UNIVERSIDAD DE COSTA RICA

Control Interno

BOLETÍN TÉCNICO **2022**

ISSN: 2215-4485

Contraloría Universitaria
UCR

Índice

Presentación

MBA GLENN SITTENFELD JOHANNING

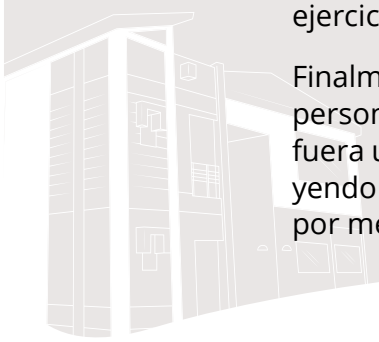
Saludos estimados lectores de nuestro Boletín Técnico de Gestión y Control, en este año 2022 con sumo agrado me permito presentarles este ejemplar que contiene varios artículos de nuestros compañeros y compañeras que dedicaron parte de su tiempo para compartir sus experiencias y conocimientos con el fin de que podamos contar con algunas herramientas que nos ayuden a comprender mejor los deberes y responsabilidades que tenemos como funcionarios universitarios en el ámbito del control interno y que, con nuestro accionar fortalezcamos, cada día, los procedimientos internos establecidos por cada una de sus dependencias para la consecución de los objetivos y metas.

Los años 2020 y 2021 fueron especiales a causa de los efectos de la pandemia por el virus Covid-19, donde nos obligó a cambiar la manera en que veníamos haciendo las cosas e innovar, nos dejó muchas enseñanzas y a su vez algunas situaciones de dolor. Dentro de ellas pudimos evidenciar que una actitud propositiva y comprometida son esenciales para alcanzar las metas establecidas en un plan de trabajo donde; las tecnologías de información fueron un aliado estratégico para su cumplimiento eficaz de nuestras labores.

Este boletín forma parte del programa de promoción de buenas prácticas y pretende mantenernos informados de algunos temas que, consideramos importantes y relevantes para el fortalecimiento de nuestra gestión y prevenir, porque no, malas prácticas y ser más eficientes en nuestra gestión.

En el presente documento encontraran artículos sobre “Del trabajo remoto y otros consejos prácticos para el control interno en tiempos de anormalidad”, “Seguridad de la Información”, “Los retos de documentar en la administración pública” y “El Valor del Control y el Control del Valor” los cuales esperamos sean de mucho utilidad y provecho en el ejercicio de su labor.

Finalmente, aprovecho la oportunidad para agradecer a todas aquellas personas que de una u otra forma colaboraron para que este ejemplar fuera una realidad y que; de esta manera, pudiéramos seguir contribuyendo en el mejoramiento del sistema de control interno institucional por medio de nuestros servicios preventivos.



OCU
BOLETÍN

Del trabajo remoto y otros consejos prácticos para el control interno en tiempos de anormalidad

LIC. FERNANDO MARTÍNEZ JIMÉNEZ
Auditor

fernando.martinez@ucr.ac.cr

Del trabajo remoto y otros consejos prácticos para el control interno en tiempos de anormalidad

Introducción

La convergencia de medidas para el distanciamiento social junto a las dificultades presupuestarias y límites al gasto catapultadas desde el asedio legislativo, han llevado a las relaciones de empleo público a un terreno, hasta hace poco, inexplorado. Y si el ejercicio de la función pública, antes de la pandemia nos parecía un viaje a marchas forzadas, la crisis sanitaria y económica por COVID-19 en el último año, acaso ha dejado a las Administraciones públicas sin caja de cambios.

La "*anormalidad*" en la cual deben cumplirse las funciones públicas obliga a navegar en aguas de incertidumbre: entre lo extraordinario de las circunstancias y la sujeción de la conducta administrativa al principio de legalidad y a la certeza jurídica en favor del administrado.

