en orden. Para que un cambio sea implementado y sostenido, un individuo debe progresar a través de cada uno de los hitos, comenzando con la conciencia.

ADKAR nació producto de las primeras investigaciones del fundador de Prosci, Jeff Hiatt, para alinear las actividades tradicionales de gestión del cambio con los objetivos y resultados de un proyecto. El modelo ADKAR se usó por primera vez para determinar la efectividad de actividades de gestión del cambio, como la comunicación y la capacitación, para lograr los resultados deseados del cambio organizacional. (…)

El modelo ADKAR se puede utilizar para identificar brechas dentro de un proceso de gestión de cambio. Al desglosar un cambio en los bloques de ADKAR, podrá ver dónde y por qué un cambio no funciona bien. Con este entendimiento, puede abordar los puntos de barrera, proporcionar coaching efectivo para sus empleados y tomar las acciones necesarias para mejorar las probabilidades de éxito del cambio.

El modelo ADKAR es útil para:

• Diagnosticar la resistencia de los empleados al cambio

• Ayudar a los empleados a hacer la transición a través del proceso de cambio

• Crear un plan de acción exitoso para el avance personal y profesional durante una iniciativa de cambio • Desarrollar un plan de gestión de cambio para sus empleados

> Los cambios cobran vida en dos dimensiones: el lado técnico del proyecto y el lado humano del cambio. El cambio es exitoso en la medida que ambas dimensiones del cambio sean exitosas simultáneamente (ver más abajo). La gestión de proyectos y la gestión del cambio son disciplinas complementarias con un objetivo común: lograr los objetivos y resultados deseados. (Hiatt, 2006, P.4)

Como parte de lo anterior, y basados en el libro ADKAR*,* ¿Cómo implementar de manera exitosa el cambio en nuestras vida personal y carrera? De Jeffrey M. Hiatt, se puede decir que el modelo ADAR se desprende del acrónimo Awareness, Desire, Knowledge, Ability y Reinforcement, que son las fases de dicho modelo y se describen a continuación:

- *Awareness (Conciencia*). Crear interés y conciencia de la necesidad de los cambios en la empresa e informar los requerimientos necesarios para lograrlos.
- *Desire (Deseo).* Generar en los empleados un anhelo por los cambios y un compromiso para hacerlos realidad.
- *Knowledge (Conocimiento).* Brindar capacitación y guía de cómo lograr los cambios estipulados.
- *Ability (Habilidad).* Destreza para lograr introducir los cambios con habilidad y capacidad.
- *Reinforcement (Reforzamiento).* Lograr mantener el cambio realizado y reforzarlo con el tiempo. (Hiatt, 2006, P.5)

Capítulo III Marco metodológico

El enfoque de este trabajo se ha sido el análisis de la importancia de establecer una cultura de ciberseguridad en los usuarios internos de los servicios de tecnologías de información y comunicaciones de la Caja Costarricense de Seguro Social.

A través de este capítulo, se pretende realizar una descripción de la metodología utilizada con el fin de llevar a cabo esta investigación. Este comenzará con el detalle del tipo de investigación que se está realizando. El segundo punto corresponde a la descripción del alcance de la investigación, asimismo, se determinarán las fuentes de información, los instrumentos y técnicas de recolección de datos. Por otro lado, se mostrará la validación de los instrumentos, población, tipo de muestreo y tamaño de la muestra.

Tipo de investigación

El tipo de investigación que se llevará a cabo es de tipo cualitativa. Hernández, Fernández y Baptista (2014, p.16), indica que la investigación cualitativa tiene como principal foco el entender los fenómenos analizándolos desde la perspectiva de los participantes en su ambiente natural y con el contexto, comprendiendo sus puntos de vista, interpretaciones y significados.

En virtud de que la presente investigación es cualitativa, la misma se trabajará con datos no numéricos, sino mas bien el análisis de datos desde el punto de vista de su significado, eventos, hechos, situaciones, entre otros. Para lo anterior, el uso de entrevista, recolección de datos cualitativos, y la búsqueda de sentido al análisis de la información, es lo que dará forma a este proyecto.

Alcance de la investigación

Según Bernal (2000, p. 114) existen varios tipos de investigación, la histórica, documental, descriptiva, correlacional, explicativa, estudio de caso.

Para la presente investigación, el alcance es explicativo en vista de que se analizará el porqué podrían ocurrir riesgos en ciberseguridad desde la perspectiva de cultura, asimismo, descriptiva ya que se exponen características del objeto de estudio.

Fuentes de información

Con el fin de llevar a cabo esta investigación las fuentes de información que se utilizan son las primarias y secundarias. Las primarias corresponden a las que la información es recolectada en una forma directa, en este caso, la entrevista a las jefaturas de la Dirección de Tecnologías de Información y Comunicaciones, que tengan que ver con temas de ciberseguridad dado su enfoque estratégico, técnico y experiencia en la materia dentro de la institución. Esta entrevista viene a brindar la información necesaria para comprender la estrategia que se sigue actualmente y la visión que tienen los lideres en materia de protección de la plataforma tecnológica institucional. Los recursos secundarios, corresponden a los que aportan información relacionada con la investigación como lo son libros, páginas de internet y documentación presentada por parte de los entrevistados.

Instrumentos y técnicas de recolección de datos

Según Hernández, Fernández y Baptista (2014, p. 429), la recolección de datos desde el enfoque cualitativo busca lo siguiente:

> Lo que se busca en un estudio cualitativo es obtener datos (que se convertirán en información) de personas, seres vivos, comunidades, situaciones o procesos en profundidad; en las propias “formas de expresión” de cada uno. Al tratarse de seres humanos, los datos que interesan son conceptos, percepciones, imágenes mentales, creencias, emociones, interacciones, pensamientos, experiencias y vivencias

manifestadas en el lenguaje de los participantes, ya sea de manera individual, grupal o colectiva.

Se recolectan con la finalidad de analizarlos y comprenderlos, y así responder a las preguntas de investigación y generar conocimiento.

Tomando en cuenta lo anterior, para el objeto de la presente investigación se utiliza la siguiente técnica de recolección de datos: entrevista a jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación directa con temas de ciberseguridad.

Validación de los instrumentos

Basado en las características del problema y los objetivos de la investigación se creó un instrumento que corresponde a una entrevista, aplicada a jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan que interactuar directamente con temas operativos y estratégicos de la ciberseguridad.

Esta entrevista tiene como principal foco los elementos técnicos, estratégicos y de percepción sobre la importancia de establecer una cultura de ciberseguridad con el fin de proteger a la institución de ataques cibernéticos o bien de fugas de información sensible, asimismo, obtener información sobre las actividades que se han venido haciendo institucionalmente sobre esta temática. Esta entrevista consta de diez preguntas y fue avalada por el tutor del proyecto.

Población

Según Según Bernal (2000, p. 158) la población consiste en los elementos a los cuales se refiere la investigación, o bien el conjunto de todas las unidades de muestreo.

La población consultada para esta investigación, corresponde a jefaturas de la Dirección de Tecnologías de Información y Comunicaciones. La elección de esta población se da en virtud del conocimiento técnico, estratégico y experiencia que han forjado en temas de ciberseguridad, asimismo, estos funcionarios son los encargados de generar los lineamientos a nivel institucional para la gestión de la ciberseguridad, es por ello que la información que se obtiene a través de los mismos es valiosa para esta investigación.

Tipo muestreo

Existen varias clasificaciones para los métodos de muestreo, según Según Bernal (2000, p. 159), las más usadas son: probabilísticos y no probabilísticas y diseños por atributos y por variables, la primera de esta es la más usual"

El método de muestreo que se realizó mediante esta investigación corresponde al de conveniencia, ya que se buscaron sujetos con los conocimientos y experiencia necesaria para brindar criterio sobre el tema.

Tamaño de la muestra y distribución

El tamaño de la muestra tiene que ver con la población que se estudiará, y esta busca siempre utilizar una cantidad importante de población con el fin de tener un nivel de confianza alto. La muestra se utiliza cuando la población de estudio es muy grande y se hace difícil o imposible estudiarla en su totalidad.

Con relación al muestreo en este caso se utiliza el muestreo a conveniencia dado que es posible abarcar al 100% de la población que involucra este proyecto de investigación, específicamente los Jefes encargados de la Ciberseguridad de la Caja Costarricense de Seguro Social quienes son las encargadas de generar las directrices, estrategias y normas en relación con la ciberseguridad.

En virtud de lo anterior, se logró determinar que la cantidad de jefaturas que tienen a cargo este tema son siete. Siendo que la cantidad es un número alcanzable y que el tiempo para realizar la presente investigación era un poco holgado, se logró obtener el apoyo de las siete jefaturas encargadas del tema.

Por lo anterior, no se requirió utilizar una muestra, dado que se logró entrevistar al 100% de la población requerida para el estudio, siendo que el nivel de confianza es óptimo.

Operacionalización de las variables

Según Rojas (1998, p. 186) Una variable corresponde a una característica, atributo, propiedad o cualidad que puede estar o no presente en los individuos, grupos o sociedades, puede presentarse en matices o modalidades diferentes o en grados, magnitudes o medidas distintas a lo largo de un continuum.

De acuerdo con la definición brindada por Rojas Soriano, se observa que las variables corresponden a una suposición de las características que están circunscritas al problema de la investigación. Considerando esto, y la importancia de estas a continuación, se describen las variables asociadas a la presente investigación a través de la tabla número 1.