Pero, ¿cómo afecta realmente la pandemia a las relaciones laborales? Sólo esta pregunta nos parece de talla extragrande. Pero podemos empezar por considerar que son las sensibilidades humanas las que, alimentadas por la incertidumbre que deja la pandemia, nos empujan a adoptar medidas que cuestionan aquello que dábamos por sentado; llegando a sacudir, incluso, las formas empleadas para traer lo público al plano material. Y, para citar un ejemplo, hemos visto que mientras la ley y la jurisprudencia de nuestros tribunales de justicia se esfuerzan por esculpir conceptos jurídicos indeterminados que consolidaban la presencialidad y el monitoreo físico, como el de "*faltas de mera constatación*"; desde la otra orilla las TI nos traen el trabajo remoto (o teletrabajo según dice la ley) y, con él, la relativización de bibliotecas enteras de derecho.

Al inicio de esta realidad, emprendimos la huida a conceptos como resiliencia o adaptación; más que todo para tratar de convencernos, los unos a los otros, de que "*tutto andrá bene (todo irá bien)*"[1]. Pero tratándose de las relaciones de empleo público, ello no es suficiente para asegurar el clima organizacional que proteja el empleo mismo, en medio de esta *terra incógnita* por la que atraviesan las relaciones laborales.

1 URZAIZ GÓMEZ, Begoña. "*¿Todo irá bien? La polémica tras el lema que quiere tranquilizarnos frente al coronavirus*". Publicado en el diario El País, el 13 de abril de 2020. España. Recuperado de https://elpais.com/ideas/2020-04-13/todo-ira-bien-la-polemica-tras-el-lema-que-quiere-tranquilizarnos-frente-al-coronavirus.html

El presente aporte encuentra motivación en esa búsqueda de nuevas formas de control interno, a sabiendas -con temeridad y algo más de resignación- de que actualmente el tema amerita un abordaje interdisciplinario, más amplio y profundo que unas cuantas páginas; pero con la convicción de que la práctica consciente del control interno puede proporcionarnos un acervo de experiencias significativas, útiles para el mantenimiento y mejora en el cumplimiento de nuestras competencias públicas y nuestro crecimiento personal y laboral.

La regulación del teletrabajo en Costa Rica y España.

Al amparo de la legislación vigente y hasta hace relativamente poco tiempo, trabajar a distancia se limitaba a circunstancias que fácilmente era posible identificar con giras o sesiones de trabajo fuera de la institución.

Con una perspectiva de pasaje, el ordenamiento jurídico costarricense preveía una regulación general en el Código de Trabajo que posibilita la realización temporal de actividades en un lugar distinto de la oficina pública o centro de trabajo.

Precisamente, la regulación específica de estas condiciones laborales a distancia casi era delegada al fuero interno de cada entidad pública y a parámetros generales de actuación señalados por la Contraloría General de la República, por ejemplo: en materia de pago de viáticos y gastos por traslados, alimentación y hospedaje, o el pago de zonaje (por desplazamiento regular a una zona distinta del domicilio), entre otros.

Así las cosas, el control interno en ese contexto privilegiaba el control presencial y el monitoreo físico de los funcionarios, de tal modo que el trabajo remoto había venido implementándose residualmente en las relaciones de empleo público, desde la entrada en vigencia de la Ley N.° 9738, desde octubre de 2019.

Esta regulación, aunque más específica sobre la materia de teletrabajo, es poco concreta en cuanto a aspectos de contenido y, menos aún, respecto al control interno. Lo que deja un amplio margen de interpretación y, consecuentemente, para el error.

Pero, ¿es idónea esta regulación en tiempos de anormalidad? La respuesta podemos encontrarla en el derecho comparado; propiamente en el espacio europeo, en donde la experiencia en teletrabajo en lo público tiene su principal antecedente en el Acuerdo Marco Europeo sobre Teletrabajo, suscrito en julio de 2005 y revisado en 2009.

Más específicamente y considerando su cercanía cultural con nuestro país, vemos que en España, por ejemplo, hay una normativa específica para el teletrabajo en el empleo público, según se autoriza a partir de la modificación al artículo 47 de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto 5/2015 del 30 de octubre de 2015.

Entre los aspectos más destacados de esa normativa española es que establece la flexibilidad para el trabajador en la escogencia del lugar para desempeñar funciones y en el cumplimiento de horarios. Además, fomenta la co-gobernanza entre el Estado y las organizaciones de trabajadores, al contemplar la posibilidad de negociar colectivamente las condiciones de prestación del teletrabajo.

Además, la legislación española ha incorporado el derecho a la desconexión digital desde el año 2018, mediante el artículo 88 de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de Derechos Digitales, del 5 de diciembre de 2018, y con él se establece un límite claro en beneficio de la intimidad personal y la salud del trabajador.

Resulta tentador considerar que algunos elementos presentes en esa legislación extranjera podrían considerarse oportunidades de mejora de la regulación costarricense. Por tal motivo, a continuación, presentamos comparativamente las características del teletrabajo que, al menos en el plano formal, proporcionan las legislaciones de España y Costa Rica.

Aspecto	Teletrabajo en Costa Rica	Teletrabajo en España
Tipo de contrato	Por escrito	Por escrito
Horario de teletrabajo	El establecido en el contrato de teletrabajo y limitado por Código de Trabajo	Flexible, sujeto al cumplimiento de funciones y al cumplimiento de los objetivos
Margen para negociar condiciones	No cabe la negociación colectiva, sólo el mutuo acuerdo en cada caso individual	Si cabe la negociación colectiva
Derechos del trabajador presencial que se incorpora al teletrabajo	Mantiene los mismos derechos	Mantiene los mismos derechos
Incorporación al teletrabajo	Voluntaria	Voluntaria
Derecho del trabajador a la desconexión digital	No se reconoce	Sí se reconoce
Revocación del teletrabajo	Sólo a criterio del patrono	Reversible en cualquier momento, a solicitud de cualquiera de las partes.
Definición de objetivos, evaluación de resultados y control	Por mutuo acuerdo	Definidos por Ley o normativa institucional interna, pudiéndose negociar colectivamente
Igualdad respecto a trabajadores en modalidad presencial	Se prohíbe la discriminación	Se prohíbe la discriminación
Provisión de equipos, software, insumos y otras herramientas para teletrabajo	Es deber del patrono, salvo que por mutuo acuerdo se use equipo personal.	Es deber del patrono
Protección de información pública	El trabajador debe mantener la confidencialidad y dar acceso al patrono de toda la información institucional	El Patrono debe garantizar la protección de datos
Cumplimiento de criterios de evaluación, medición y control	Es deber del teletrabajador	Es deber del teletrabajador
Protección ante riesgos del trabajo	Cubre únicamente los accidentes o enfermedades derivados del teletrabajo y acontecidos directamente al trabajador.	Cubre todos los riesgos, exceptuando los relacionados con el trabajo presencial.

Del control físico en presencialidad, a la templanza personal en el trabajo remoto

Tras el velo de precisión que pretenden proporcionar las leyes y reglamentos y más allá de la orilla del control aún en trance de presencialidad, la práctica reciente del teletrabajo, o trabajo remoto como se ha preferido llamarle en la Universidad de Costa Rica, ha puesto al descubierto los riesgos que la virtualidad trae consigo a nivel físico, operativo e interpersonal para las relaciones de empleo. La posibilidad de que el trabajador determine el lugar dónde desempeñar sus funciones (deslocación), el aislamiento del trabajador y la despersonalización por el uso intensivo de las tecnologías para mantenerse conectado y pérdida de compromiso respecto a los valores personales y de la organización, son tal vez los riesgos más importantes a los que actualmente se enfrentan las relaciones de empleo público, a causa del teletrabajo.

La movilidad que veníamos disfrutando en los ambientes más íntimos y personales, gracias a las nuevas tecnologías, nos ha impuesto, en forma casi desapercibida, una flexibilidad que ha sido impuesta por necesidades de confinamiento. Y, aunque se habla mucho de las bondades presupuestarias que tiene el trabajo remoto en cuanto a reducción de gastos operativos de la Entidad, para el trabajador, al fin de cuentas, la prometida movilidad tecnológica y la virtualidad se han traducido en una ausencia de paisaje; lo que, a la larga, puede atentar contra su productividad y desempeño.

El uso intensivo de la virtualidad a través de los medios tecnológicos reduce la realidad a un plano bidimensional, en el que "*ser persona*" adquiere un aspecto cinematográfico. Y así como el sétimo arte despierta los más diversos gustos, el teletrabajo es terreno fértil para las más diversas interpretaciones y, consecuentemente, para el malentendido en las relaciones de trabajo, debido a la pérdida de interacción social y de percepción sensorial en el proceso comunicativo.