Tabla N° 3

Tabla de variables

Objetivo específico	Variables de estudio	Definición conceptual de la variable	Indicadores	Definición Instrumental	Definición operacional
Conocer la importancia de establecer una cultura de ciberseguridad en los usuarios internos de servicios informáticos en la Caja Costarricense de Seguro Social.	Cultura de ciberseguridad	La cultura de la ciberseguridad tiene que ver con los hábitos, normas, conocimientos y actitudes en relación con la ciberseguridad. (ENISA, 2023, sección about ENISA)	Grado de conocimiento de aspectos básicos de ciberseguridad en usuarios de servicios TIC	Entrevista a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, ver preguntas 1 y 2.	Determinar la importancia de llevar a cabo actividades para la concientización en ciberseguridad.
Identificar cuáles son las actividades que se llevan a cabo actualmente en la Caja	Actividades para fomentar cultura de ciberseguridad	Las actividades para fomentar una cultura de ciberseguridad corresponden a todas	Grado de cumplimiento de cronograma para implementación de	Entrevista a Jefaturas de la Dirección de Tecnologías de	Identificar las actividades que la Dirección de Tecnologías

Costarricense de Seguro Social para fomentar una cultura de seguridad en los usuarios internos de los servicios informáticos.		aquellas acciones que se desarrollan en los usuarios de los servicios tecnológicos con el fin de concientizarlos en el uso correcto de las tecnologías de información.	cultura de ciberseguridad	Información y Comunicaciones que tengan relación con temas de ciberseguridad. Ver preguntas 4, 5, 7, 8, 9 y 11	viene desarrollando para establecer una cultura de ciberseguridad y de esta manera reforzar la seguridad informática.
	Gestión del Cambio	La gestión de cambio es una metodología con la que una empresa busca facilitar la implementación y transformación de procesos de forma ágil y eficaz. Esta se aplica de manera estructurada con el apoyo de herramientas, a fin de involucrar a todos los miembros de una organización. (Licari,2022, sección marketing):	Grado de cumplimiento del instrumento de evaluación de sostenibilidad de cultura ciberseguridad		

Valorar elementos que permitan llevar a cabo una cultura de ciberseguridad en la Caja Costarricense de Seguro Social.	Elementos de cultura de ciberseguridad	Los elementos para establecer una cultura de ciberseguridad corresponden a las actividades o comportamientos que se realicen por parte de los usuarios de servicios TIC que fortalezcan la ciberseguridad de la institución.	Grado de cumplimiento de sesiones de sensibilización y capacitación.	Aplicación de entrevista a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad. Ver preguntas 3, 6, 10 y 12	Los elementos para mantener la ciberseguridad desde el punto de vista usuario son fundamentales para el desarrollo de la propuesta para concientizar hacia una cultura de ciberseguridad.
Sugerir una propuesta para fomentar un cambio de mentalidad para el uso seguro de las TIC.	Propuesta para fomentar cultura de ciberseguridad	La propuesta para fomentar la cultura de ciberseguridad corresponde al conjunto de actividades a realizar que permitan concientizar a la población usuaria de los servicios TIC a nivel	Propuesta de plan de Trabajo para el desarrollo de cultura de ciberseguridad en usuarios internos de los servicios TIC de la Caja	Entrevista a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan	Propuesta para fomentar la cultura de ciberseguridad en la Caja Costarricense

		institucional en el uso correcto y seguro de las tecnologías de información.	Costarricense de Seguro Social	relación con temas de ciberseguridad. Propuesta de plan.	de Seguro Social.

Fuente: elaboración propia (2023)

Capítulo III Análisis e interpretación de datos

A través de este capítulo se analiza la información obtenida en las entrevistas realizadas a las jefaturas de la Dirección de Tecnologías de Información y Comunicaciones de la Caja Costarricense de Seguro Social, que tengan relación directa con temas de ciberseguridad dentro de su conducción. La información conseguida está organizada por variables y mostrada mediante gráficos y tablas. Cabe indicar que junto a cada gráfico y tabla se encuentra el análisis de los resultados de la pregunta.

En vista de que este proyecto presenta cuatro variables, las preguntas de la entrevista se analizaron en función de cada una de ellas. La primera variable corresponde a la cultura de ciberseguridad, enfocada en el objetivo de conocer la importancia de una cultura de ciberseguridad en los usuarios internos de servicios informáticos en la Caja Costarricense de Seguro Social. La segunda variable corresponde a actividades para fomentar cultura de ciberseguridad, la cual se relaciona con el objetivo de identificar cuáles son las actividades que se llevan a cabo actualmente en la Caja Costarricense de Seguro Social para fomentar una cultura de ciberseguridad en los usuarios internos de los servicios informáticos. La tercera variable tiene que ver con la gestión del cambio, que se alinea con el objetivo de valorar elementos que permitan llevar a cabo una cultura de ciberseguridad en la Caja Costarricense de Seguro Social. Finalmente, encontramos la variable cuatro la cual tiene que ver con una propuesta para fomentar un cambio de mentalidad para el uso seguro de las TIC, sin embargo, debido a que la naturaleza de esta variable corresponde a la elaboración de una propuesta, no se realizaron preguntas sobre la misma en la encuesta.

La entrevista aplicada , tuvo como objetivo además de la obtención de datos puntuales, mismos que fueron respondidos a lo largo del instrumento, de generar un acercamiento con las

jefaturas que tienen relación directa con generar disposiciones, estrategias, normativa y aseguramiento de los servicios tecnológicos en temas de ciberseguridad con el fin de estructurar una conversación que brindara elementos para el análisis de la información y la generación de conclusiones una propuesta.

Variable 1

Cultura de ciberseguridad, enfocada en el objetivo de conocer la importancia de una cultura de ciberseguridad en los usuarios internos de servicios informáticos en la Caja Costarricense de Seguro Social. A continuación, las preguntas asociadas a esta variable:

Pregunta #1: ¿Cuánto considera usted que impacta el compromiso de los usuarios de los servicios TIC con la ciberseguridad en el riesgo cibernético?

Tabla N° 4

Impacto del compromiso de usuarios de servicios TIC en riesgo cibernético

Variable	***Cantidad de respuestas***	***Valor relativo***
No impacta	0	0
Impacta un poco	0	0
Impacta mucho	0	0
Impacta demasiado	7	1

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Para esta pregunta, todos los encuestados concordaron en que el compromiso de los usuarios de los servicios tecnológicos con la ciberseguridad tiene un alto impacto ante la mitigación de los riesgos cibernéticos. Como se puede observar, a través de esta encuesta y los aspectos técnicos sobre los componentes de la ciberseguridad detallados en el marco teórico

del presente documento, se determina que efectivamente el componente humano es una de piezas que conforman la ciberseguridad, siendo que los usuarios de las tecnologías tienen un rol fundamental no solo en custodiar la información, sino también en utilizar de manera adecuada el parque tecnológico, ya que al estar comprometidos con esto, serán vigilantes ante cualquier intento de violación a la plataforma de servicios tecnológicos o bien, adoptarán hábitos que promuevan un ambiente tecnológico seguro.

Pregunta #2: Cuán importante considera usted que los funcionarios de la CCSS tengan una cultura de ciberseguridad?

Tabla N° 5

Importancia de que los funcionarios de la Caja Costarricense de Seguro Social tengan cultura de ciberseguridad

Variable	***Valor absoluto***	***Valor relativo***
No es importante	0	0
Un poco importante	0	0
Importante	0	0
Muy importante	7	1

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

La tabla anterior describe que el total de encuestados consideran que es muy importante que los funcionarios de la Caja Costarricense de Seguro Social tengan una cultura de ciberseguridad. Este dato permite mostrar que en la institución las jefaturas encargadas de proteger y brindar los servicios tecnológicos son conscientes de la importancia y necesidad de promover una cultura de ciberseguridad como parte de las acciones que deben llevarse a cabo a fin de prevenir un ciberataque. Este dato es de gran relevancia ya que los lideres de una organización vienen a ser los que impulsan no solo las estrategias, sino también a generar a través de su ejemplo e impulso los cambios que se requieran para la mejora continua, en ese

sentido, entendiendo que es necesaria una cultura de ciberseguridad en las instituciones y siendo que las jefaturas de esta unidad son las que brindan la estrategia y acciones para que a nivel institucional se manejen todos los elementos necesarios para la buena gestión de las TIC se puede ver apertura hacia el tema de cultura de ciberseguridad en la institución.

Variable 2:

Actividades para fomentar cultura de ciberseguridad, enfocada en el objetivo de identificar cuáles son las actividades que se llevan a cabo actualmente en la Caja Costarricense de Seguro Social para fomentar una cultura de ciberseguridad en los usuarios internos de los servicios informáticos. A continuación, las preguntas asociadas a esta variable:

Pregunta #4: ¿Actualmente se promueve de manera formal y estructurada una estrategia de desarrollo y fortalecimiento de la cultura de ciberseguridad en los usuarios internos de los servicios informáticos en la CCSS?

Tabla N° 6

Promoción de una estrategia formal y estructurada para el desarrollo y fortalecimiento de la cultura de ciberseguridad en la Caja Costarricense de Seguro Social

Variable	***Valor absoluto***	***Valor relativo***
Si se promueve	7	1
No se promueve	0	0
No sabe / No responde	0	0

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

El total de entrevistados concordó con que actualmente se promueve de manera formal y estructurada una estrategia de desarrollo y fortalecimiento de la cultura de ciberseguridad en los usuarios internos de los servicios informáticos de la Caja Costarricense de Seguro Social a través del envío de capsulas informativas a los usuarios por medio de correo electrónico. Para este punto, se obtuvieron durante la aplicación de la entrevista los comentarios relaciondos con que existe un plan que se desarrolla pero el mismo se está haciendo con los recursos humanos disponibles los cuales no son muchos dado el aumento en el volumen de trabajo y el estancamiento en la asignación de plazas para la contratación de personal en la institución.

Pregunta #5 ¿Existe un plan actualizado, posterior al ciberataque del 31 de mayo de 2022 en la CCSS, en acciones que tendrán como objetivo aumentar de forma gradual el acercamiento a la concientización en ciberseguridad?