La virtualidad tiende a precarizar la interpretación del mensaje que damos y recibimos y, si a esto añadimos que, por naturaleza humana, el lenguaje es preponderantemente gestual, no hablado; vemos que, sin duda alguna, el empobrecimiento de los personalismos puede afectar sensiblemente la comunicación.

La distancia relacional o aislamiento como factor de riesgo derivado del trabajo remoto puede ser un catalizador para la pérdida de intersubjetividad en la comunicación y, finalmente, para la despersonalización del individuo.

Estrictamente, en cuanto a la dinámica de la relación laboral, el teletrabajo en lo público puede propiciar que el jefe, acostumbrado al control en la presencialidad, perciba una pérdida de control sobre lo que hacen o no hacen sus subalternos, afectando la confianza mutua con los empleados y entre éstos mismos; lo que se puede tratar de

compensar erróneamente con sistemas de control y supervisión innecesariamente detallista. A estas alturas, la idea de incorporar software en los computadores para controlar el inicio y fin de jornadas en teletrabajo, más que contraproducente, es una práctica laboral antiética[2] que mina la confianza mutua entre personas.

Desde la perspectiva del empleado público, el teletrabajo propicia el aislamiento personal. Lo que antes era fácilmente abordado en una conversación de pasillo, en el comedor, o durante una pequeña interrupción al jefe, ahora muchas veces queda fuera del área de cobertura de la virtualidad. Esto puede hacer que el trabajador se sienta invisibilizado: excluido de los procesos de toma de decisiones, lejos de oportunidades de crecimiento o, lo que es peor, percibir traicionada su dedicación en el empleo. Todo lo cual puede afectar su moral y compromiso con los objetivos de la organización.

Frente a tales riesgos y en medio de la anormalidad actual y su incertidumbre, puede hacernos pensar que el trabajo remoto hace innecesario el control interno en tiempos de trabajo remoto; o bien, que es un obstáculo para realizar los fines que dicte la ley. Pero, lo cierto es que, en medio del naufragio, las formas que adopte el control interno pueden ser las tablas de salvación para que, individualmente y como organización, se propicie un ambiente organizacional que asegure los derechos laborales y la satisfacción al interés público.

Precisamente, la práctica del trabajo remoto, en tiempos de anormalidad, parece haber acelerado un cambio de paradigma que ya se vislumbraba, desde hacía algún tiempo, en las relaciones laborales en teletrabajo: la clave para el mantenimiento y mejora del control interno no está en la inmutabilidad aparente del Principio de Legalidad (en la obligatoriedad de las normas que regulan el empleo público), sino en la relevancia relativa de las formas de control empleadas para alcanzar el fin público perseguido... *El control interno no es una leguleyada, ni un fin en sí mismo*.

El carácter excepcional de las medidas en tiempos de anormalidad o urgencia no resta importancia o aplicabilidad a la ley o los reglamentos. Más bien, se trata de que la flexibilidad y pragmatismo en las formas de control permitan alcanzar los resultados esperados por el propio ordenamiento jurídico en el cumplimiento de las competencias públicas.

Tampoco se trata de que el control interno haya perdido utilidad. Por el contrario, las necesidades de flexibilidad en las formas en que se desarrollan las relaciones de empleo público, como las que supone el trabajo remoto en el contexto de la crisis sanitaria, expropia el control interno de manos del Superior Jerarca y los titulares subordinados, para trasladarlo al funcionario público, en todos los niveles jerárquicos, como parte de su rol diario de actividades.

2 DANS, Enrique. "*Teletrabajo: Mirando más allá*". Publicado en Harvard Deusto-Bussines Review, Sumando ideas: Luces y sombras del Teletrabajo. Página 45. Recuperado de www.harvard-deusto.com

En ese sentido, podemos decir que la pandemia ha democratizado el control interno a lo interno de las organizaciones.

A un nivel más personal, bien decía Marco Tulio Cicerón que "*la que llamamos prudencia, y con nombre más grave, sabiduría, descansa en la ciencia. La templanza, que modera y rige los afectos del ánimo, se dirige a la acción. La prudencia se divide en doméstica y civil, según que se aplica a los negocios privados o a los públicos. La templanza admite igual división, y en la prosperidad obra de dos modos: no apeteciendo lo que le falta y absteniéndose de lo que posee. En la desgracia es también doble, pues cuando pone el rostro a los males se llama fortaleza, cuando los tolera y sufre, paciencia (...)*"[3]

Algunas consideraciones finales para reflexionar

La legislación costarricense que regula el teletrabajo desde hace algunos años, continúa permeando una perspectiva que privilegia la presencialidad y el control físico sobre los procesos, lo que se refleja en mecanismos tradicionales de control en el trabajo remoto. Esto se corresponde con una organización del control interno estructurada jerárquicamente de arriba abajo que no necesariamente coincide con el rol que la virtualización de las competencias públicas a cargo de funcionarios que laboran en modalidad remota.

Aunque la actual ley de teletrabajo en nuestro país permite su aplicación de manera indiferenciada para el trabajo en lo privado y lo público, A diferencia de la legislación española, el ordenamiento jurídico no incorpora una regulación específica para el trabajo remoto en el sector público. Además, la legislación costarricense es más restrictiva en materia de negociación colectiva y no incorpora un derecho del funcionario público a la desconexión digital que lo proteja ante el abuso en el ejercicio de la autoridad por parte de su patrono o superior inmediato. Lo cual representa importantes oportunidades de mejora de nuestra legislación que pueden incidir en la valoración del control interno en la Institución.

A falta de precisión y especificidad en la legislación que regula el trabajo remoto en nuestro país y ante la crisis por COVID-19 y su impronta de anormalidad, se hace necesario desarrollar nuevas formas de control interno, tal vez más horizontales; que se ajusten al nuevo papel que juegan los empleados públicos en trabajo remoto. Dichas formas alternativas de control nacen, precisamente, del empoderamiento de los trabajadores dentro de las organizaciones, y del rol que juega el control interno como parte intrínseca de su desempeño individual.

Pero las nuevas formas del control interno en el empleo público y, particularmente, en el teletrabajo o trabajo remoto, deben hacer del trabajo algo más que "*human experience*"[4].

3 CICERON,Marco Tulio. Obras Completas de Cicerón. Ebookclasicos, primera edicion, mayo 2021.
4 Deloitte Digital, "*The Human Experience. Quantifying the value of human values*". Recuperado de https://www.deloittedigital.com/content/dam/deloittedigital/us/documents/blog/blog-20190807-ehx.pdf

Deben propiciar la conservación del empleo mismo y las condiciones en que éste permite al empleado público proyectar su condición de persona, mientras potencializa sus capacidades y las capacidades de la Entidad, para el cumplimiento de las funciones.

El empleado público debe ser consciente del momento histórico de inflexión en el que asume un mayor grado de importancia dentro de la organización. En momentos en que la evaluación de su desempeño depende, casi exclusivamente del análisis de los resultados, le conviene mantener control sobre el entorno de su actividad, renunciar a las diferencias en el trabajo, asumir con disciplina y responsabilidad sus tareas y velar con pragmatismo y asertividad por la adecuada comunicación con sus superiores.

En el orden está Dios.

Por tal motivo, conviene al trabajador ser consciente de que escoger el lugar y el espacio físico para desempeñar su trabajo no debe ensombrecer las posibilidades de cumplir sus deberes. Lo más conveniente es minimizar los riesgos a nivel personal y familiar que puedan generarse en el entorno físico más inmediato, que puedan comprometer su desempeño en el trabajo.

Además, la adaptabilidad a las circunstancias es una realidad en las relaciones de empleo público. Lo idóneo es que previamente exista un procedimiento institucional que determine el procedimiento que prevea al máximo esas contingencias. No obstante, la anormalidad nos ha enseñado que debemos estar preparados para cualquier eventualidad. Incluso durante el teletrabajo es conveniente prever los escenarios posibles y las medidas a tomar frente a riesgos o situaciones imprevistas, como, por ejemplo: suspensión del fluido eléctrico o de internet.

**Donde me la pinten, brinco,
y en cualquier mecate tiendo.**

Ojo al Cristo y mano a la chuspa.