Tabla N° 7

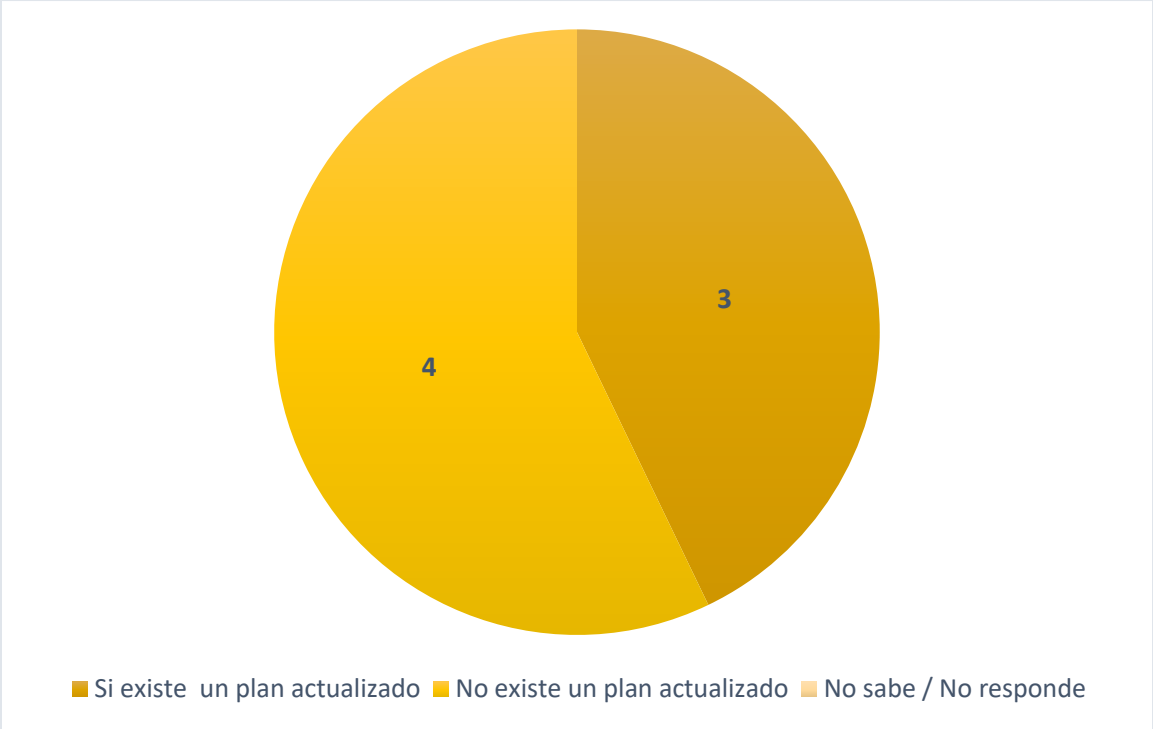
Existencia de un plan actualizado posterior al ciberataque del 31 de mayo de 2022 con acciones para el aumento y concientización en ciberseguridad

Variable	***Valor absoluto***	***Valor relativo***
Si existe un plan actualizado	3	0,42
No existe un plan actualizado	4	0,57
No sabe / No responde	0	0

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Gráfico N° 1

Existencia de un plan actualizado para concientización en ciberseguridad posterior al ciberataque del 31 de mayo de 2022



Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Para esta pregunta cuatro de las siete jefaturas consultadas indicaron que si existe un plan actualizado, posterior al ciberataque del 31 de mayo de 2022 en la CCSS, con acciones que tendrán como objetivo aumentar de forma gradual el acercamiento a la concientización en ciberseguridad. Por otro lado, tres de las siete jefaturas indican que no existe el plan. Durante el desarrollo de la entrevista se pudo comprender que la diferencia de opiniones radica en que efectivamente se realizó un plan para el reforzamiento de la ciberseguridad en la institución pero el mismo abarca no solo temas de concientización sino también técnicos, en ese sentido, las jefaturas que indicaron que no existe, es dado que el plan de reforzamiento en cultura de

ciberseguridad aún permanece como iniciativa y no ha pasado a proyecto, por lo cual si bien es cierto está establecido el que debe realizarse y se dará una fecha para el inicio de su realización aún no está conceptualizado completamente.

Ahora bien, las restantes cuatro jefaturas indicaron que el plan y la iniciativa está y que se creó tomando en cuenta el ciberataque sufrido así como también el análisis previo al ciberataque realizado de la necesidad del mismo, por lo que en su criterio el plan existe.

Pregunta #7: ¿Existe una hoja de ruta para ir aumentando la cultura de ciberseguridad de la organización a lo largo de los años?

Tabla N° 8

Existencia de una hoja de ruta para aumentar la cultura de ciberseguridad en la Caja Costarricense de Seguro Social a lo largo de los años

Variable	***Valor absoluto***	***Valor relativo***
Si existe una hoja de ruta	7	1
No existe una hoja de ruta	0	0
No sabe / No responde	0	0

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

La totalidad de jefaturas respondieron que en la Caja Costarricense de Seguro Social existe una hoja de ruta para ir aumentando la cultura de ciberseguridad de la organización a lo largo de los años. Para esta pregunta durante la realización de las entrevistas se indicó que esta hoja de ruta está incluida en las iniciativas para el reforzamiento la ciberseguridad de la institución, sin embargo, no ha podido gestionarse en su totalidad dada la falta de recurso humano que enfrenta la Dirección de Tecnologías de Información y Comunicaciones.

De acuerdo con la información antes brindada, se puede observar que actualmente esa hoja de ruta está plasmada como iniciativa, sin embargo, su ejecución aún no es del todo delimitada.

Pregunta #8: ¿La CCSS brinda información constante o periódicamente a los usuarios internos de los servicios TIC en temas de ciberseguridad?

Tabla N° 9

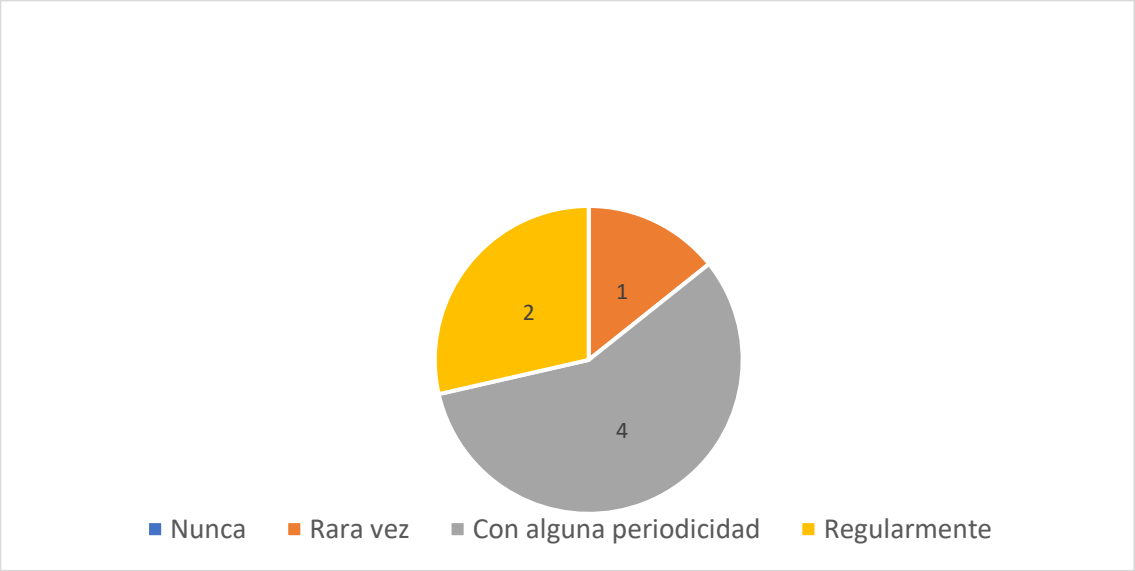
Entrega de información constante o periódica a los usuarios de los servicios TIC de la Caja Costarricense de Seguro Social, en temas de ciberseguridad

Variable	***Valor absoluto***	***Valor relativo***
Nunca	0	0
Rara vez	1	0,14
Con alguna periodicidad	4	0,57
Regularmente	2	0,28

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Gráfico N° 2

Periodicidad de entrega de información sobre ciberseguridad a usuarios de servicios TIC de la Caja Costarricense de Seguro Social



Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Para esta pregunta se utilizaron variables ordinales para brindar las respuestas, como resultado, se obtuvieron datos y percepciones distintas, siendo que cuatro de las siete jefaturas indicaron que con alguna periodicidad se entrega información constante a los usuarios de los servicios TIC de la Caja Costarricense de Seguro Social en temas de ciberseguridad; dos de las siete jefaturas indicaron que regularmente se entrega información constante sobre temas de ciberseguridad y una jefatura indicó que rara vez se entrega ese tipo de información.

Para dicha pregunta se puede observar que la mayoría de las respuestas apuntan a que los periodos de entrega periódica ó constante de información no son constantes Enel tiempo, si bien es cierto, existen momentos en donde se hace de un momento a otro cambia la periodicidad de entrega de esa información con tendencia a la baja.

Pregunta #9: ¿La CCSS brinda información actualizada a los usuarios internos de los servicios TIC en temas de ciberseguridad?

Tabla N° 10

Entrega de información actualizada sobre ciberseguridad a usuarios internos de servicios TIC de la Caja Costarricense de Seguro Social

Variable	***Valor absoluto***	***Valor relativo***
Si se brinda información actualizada	7	1
No se brinda información actualizada	0	0
No sabe / No responde	0	0

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Los resultados observados para esta pregunta muestran que la totalidad de jefaturas concuerda con que la información que se brinda en temas de ciberseguridad a los usuarios internos de los servicios tecnológicos de la Caja Costarricense de Seguro Social es actualizada.