Es importante que el trabajador o funcionario público, sea disciplinado y mantenga el control sobre la gestión de su tiempo. Es conveniente llevar agendas bien planificadas, por día o por semana. Pero, al mismo tiempo, debe ser consciente de las necesidades de adaptabilidad que normalmente exigen sus funciones. Si es necesario, puede ser conveniente reformular prioridades, tomar actas de las reuniones efectuadas mediante plataformas electrónicas, sistemas de mensajes o llamadas telefónicas.

Es importante y conviene al trabajador que, en caso de dudas sobre aspectos jurídicos o técnicos de su trabajo, busque orientación internamente, en su equipo de trabajo o en alguna instancia interna de asesoría, acudiendo al funcionario, oficina u órgano institucional más competente en la materia.

A pellizcos se mata un burro.

Cierto es poco o nada se obtiene si la prudencia y buena fe del trabajador no es correspondida con acciones que a nivel estratégico promuevan políticas institucionales claras y que revisen y elaboren normativa interna que sea necesaria y que permita fijar bases sólidas para una cultura organizacional basada en la confianza mutua, el empoderamiento del trabajador, el reconocimiento a su buen desempeño y a la autonomía relativa en la ejecución de funciones a nivel operativo.

Por tal motivo es necesario que los jerarcas institucionales evalúen seriamente los riesgos presentes en la organización, con el fin de conocer el presente y futuro de la institución.
Al mismo tiempo, se deben establecer políticas generales y normativa interna que defina los valores de la organización y permita construir una cultura organizacional que se caracterice por la confianza mutua y la igualdad de trato y de oportunidades laborales; evitando la discriminación en el empleo y las dinámicas de poder en los niveles intermedios y operativos de la organización, la inequidad entre los empleados o su aislamiento. En pocas palabras, a nivel estratégico es preciso implementar acciones que disminuyan la brecha tecnológica, la distancia operativa y el aislamiento entre el personal y de este con respecto a la Institución.

**Sin cacao,
no hay chocolate.**

Si el trabajador en los tiempos actuales es la pieza angular en el entramado del control interno, el nivel intermedio o de jefatura es el punto crítico en el aseguramiento y mejora del control interno; particularmente en el contexto del trabajo remoto. El jefe o líder de grupo de trabajo posee un grado de información privilegiado y reúne en sí mismo esas dos naturalezas: por un lado, actúa como brazo ejecutor de las decisiones y planes estratégicos y, al mismo tiempo, debe actuar como guía y motivador de sus compañeros subalternos. Por tal motivo, para el control interno conviene que el jefe sea accesible, consciente de los riesgos y de las dinámicas de poder que se generan entorno al trabajo remoto; pero, sobre todo, capaz de inspirar a otros, generando valor y facilitar el desarrollo personal del empleado subalterno.

El talento gana partidos, pero el equipo gana campeonatos.

El jefe o líder debe ser auténtico en su interacción con el equipo, ya que está llamado a generar un entorno de cercanía y calidez que fomente entre los colaboradores el aporte de ideas útiles y la generación de valor.

Debe tener tacto y empatía con los colaboradores, de tal modo que el trato al empleado no genere inequidades o tratos odiosamente desiguales en cuanto oportunidades de crecimiento laboral o que afecten la moral del empleado.

En palabras de Jorge Valdano:

> *"(...) el líder debe fortalecer un sentimiento solidario, lograr que todos se sientan orgullosos de la idea que representan (...) Pero existe una aspiración que a todos hace igual de felices: sentirse importante. Si cada miembro del equipo siente que es valorado por el grupo, a ese vestuario dará gusto entrar y en ese equipo dará gusto jugar"*[5].

Cuentas claras, chocolate espeso.

Precisamente, para facilitarse así mismo el cumplimiento de esas tareas y expectativas, es importante que el jefe:

- Establezca reglas claras para las reuniones y cumplimiento del trabajo, así como para el uso de las tecnologías durante la jornada.
- Fije claramente las expectativas de resultados y una frecuencia razonable para las reuniones de equipo. Que cada colaborador tenga claro su rol y funciones dentro del equipo.