Los resultados muestran que existe una coordinación para que la información que se entregue sea la indicada y en el momento correcto en el tiempo para poder ser entregada, lo cual es de gran beneficio para la prevención y notificación de amenazas que pueda estar sufriendo la institución.

Pregunta #11: ¿Se están realizando periódicamente campañas de sensibilización sobre ciberseguridad dirigidas a los usuarios internos de los servicios TIC?

Tabla N° 11

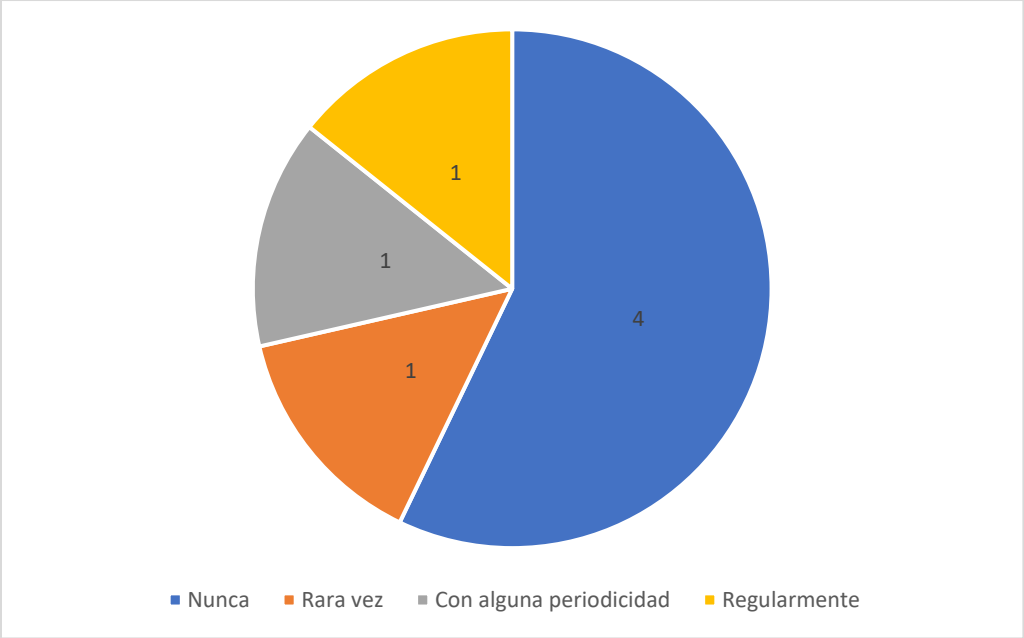
Desarrollo periódico de campañas de sensibilización sobre ciberseguridad hacia usuarios de los servicios TIC de la Caja Costarricense de Seguro Social

Variable	***Valor absoluto***	***Valor relativo***
Nunca	4	0,57
Rara vez	1	0,14
Con alguna periodicidad	1	0,14
Regularmente	1	0,14

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Gráfico N° 3

Periodicidad de campañas de sensibilización en ciberseguridad a usuarios internos de los servicios TIC de la Caja Costarricense de Seguro Social



Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Como se puede observar, para esta pregunta, cuatro de las siete jefaturas concuerdan con que no se están realizando campañas de sensibilización sobre ciberseguridad, asimismo, para las variables ordinales, rara vez, con alguna periodicidad y regularmente, solamente una jefatura indicó cada una de dichas opciones.

El resultado de esta pregunta muestra que mas de la mitad concuerda con que no se están realizando campañas de sensibilización, de acuerdo con los datos obtenidos durante la aplicación de la entrevista a las jefaturas, se puede observar que los que respondieron utilizando el resto de variables, cree que las campañas de sensibilización corresponden a brindar alguna información sobre temas de ciberseguridad por medio de correo electrónico como se viene realizando por lo cual indicaron dichas opciones.

Variable 3

Gestión del cambio, que se enfoca en el objetivo de valorar elementos que permitan llevar a cabo una cultura de ciberseguridad en la Caja Costarricense de Seguro Social. A continuación, las preguntas asociadas a esta variable:

Pregunta #3: En una escala de 0 a 10, donde 0 es nada y 10 es el valor máximo ¿Cuál es el nivel de cultura de ciberseguridad que considera usted que existe dentro de la CCSS?

Tabla N° 12

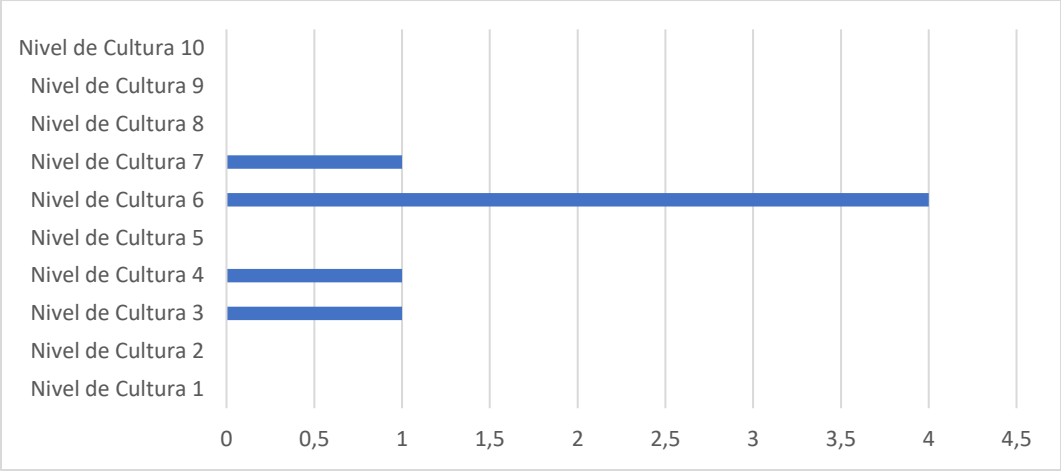
Percepción sobre nivel de cultura de ciberseguridad en la Caja Costarricense de Seguro Social.

Nivel percepción cultura ciberseguridad	***Valor absoluto***	***Valor relativo***
Nivel de Cultura 1	0	0
Nivel de Cultura 2	0	0
Nivel de Cultura 3	1	0,14
Nivel de Cultura 4	1	0,14
Nivel de Cultura 5	0	0
Nivel de Cultura 6	4	0,57
Nivel de Cultura 7	1	0,14
Nivel de Cultura 8	0	0
Nivel de Cultura 9	0	0
Nivel de Cultura 10	0	0

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Gráfico N° 4

Percepción de jefaturas estratégicas sobre el nivel de cultura de ciberseguridad en la Caja Costarricense de Seguro Social



Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Los datos obtenidos en esta pregunta concluyen con que cuatro de las siete jefaturas consideran que el nivel de cultura de ciberseguridad de los usuarios internos de los servicios tecnológicos de la Caja Costarricense de Seguro Social en una escala del 0 al 10 donde cero es nada y diez el valor máximo, es 6; mientras que los valores 6, 4 y 7 solamente una jefatura los está considerando.

Con los datos obtenidos, se puede observar que la percepción es variada, sin embargo, se mantiene en un intermedio, lo cual ofrece una oportunidad para no partir de cero en términos de establecer una estrategia, ya que se ve que si existe percepción sobre algún conocimiento básico.

Pregunta #6: ¿Existe una medición posterior al ciberataque del nivel de conocimiento, concientización y hábitos de ciberseguridad en los funcionarios de la CCSS?

Tabla N° 13

Existencia sobre medición de concientización y hábitos ciberseguridad posterior al ciberataque del 31 de mayo de 2022

Variable	*Valor absoluto*	*Valor relativo*
Si existe una medición	0	0
No existe una medición	7	1
No sabe / No responde	0	0

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Para esta pregunta, la totalidad de jefaturas concluyeron con que no se ha realizado un estudio del nivel de conocimiento, concientización y hábitos de ciberseguridad en los usuarios internos de los servicios tecnológicos de la Caja Costarricense de Seguro Social posterior al ciberataque sucedido el 31 de mayo de 2022.

Este dato es de suma importancia ya que dicho ciberataque impactó el funcionamiento de toda la institución lo cual de cierta manera genera en las personas lecciones aprendidas y puede acarrear un interés por parte de los funcionarios por mejorar los hábitos de ciberseguridad, lo cual puede ser aprovechado con el fin de concientizar y educar a una de las partes mas importantes de la ciberseguridad: el componente humano.

Pregunta #10: ¿Existe un responsable formal de desplegar el entrenamiento requerido de concientización en ciberseguridad?

Tabla N° 14

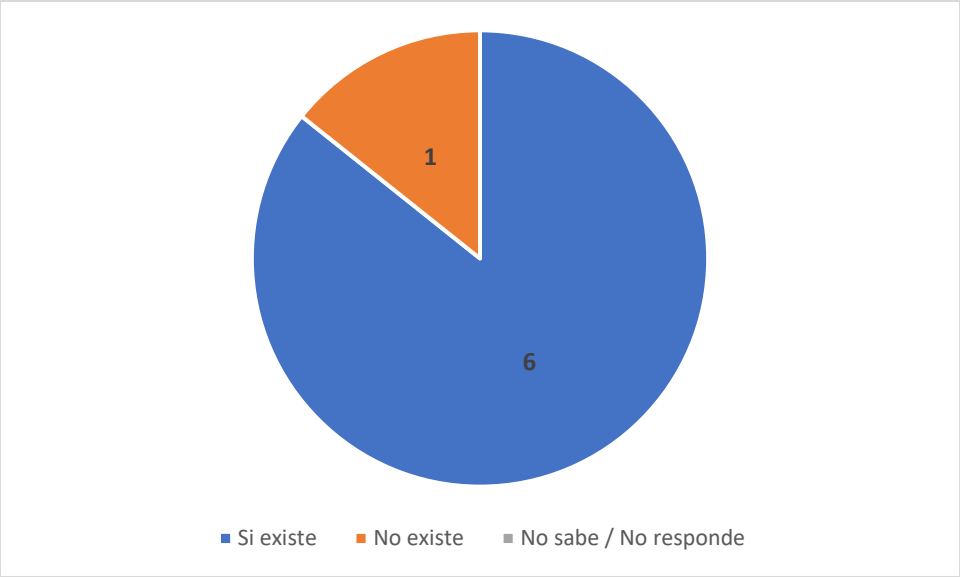
Existencia de un responsable de desplegar entrenamiento para concientización en ciberseguridad

Variable	*Valor absoluto*	*Valor relativo*
Si existe	6	0,85
No existe	1	0,14
No sabe / No responde	0	0

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Gráfico N° 5

Existencia de un responsable de desplegar entrenamiento para concientización en ciberseguridad



Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Según la encuesta aplicada, seis de las siete jefaturas de la Dirección de Tecnologías de Información y Comunicaciones, indica que existe un responsable formal de desplegar el

entrenamiento requerido de concientización en ciberseguridad, siendo que solamente una jefatura considera que no existe.

Para el análisis de datos de esta pregunta, se toma en cuenta lo indicado verbalmente durante la aplicación de la entrevista a las jefaturas, en donde se indica que si existe un funcionario capacitado para brindar entrenamientos sobre concientización en ciberseguridad, mismo que ha brindado algunas capacitaciones, por lo cual responden que si existe, sin embargo, la jefatura que indica que no existe, hace referencia a que este funcionario si bien es cierto ha brindado entrenamientos y tiene la expertiz actualmente está realizando una gran cantidad de tareas operativas de gran criticidad lo cual le impide brindar una cantidad de tiempo suficiente para realizar estas actividades de concientización. A partir de dicho hecho y de otros observados durante la aplicación de las encuestas, existe un faltante de personal que permita desarrollar las actividades requeridas en tiempo y forma para fortalecer una cultura de ciberseguridad en la institución.

Pregunta # 12: ¿Existe recurso humano suficiente dentro de la DTIC para desarrollar y ejecutar un plan para el fortalecimiento de la cultura de ciberseguridad en la CCSS?

Tabla N° 15

Existencia de recurso humano suficiente para desarrollar y ejecutar un plan para el fortalecimiento de la ciberseguridad en la Caja Costarricense de Seguro Social

Variable	***Valor absoluto***	***Valor relativo***
Si existe	0	0
No existe	7	1
No sabe / No responde	0	0

Fuente: Encuesta a Jefaturas de la Dirección de Tecnologías de Información y Comunicaciones que tengan relación con temas de ciberseguridad, mayo 2023.

Para esta pregunta se obtuvo la totalidad de respuestas indicando que no existe el recurso humano suficiente dentro de la Dirección de Tecnologías de Información y Comunicaciones para desarrollar y ejecutar un plan para el fortalecimiento de la cultura de ciberseguridad en la Caja Costarricense de Seguro Social.

Si bien es cierto, esta fue la última pregunta del formulario, desde el inicio y a través de las conversaciones desarrolladas a partir de la aplicación de la encuesta se logró detectar que una de las oportunidades de mejora para el desarrollo de una cultura de ciberseguridad en esta institución es el asignar recurso humano a esta Dirección, específicamente en la Subárea Seguridad Informática laboran cinco personas las cuales tienen a cargo toda la gestión de ciberseguridad de la institución.

Capitulo V Conclusiones y recomendaciones

Conclusiones

El año 2022 fue histórico para la Caja Costarricense de Seguro Social en materia de ciberseguridad, siendo que el 31 de mayo fue víctima de un ciberataque. Los hackers se aprovecharon de las vulnerabilidades en materia de ciberseguridad para irrumpir en la plataforma tecnológica y acceder a información institucional, lo cual provocó que al tratar de bloquear a estos ciberdelincuentes el funcionamiento de los sistemas de las instituciones se paralizara afectando la prestación de los servicios.

Esta institución gubernamental, para poder brindar sus servicios de salud, pensiones y recaudación, depende de la información, sistemas y soluciones tecnológicas, de ahí la importancia de la ciberseguridad que permite resguardar los procesos tecnológicos y asegurar la prestación de los servicios. Considerando esto, el ciberataque desembocó en una alteración de la continuidad de los servicios provocando que se tuvieran que poner en funcionamiento los planes de continuidad del negocio.

Ahora bien, a lo largo de esta investigación se logró determinar la importancia de la ciberseguridad y los elementos que la conforman, siendo el elemento humano uno de los principales. Para comprender esto, se hizo importante conocer el significado de procesos tales como seguridad informática, seguridad de la información y ciberseguridad; siendo que seguridad informática corresponde a los procesos utilizados para proteger la infraestructura tecnológica (redes, equipos, servidores, etc); seguridad de la información corresponde a los procesos que se realizan en una institución con el fin de asegurar que la información no sea divulgada o modificada por personas no autorizadas, siendo que se generan las normas para su uso, resguardo y procesamiento; finalmente la ciberseguridad comprende las actividades para

defender los sistemas interconectados y comprende a la vez la seguridad de la información, es por ello, que uno de los elementos esenciales de la misma es el factor humano.

Se pudo comprender que el ser humano es uno de los elementos que componen la ciberseguridad, y el más débil en la protección de los sistemas y la información dada la falta de capacitación y concientización que muchas veces existe en los usuarios de las tecnologías. En ese sentido, y tomando en consideración que el objetivo general de este proyecto de investigación consiste en analizar la importancia de una cultura de ciberseguridad para la Caja Costarricense de Seguro Social se pudo concluir:

- La ciberseguridad comprende varios elementos, en lenguaje técnico se le conocen como capas de protección, los mismos son las personas, los procesos y la tecnología. Cada uno debe ser gestionado correctamente con el fin de proteger la infraestructura tecnológica y la información. Para abordar el elemento “persona” se debe gestionar la cultura de seguridad en las organizaciones la cual se enfoca en conocimientos, hábitos normas, valores y otros aspectos que permitan gestionar buenos hábitos en las personas con respecto al uso de las tecnologías de información.

- Existen normas tales como la ISO 27701, que se encargan de brindar los aspectos necesarios para desarrollar un Sistema de Gestión de Seguridad de la Información. Esta norma se enfoca en tres principios de gestión los cuales se basan en enfoque al cliente, liderazgo y participación de las personas. En virtud de esto, se puede concluir que el elemento persona es fundamental para proteger la información y los sistemas de un ataque cibernético o bien de un uso inadecuado o no autorizado de la información.

- La cultura de ciberseguridad es crucial para robustecer la seguridad de las tecnologías en una empresa, esto ya que no importa lo actualizada que se encuentre una plataforma

tecnológica, procedimientos y sistemas de seguridad, el punto más vulnerable es y ha sido siempre el usuario, el manejo que le de a las tecnologías y la información que comparte. En ese sentido, la cultura de ciberseguridad comienza con la capacitación, formación y concientización de los usuarios de las tecnologías.

- El componente gestión del cambio es un elemento crucial al momento de establecer una estrategia de concientización y educación en ciberseguridad, esto ya que permite definir los análisis y hoja de ruta para generar un cambio en la forma de hacer las cosas, manejando de manera adecuada las resistencias y con ello facilitando la entrada de la nueva manera de hacer y ver las cosas.

- Tomando en cuenta elementos teóricos que indican que la cultura de ciberseguridad forma parte de los elementos esenciales para proteger los sistemas y la información de una institución, así como la opinión de todas las jefaturas que tienen que ver con temas de ciberseguridad en la Caja Costarricense de Seguro Social que indican que el compromiso de los usuarios de los servicios TIC con la ciberseguridad impacta en gran cantidad en el riesgo cibernético, se concluye que es fundamental realizar actividades que permitan generar una concientización hacia la buenas prácticas en el uso de las tecnologías y manejo de la información.

- Se concluye que todas las jefaturas que tienen que ver con temas de ciberseguridad en la Caja Costarricense de Seguro Social, consideran que es muy importante que los funcionarios de la CCSS tengan una cultura de ciberseguridad, lo cual coincide con los aspectos teóricos que se pudieron investigar en fuentes tales como normas internacionales y firmas consultoras expertas en temas informáticos. En ese sentido, se entiende que es vital una cultura de ciberseguridad en la institución con el fin de reducir riesgos de ciberataques y mal uso de la información

- De acuerdo a las entrevistas realizadas a las jefaturas que tienen relación directa con temas de ciberseguridad en la Caja Costarricense de Seguro Social se conoce que actualmente la institución cuenta con una iniciativa formal y estructurada para el desarrollo y fortalecimiento de la cultura de ciberseguridad en los usuarios internos de los servicios informáticos en la CCSS, sin embargo la misma no ha podido ser implementada con la constancia esperada.

- Previo al ciberataque existían un proyecto llamado Cibertic, tendiente a establecer un Plan Táctico de Ciberseguridad, el cual tenía por objetivo prevenir y mitigar las vulnerabilidades y amenazas a la seguridad informática, desde una perspectiva táctica y operativa, sin embargo el 31 de mayo del 2022, la Institución sufrió un ciberataque que obligó a la desconexión de los servicios y sistemas institucionales, razón por lo cual se reorientaron los esfuerzos que se estaban realizando en esta materia y la Dirección de Tecnologías de Información y Comunicaciones se enfocó en la habilitación de los servicios tecnológicos y a la protección de su infraestructura y plataformas. Posterior a ello, se creó un plan de fortalecimiento a dicho proyecto con una serie de lecciones aprendidas y procesos de mejora que deben ser incorporados en los esfuerzos que la Institución venía realizando en materia de ciberseguridad, por lo que se encuentra dentro de dichas iniciativas el establecer un plan de concientización en ciberseguridad.

- La Dirección de Tecnologias de Información y Comunicaciones brinda alguna información a los usuarios internos de los servicios TIC en temas de ciberseguridad, sin embargo, el envío de esta información no tiene la periodicidad esperada, esto de acuerdo con la encuesta realizada a las jefaturas de la institución que tiene relación directa con temas de ciberseguridad. El motivo que refieren es la falta de personal que pueda apoyar esta

labor de informar, educar y concientizar en estos temas, ya que actualmente la Subárea Seguridad Informática cuenta con cinco funcionarios incluyendo la jefatura.

- De acuerdo con la encuesta realizada para este proyecto de investigación se conoce que la Dirección de Tecnologías de Información y Comunicaciones CCSS brinda información actualizada a los usuarios internos de los servicios TIC en temas de ciberseguridad como parte de las actividades que se llevan a cabo actualmente en la Caja Costarricense de Seguro Social para fomentar una cultura de ciberseguridad en los usuarios internos de los servicios informáticos, sin embargo, la periodicidad no es regular, y no se visualiza que exista alguna medición del impacto de estas campañas.

- Para desarrollar una cultura de ciberseguridad en la Caja Costarricense de Seguro Social se deben tomar elementos tales como capacitación a los funcionarios en temas de ciberseguridad, envío de información constante en relación con riesgos que se estén enfrentando, campañas de sensibilización, realizar un proceso continuo de implementación de cultura que permita la medición del avance y el mantenimiento.

- La Dirección de Tecnologías está realizando actividades con el fin de promover una cultura de ciberseguridad, sin embargo, de acuerdo con las entrevistas realizadas se observa que las actividades no son tan periódicas lo cual no genera la permanencia de la cultura, las estrategias deben mantenerse actualizadas y en constante acción para que los funcionarios estén preparados ante cualquier amenaza.

- Se concluye que establecer una cultura de ciberseguridad que se mantenga en el tiempo, que esté en constante medición y cuente con el apoyo de los altos jerarcas de la institución es imperante con el fin de salvaguardar la plataforma tecnológica de la

institución así como la información que la misma contiene, con ello se logra mantener la correcta prestación de servicios reduciendo el riesgo de una posible interrupción de los mismos a causa de un ciberataque.

Recomendaciones

- Con el fin de abordar el elemento persona se recomienda realizar un plan de concientización en ciberseguridad con actividades que permitan aumentar de manera gradual el entendimiento sobre el problema que acarrea el no manejar las herramientas tecnológicas ni la información de acuerdo con políticas y hábitos que permitan salvaguardar los sistemas y la información de la institución.

- Se recomienda al momento de realizar las campañas de concientización en ciberseguridad, mencionar que existen normas y teoría que fundamenta la importancia de que el usuario maneje las tecnologías responsablemente con el fin de evitar fugas de información o un ciberataque, esto por cuanto vendría a reforzar la iniciativa dando credibilidad y elementos técnicos.

- Se recomienda crear un plan de capacitación que permita educar a los usuarios internos de los servicios TIC en temas de ciberseguridad con la información necesaria que permita generar el conocimiento para evitar cualquier fuga de información o debilidad a nivel de ciberseguridad en la institución.

- Se recomienda que al momento de implementar y desarrollar un plan para establecer una cultura de ciberseguridad se tome en cuenta alguna metodología de gestión del cambio que permita facilitar la transición al nuevo estado futuro en virtud de los elementos que

contempla y el manejo que permite dar a las resistencias que puedan aparecer en el camino.

- Se recomienda que se generen espacios de concientización para los altos mandos de la institución con el fin de que los mismos apoyen el instaurar una cultura de ciberseguridad sostenida en el tiempo, a través del ejemplo y línea estratégica que estos brindan.

- Se recomienda que las jefaturas a través de los esquemas de estrategia que generan focalicen parte de sus esfuerzos en concientizar y brindar ejemplo hacia los colaboradores de la institución de la necesidad de que el manejo de las tecnologías se haga de forma segura, asimismo, dadas su obligaciones en la materia, impulsen en cada uno de los elementos de su gestión la estrategia para establecer una cultura de ciberseguridad en la institución.

- Se recomienda que para la implementación del plan reforzado de ciberseguridad, se incluya dentro de cada una de sus iniciativas campañas de concientización y educación para los usuarios de los servicios TIC y los involucrados de llevar a cabo las iniciativas, esto dentro de los alcances de cada iniciativa.

- Tomando como referencia el proyecto cibertic que se gesta en la Dirección de Tecnologías de Información y Comunicaciones, se recomienda dar inicio con la implementación de una estrategia de concientización a más tardar el segundo semestre del 2023 con el fin de ir minimizando los riesgos que puedan haber en materia de ciberataques.

- En virtud de la falta de personal interno en la Dirección de Tecnologías de Información y Comunicaciones para apoyar el desarrollo de una cultura de ciberseguridad y en vista de la cantidad de recurso informático que se visualiza en Centros de Gestión Informática de la Institución, se recomienda solicitar apoyo para que desde los mismos, se generen redes de cambio que permitan impulsar esta cultura desde el apoyo a la generación de la estrategia.
- Tomando como referencia que actualmente se brinda información actualizada a los usuarios internos de los servicios TIC en temas de ciberseguridad pero que la periodicidad no es regular, y no se visualiza que exista alguna medición del impacto de estas campañas, se recomienda generar métricas o herramientas que permitan medir el grado de cultura de ciberseguridad con el fin de tender estrategias para las brechas que se vayan detectando en el camino.
- Se recomienda conformar un equipo de trabajo que además de incluir personal técnico como lo son ingenieros informáticos, que dada la temática y expertiz son requeridos , se deben involucrar también administradores de empresas ya que por su perfil experto en planificar, organizar, dirigir y controlar recursos, tiene la formación necesaria para poder guiar los procesos propios de la gestión del cambio.
- Con el fin de poner en marcha y mantener operando el plan de concientización y capacitación en ciberseguridad, se recomienda solicitar apoyo de funcionarios de otras áreas adscritas a la Dirección de Tecnologías de Información y Comunicaciones, Centros de Gestión Informática y unidades del negocio, con el fin de apoyar a la Subárea Seguridad Informática, esto ya que por su limitada cantidad de personal no se le hace posible realizar actividades de este tipo con la periodicidad requerida.
- Como parte del análisis realizado a los datos obtenidos de la encuesta y a la información teórica consultada, se recomienda que es necesario desarrollar e implementar a partir del

segundo semestre del 2023 un plan de trabajo para el desarrollo de cultura de ciberseguridad en usuarios internos de los servicios TIC de la Caja Costarricense de Seguro Social para el año 2023 como la que se anexa a este proyecto de investigación que sea liderada por personal con perfil de administración, esto dado que se visualiza que para la gestión de esta cultura solamente se está involucrando personal técnico que además de encontrarse casi que en la totalidad de su tiempo atendiendo labores críticas dentro de la plataforma tecnológica, no tiene la formación que posee un administrador de empresas para impulsar un tema que tiene componentes propios de las ciencias sociales.

Capítulo VI Propuesta de mejora

En virtud de las conclusiones y recomendaciones vertidas en este proyecto de investigación y dada la necesidad que se encuentra de definir una hoja de ruta clara respecto a la concientización en ciberseguridad para usuarios internos de los servicios TIC de la Caja Costarricense de Seguro Social, se presenta propuesta para dar inicio con la implementación de una cultura de ciberseguridad en la institución. Esta propuesta se basa en elementos básicos al momento de implementar una gestión del cambio, lo cual viene a apoyar a los colaboradores en el proceso de aceptación del cambio durante la transición a un nuevo estado futuro. Un proceso de cambio bien administrado facilita el entendimiento del cambio, la atención de las inquietudes que pueden surgir del personal, el apoyo a las personas durante el proceso y la generación del compromiso.

Objetivo general

Proponer a la Dirección de Tecnologías de Información y Comunicaciones un plan de trabajo para fomentar una cultura de ciberseguridad en los usuarios internos de los servicios TIC para el año 2023.

Descripción de actividades

A continuación, se describen los pasos a seguir para fomentar un cambio de mentalidad para el uso seguro de las TIC a través del uso del componente de Gestión de Cambio, con el fin de proveer una planificación detallada que oriente la ejecución de las actividades.

Para conceptualizar la metodología de trabajo dentro de los elementos que compone una gestión de cambio, se tienen marcadas tres dimensiones guía que permitirán su desarrollo, a saber:

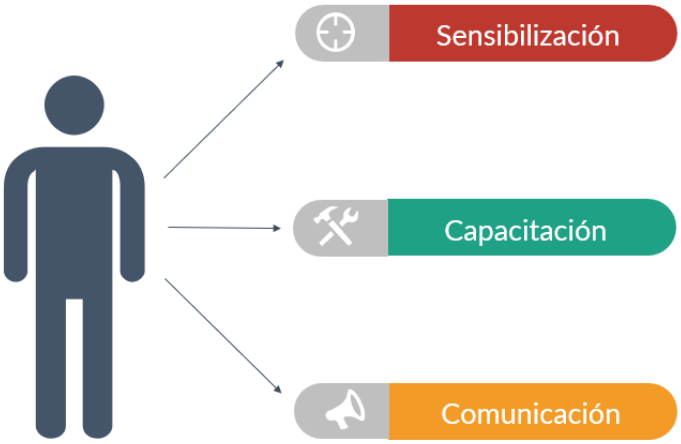


Ilustración 4 Dimensiones de Gestión del Cambio

Fuente: Elaboración propia (2023)

A continuación, se detallan los pasos que se estarán utilizando para desarrollar la propuesta para fomentar un cambio de mentalidad para el uso seguro de las TIC:

Planificación

La planificación de las actividades contemplará el desarrollo de los siguientes puntos:

Definición de responsables

La definición de responsables corresponde a una etapa vital dentro de la propuesta para fomentar una cambio de mentalidad en el uso seguro de las TIC, esto ya que van a ser estos responsables los encargados de realizar la definición de actividades, contenidos e implementación del cronograma de trabajo.

Actividades de sensibilización

Las actividades de sensibilización son un punto medular en el cambio de mentalidad para el uso seguro de las TIC, esto ya que deben mostrar el problema y con esto generar conciencia en el cambio que se debe hacer para controlar los riesgos de ciberataques y mal uso de la información contenida en los sistemas institucionales.

Las actividades de sensibilización se deben desarrollar en dos líneas, la primera enfocada en los altos mandos, ya que de ellos se requiere de su apoyo para poder desarrollar las estrategias de capacitación y comunicación, asimismo, el obtener los recursos necesarios. La segunda línea se enfoca en los usuarios internos de los servicios TIC, los cuales son la población meta a impactar.

Definición de capacitaciones requeridas.

Este punto es de vital importancia ya que de aquí parte la educación en ciberseguridad que es requerida para poder minimizar los riesgos cibernéticos, esta debe adecuarse a las necesidades y particularidades de los distintos involucrados, este proceso se convierte en una herramienta importante para derribar temores, mitos y resistencias generadas por los procesos de cambio y evolución.

Las capacitaciones deben realizarse a todos los usuarios de los servicios TIC de la Caja Costarricense de Seguro Social, se recomienda que las mismas se incluyan en el curso de inducción a los nuevos trabajadores de la institución y sean realizadas al menos una vez al año a todos los funcionarios con el fin de crear sostenibilidad en el cambio.

Definición de plan de comunicaciones

El plan de comunicaciones es un elemento fundamental para dar sostenibilidad al cambio que se busca generar, asimismo, continuar con la tarea de capacitar, informar y prevenir. Es importante tomar en cuenta que este plan debe llevar un orden lógico en el material que se comparte. Un aspecto relevante para este punto es impactar la población institucional en la manera que lo requieren, así como también encontrar el canal de comunicación más efectivo.

Implementación

La implementación del plan de trabajo incluye la realización de actividades que se relacionan con, capacitaciones, reuniones, actividades de sensibilización, publicación de comunicados que permitan trabajar sobre la temática de cultura de ciberseguridad.

Sostenibilidad del cambio

Durante la ejecución de las actividades se debe estar midiendo su avance, los nuevos requerimientos, las expectativas y el conocimiento de las personas, con el objetivo de potenciar las actividades que se planificaron para gestionar el cambio.

Para lo anterior, se deberán llevar a cabo reuniones de seguimiento bimensuales con los encargados de gestionar el plan.

En las sesiones se estará revisando el avance del cronograma, realizando actividades de retroalimentación, analizando si han existido obstáculos, si existen nuevos requerimientos,

revisando los logros obtenidos. Lo anterior, con el fin de observar si es requerida la realización de actividades extra, como lo son encuestas, reuniones individuales o grupales, talleres.

Tabla N° 16

Propuesta de plan de trabajo

Propuesta de Plan de Trabajo Desarrollo de cultura de ciberseguridad en usuarios internos de los servicios TIC de la Caja Costarricense de Seguro Social para el año 2023	
Tareas	**Detalle de actividades**
Definición de Equipo de Trabajo	
Definición de equipo para el desarrollo de cultura de ciberseguridad en usuarios internos de Servicios TIC de la CCSS	Validar el perfil del equipo conductor Seleccionar el equipo conductor
Preparar la inducción para el equipo conductor	Preparar presentación para inducción a equipo
Generar inducción al equipo conductor	Realizar sesión de inducción
Sensibilización a altas Gerencias para que apoyen la implementación de una cultura de ciberseguridad	
Diseño del taller de sensibilización	Definir enfoque del taller Validar enfoque del taller Preparar material
Seleccionar población participante	Realizar sesión para definir población participante
Ejecutar talleres de sensibilización	Realizar el taller
Sensibilización para usuarios internos de los servicios TIC en general	
Diseño del taller de sensibilización	Definir enfoque del taller Validar enfoque del taller Preparar material
Seleccionar población participante	Definir población participante
Ejecutar talleres de sensibilización	Realizar el taller
Comunicación	

Preparar mensajes de comunicación	Realizar una sesión de trabajo para identificar los mensajes clave a generar y poblaciones impactadas.
	Definir medios de comunicación
	Definir arte y redacción de mensajes
	Realizar cronograma para difusión de mensajes
Capacitación	
Preparar plan de capacitación virtual	Realizar una sesión de trabajo para identificar el contenido de las capacitaciones y orden de los funcionarios a capacitar
	Definir modalidad de capacitaciones
	Realizar cronograma para implementación de capacitaciones
Sostenibilidad	
Definir la propuesta de instrumento que se utilizará en sesion de encargados de gestionar la cultura de ciberseguridad	Definir instrumento de evaluación de sostenibilidad de cultura ciberseguridad
	Validar instrumento de evaluación de sostenibilidad de cultura ciberseguridad
Definir cronograma sesiones de seguimiento	Realizar cronograma de sesiones y llevarlas a cabo
Definición del Plan de Gestión del Cambio para el año 2024	
Revisar los resultados del primer ciclo del Plan de Gestión del Cambio de acuerdo con el instrumento creado para la sostenibilidad	Realizar sesión de análisis de resultados y lecciones aprendidas
Definir el Plan de desarrollo de cultura de ciberseguridad para el año 2024	Definir plan para el segundo ciclo
	Validar plan para el segundo ciclo
	Realizar ajustes para el plan del segundo ciclo

Fuente: elaboración propia (2023)

Tabla N° 17

Cronograma de implementación

Desarrollo de cultura de ciberseguridad en usuarios internos de los servicios TIC de la Caja Costarricense de Seguro Social para el año 2023									
Tareas	**Detalle de actividades**								
Definición de Equipo de Trabajo		***Inicio***	***Fin***	***Jul***	***Ago***	***Set***	***Oct***	***Nov***	***Dic***
Definición de equipo para el desarrollo de cultura de ciberseguridad en usuarios internos de Servicios TIC de la CCSS	Validar el perfil del equipo conductor	3/07/2023	05/07/2023						
	Seleccionar el equipo conductor	3/07/2023	05/07/2023						
Preparar la inducción para el equipo conductor	Preparar presentación para inducción a equipo	06/07/2023	12/07/2023						
Generar inducción al equipo conductor	Realizar sesión de inducción	15/07/2023	19/07/2023						
Sensibilización a altas Gerencias para que apoyen la implementación de una cultura de ciberseguridad									
Diseño del taller de sensibilización	Definir enfoque del taller	20/07/2023	27/07/2023						
	Validar enfoque del taller								
	Preparar material								
Seleccionar población participante	Realizar sesión para definir población participante								
Ejecutar talleres de sensibilización	Realizar el taller	31/07/2023	11/08/2023						
Sensibilización para usuarios internos de los servicios TIC en general									
Diseño del taller de sensibilización	Definir enfoque del taller	31/07/2023	16/08/2023						
	Validar enfoque del taller								
	Preparar material								
Seleccionar población participante	Definir población participante								
Ejecutar talleres de sensibilización	Realizar el taller	17/08/2023	8/09/2023						

Comunicación									
Preparar mensajes de comunicación	Realizar una sesión de trabajo para identificar los mensajes clave a generar y poblaciones impactadas.	17/08/2023	15/09/2023						
	Definir medios de comunicación								
	Definir arte y redacción de mensajes								
	Realizar cronograma para difusión de mensajes								
	Distribución de comunicados	16/09/2023	31/12/2023						
Capacitación									
Preparar plan de capacitación	Realizar una sesión de trabajo para identificar el contenido de las capacitaciones y orden de los funcionarios a capacitar	18/09/2023	13/10/2023						
	Definir modalidad de capacitaciones								
	Realizar cronograma para implementación de capacitaciones								
	Implementación de Capacitaciones	16/10/2023	31/12/2023						
Sostenibilidad									
Definir la propuesta de instrumento que se utilizará en sesión de encargados de gestionar la cultura de ciberseguridad	Definir instrumento de evaluación de sostenibilidad de cultura ciberseguridad	20/07/2023	28/07/2023						
	Validar instrumento de evaluación de sostenibilidad de cultura ciberseguridad								
Definir cronograma sesiones de seguimiento	Realizar cronograma de sesiones y llevarlas a cabo	20/07/2023	22/12/2023						
Definición del Plan de Gestión del Cambio para el año 2024									
Revisar los resultados del primer ciclo del Plan de Gestión del Cambio de acuerdo con el	Realizar sesión de análisis de resultados y lecciones aprendidas								

instrumento creado para la sostenibilidad		16/10/2023	31/12/2023						
Definir el Plan de desarrollo de cultura de ciberseguridad para el año 2024	Definir plan para el segundo ciclo								
	Validar plan para el segundo ciclo								
	Realizar ajustes para el plan del segundo ciclo								

Fuente: elaboración propia (2023)

Presupuesto

Según el estudio realizado, para implementar la propuesta del plan de trabajo para el desarrollo de cultura de ciberseguridad en usuarios internos de los servicios TIC de la Caja Costarricense de Seguro Social para el año 2023 se requiere de dos ingenieros informáticos y un administrador de empresas.

Tomando en cuenta lo anterior, se analiza según el Manual Descriptivo de Puestos de la Institución la categoría que corresponden estas dos profesiones siendo que un Analista en Sistemas 4 es el Ingeniero Informático y el Profesional 4 el Administrador de Empresas. Una vez determinados los perfiles, se revisa la escala salarial de cada uno de esos puestos, utilizando el salario global transitorio de los empleados de la CCSS de conformidad con la Ley Marco de Empleo Público, Ley N°10.159 y su respectivo Reglamento.

Tomando en cuenta lo anterior, se procede a realizar el cálculo económico para la implementación del plan estimando seis meses y desglosando el costo total por cada uno de esos meses, a saber:

Tabla N° 18

Valoración económica

Periodos	Cantidad de horas	Perfil Puestos CCSS	Profesión	# de funcionarios.	Costo por hora	Costo total
1 mes	80	Analista de sistemas 4	Ingeniero Informático	2	¢4,043.40	646,944
	100	Profesional 4	Administrador de Empresas	1	¢4,043.40	404,340
2 meses	160	Analista de sistemas 4	Ingeniero Informático	2	¢4,043.40	1,293,888
	200	Profesional 4	Administrador de Empresas	1	¢4,043.40	808,680
3 meses	240	Analista de sistemas 4	Ingeniero Informático	2	¢4,043.40	1940,832
	300	Profesional 4	Administrador de Empresas	1	¢4,043.40	1,213,020
4 meses	320	Analista de sistemas 4	Ingeniero Informático	2	¢4,043.40	2,587,776
	400	Profesional 4	Administrador de Empresas	1	¢4,043.40	1,617,360
5 meses	400	Analista de sistemas 4	Ingeniero Informático	2	¢4,043.40	3,234,720
	500	Profesional 4	Administrador de Empresas	1	¢4,043.40	2,021,700
6 meses	480	Analista de sistemas 4	Ingeniero Informático	2	¢4,043.40	3,881,664
	600	Profesional 4	Administrador de Empresas	1	¢4,043.40	2,426,040

Fuente: elaboración propia, montos salariales tomados del índice salarial global transitorio empleados de la CCSS (2023).

Referencias

- Consejo de la Unión Europea. (11 de enero de 2023). Ciberseguridad: cómo combate la UE las amenazas cibernéticas. Recuperado de: https://www.consilium.europa.eu/es/policies/cybersecurity/ .
- Alan Calder. (17 de agosto de 2017). El Derecho.com Notas Jurídicas y de Actualidad . Recuperado de: https://elderecho.com/la-ciberseguridad-depende-de-tres-factores-relacionados-entre-si-las-personas-los-procesos-y-la-tecnologia.
- Caja Costarricense de Seguro Social, Gerencia Administrativa, Dirección de Desarrollo Organizacional. (Octubre 2013). Modelo de Organización de los Centros de Gestión Informática (segunda actualización)
- Caja Costarricense de Seguro Social, Gerencia Administrativa, Dirección de Desarrollo Organizacional, (Octubre 2013). Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones (segunda actualización),
- Harold Koontz; Heinz Weihrich y Mark Cannice, (2014). Administración una Perspectiva Global y Empresarial. 14 ed; Mc Graw Hill
- CISCO, ¿Qué es la ciberseguridad? Recuperado de: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html
- *Noma ISO 27001, Pilares fundamentales de un SGSI, https://www.isotools.us/2015/01/13/iso-27001-pilares-fundamentales-sgsi/*
- Universidad Piloto de Colombia. Cañón Parada Lady Johana, Ataques inf., Eth. Hacking y conciencia Seg. Inf. Niños, http://polux.unipiloto.edu.co:8080/00002427.pdf
- Malwarebytes, Definición de malware, https://es.malwarebytes.com/ransomware/

- Hellriegel, D. ; Jackson, S.E. y Slocum, J.W. (2017). Administración : Un enfoque basado en competencias. 12 ed. México D.F. : Cengage Learning
- ENISA, Acerca de ENISA – La Agencia de Ciberseguridad Europea, , https://www.enisa.europa.eu/about-enisa
- ISO TOOLS, (8 de setiembre de 2022) ¿Cómo crear una cultura de ciberseguridad en la institución?, ISO 27001:2013, , https://www.pmg-ssi.com/2022/09/como-crear-una-cultura-de-ciberseguridad-en-la-organizacion/
- ISO 450001, (29 de enero de 2020) ¿Qué es la cultura de seguridad en las organizaciones?, https://www.nueva-iso-45001.com/2020/01/que-es-la-cultura-de-seguridad-en-las-organizaciones/
- AWS, ¿Qué es la ciberseguridad?, https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20pr%C3%A1ctica,cliente%20y%20cumplir%20la%20normativa.
- Sharon Licari, HubSpot (20 de enero de 2023), ¿Qué es la gestión del cambio organizacional y por qué es importante?, , https://blog.hubspot.es/marketing/gestion-de-cambio
- Jeff Hiatt, The PROSCI, (2016) ADKAR model, Un modelo de gestión del cambio orientado a resultados para guiar cambios individuales y organizacionales.
- Jeffrey M. Hiatt ADKAR, ¿Cómo implementar de manera exitosa el cambio en nuestras vida personal y carrera?
- Hernández Sanpieri Roberto, (2018). Metodología de la Investigación: Las rutas cuantitativa, cualitativa y mixta, Me Graw Hill
- Roberto Hernández Sanpieri, Carlos Fernandez Collado, Pilar Batista Lucio (2014) Metodología de la Investigación. Editorial Mc Graw Hill

- César Augusto Bernal T. (2000). Metodología de la Investigación para la Administración y Economía. Editorial Pearson
- Rojas Soriano R, (1998) Guía para Realizar Investigaciones Sociales. Editorial Mc Graw Hill
- Sharon Licari, HubSpot, (20 de enero de 2023), ¿Qué es la gestión del cambio organizacional y por qué es importante?, https://blog.hubspot.es/marketing/gestion-de-cambio
- Briones, Guillermo. (1996) Métodos y técnicas de investigación para las ciencias sociales. México: Editorial Trillas. Varias reimpresiones a partir de la segunda edición de l996
- Guía Resumen del Estilo APA Sétima Edición (2020), Guía Resumida del Manual de Normas APA Séptima Edición.
- Caja Costarricense de Seguro Social, Dirección Administración y Gestión de Personal, Índice Salarial Global Transitorio Empleados de la CCSS, https://rrhh.ccss.sa.cr/indice_salarial/pdf/Indice_Salarial_Global_Transitorio_2023.pdf
- Caja Costarricense de Seguro Social, Dirección Administración y Gestión de Personal, Manual Descriptivo de Puestos CCSS, https://rrhh.ccss.sa.cr/portalrh/documentos/manual-puestos.pdf

Anexo

Encuesta sobre la importancia de la cultura de ciberseguridad en la Caja Costarricense de Seguro Social, (CCSS)

Introducción:

Este es un instrumento que pretende recoger alguna información básica sobre la importancia de la cultura en ciberseguridad en la Caja Costarricense de Seguro Social, de ahora en adelante en el presente documento CCSS.

Agradezco la colaboración que brindará y al ser un instrumento que se llena en forma anónima le garantizo absoluta confidencialidad.

1. **¿Cuánto considera usted que impacta el compromiso de los usuarios de los servicios TIC con la ciberseguridad en el riesgo cibernético?**

☐ No Impacta
☐ Impacta un poco
☐ Impacta mucho
☐ Impacta demasiado

2. **¿Cuán importante considera usted que los funcionarios de la CCSS tengan una cultura de ciberseguridad?**

☐No es importante
☐Un poco importante
☐Importante
☐Muy importante

3. **En una escala de 0 a 10, donde 0 es nada y 10 es el valor máximo ¿Cuál es el nivel de cultura de ciberseguridad que considera usted que existe dentro de la CCSS?**

_____

4. **¿Actualmente se promueve de manera formal y estructurada una estrategia de desarrollo y fortalecimiento de la cultura de ciberseguridad en los usuarios internos de los servicios informáticos en la CCSS?**

Si ☐ No ☐ No sabe /No Responde ☐

5. **¿Existe un plan actualizado, posterior al ciberataque del 31 de mayo de 2022 en la CCSS, en acciones que tendrán como objetivo aumentar de forma gradual el acercamiento a la concientización en ciberseguridad?**

   Si ☐ No ☐ No sabe /No Responde ☐

6. **¿Existe una medición posterior al ciberataque del nivel de conocimiento, concientización y hábitos de ciberseguridad en los funcionarios de la CCSS?**

   Si ☐ No ☐ No sabe /No Responde ☐

7. **¿Existe una hoja de ruta para ir aumentando la cultura de ciberseguridad de la organización a lo largo de los años?**

   Si ☐ No ☐ No sabe /No Responde ☐

8. **¿La CCSS brinda información <u>constante o periódicamente</u> a los usuarios internos de los servicios TIC en temas de ciberseguridad?**

   ☐Nunca
   ☐Rara vez
   ☐Con alguna periodicidad
   ☐Regularmente

9. **¿La CCSS brinda información actualizada a los usuarios internos de los servicios TIC en temas de ciberseguridad?**
   Si ☐ No ☐ No sabe /No Responde ☐

10. **¿Existe un responsable formal de desplegar el entrenamiento requerido de concientización en ciberseguridad?**

    Si ☐ No ☐ No sabe /No Responde ☐

11. **¿Se están realizando periódicamente campañas de sensibilización sobre ciberseguridad dirigidas a los usuarios internos de los servicios TIC?**
    ☐Nunca
    ☐Rara vez
    ☐Con alguna periodicidad
    ☐Regularmente

12. **Finalmente ¿Existe recurso humano suficiente dentro de la Dirección de Tecnologías de Información y Comunicaciones para desarrollar y ejecutar un plan para el fortalecimiento de la cultura de ciberseguridad en la CCSS?**

Si ☐ No ☐ No sabe /No Responde ☐

¡Muchas Gracias!