5 VALDANO, Jorge. *Los 11 poderes del Líder*. Drokerz Impresiones de México, S.A. de C.V, 2014, México D.F., página 145.

Puede que estos consejos prácticos sirvan para desarrollar estrategias en materia de control interno, y faciliten su mejora durante el periodo en que realicemos trabajo remoto. Así como el "*autocuidado*" es talvez la recomendación más repetida por los expertos en salud pública desde que inició la pandemia, puede que ésta sea la definición más sintética, que resuma, en una palabra, el devenir el control interno en los tiempos actuales, en los que la insuficiencia en los conceptos, en las formas y en la ley, nos lleva de vuelta a los clásicos, como a las virtudes de la templanza y la prudencia, útiles para el buen vivir, de las que hablan el filósofo Marco Tulio Cicerón y otros tantos más.

Pero, más que los buenos consejos, es la correcta actitud del funcionario, de cada uno y de todos a la vez, independientemente de su grado de jerarquía, la herramienta más eficaz que verdaderamente puede propiciar la generación de experiencia, individual y colectiva, que permita hacer los ajustes necesarios, en el momento oportuno, adaptando el control interno a las necesidades más actuales e inmediatas de las funciones públicas, que aseguren su cumplimiento y, con ello, permitan proteger el empleo público mismo y los derechos que de él derivan, mientras se cumple el trabajo en forma remota.

Al final, no vaya a ser que "*el uno por el otro y la casa sin barrer*"[6].

6 Refrán español, utilizado para describir situaciones en las que se tiene que realizar un trabajo en equipo y ninguna de las personas involucradas hacen su trabajo, o bien porque no se ponen de acuerdo o bien porque no quieren hacerlo, al final la tarea no se hace, y esto repercute en el rendimiento de todos y a veces llega a afectar a otras personas.

OCU
BOLETÍN

Seguridad de la Información

M.SC. GUSTAVO ROJAS GARCÍA
Auditor

gustavo.rojas@ucr.ac.cr

Seguridad de la Información

Introducción

En términos generales, ¿qué entendemos por "*seguridad*"?

En un mundo ideal, la seguridad (del latín securitas)[1] la entendemos como *"libre o exento de todo peligro, daño o riesgo, o a la confianza en algo o en alguien..."*. Otra forma de entender la seguridad, es por medio de su antónimo: la "*inseguridad*", que se define como la existencia de un peligro, de un riesgo o refleja alguna duda sobre un asunto determinado, tales como el robo, delincuencia organizada o accidentes viales, entre otros contextos.

A menudo, la seguridad es denominada como una ciencia interdisciplinaria que se encarga de la identificación, evaluación y gestión de los riesgos a los que se encuentra sometida una persona, organización, un activo o el ambiente.

El enfoque principal de la seguridad es la prevención oportuna de los riesgos existentes en el entorno, como requisito para poder realizar una correcta planificación de los requisitos para implementar un entorno razonablemente seguro.

El término "*seguridad*" puede tomar diversos sentidos de acuerdo con el área o campo al que haga referencia, así podemos encontrar que existen varios tipos de seguridad, tales como:

- Bioseguridad.
- Seguridad Ciudadana.
- Seguridad Jurídica.
- Seguridad Laboral.
- Seguridad Social.
- Seguridad Vial.
- Seguridad Bancaria.
- Seguridad Física.
- Seguridad de la Información.

A modo de ejemplo, le corresponde a la Caja Costarricense de Seguro Social (CCSS) garantizar el derecho a la Seguridad Social de los ciudadanos, el que se encuentra consignado en el Artículo 73 de nuestra Constitución Política. En aras de cumplir el mandato constitucional, la CCSS es responsable de gestionar el sistema de seguros sociales para proteger a los trabajadores contra los riesgos de la enfermedad, la invalidez, la maternidad, la vejez y la muerte.

1 Real Academia Española y Asociación de Academias de la Lengua Española (2014). «*seguridad*». Diccionario de la lengua española (23.ª edición). Madrid: España. ISBN 978-84-670-4189-7.

¿Qué es la información?

Información es el nombre por el que se conoce al "*...conjunto organizado de datos que al ser procesados constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema (capaz de emular el pensamiento humano) que recibe el mensaje*"[2].

Existen diversos enfoques para el estudio de la información. El término "*información*" es de uso común en prácticamente todas las Ciencias Biológicas, Sociales y Humanas, la Física, de muchos tipos y clases de Tecnologías, y por supuesto, en nuestra cotidianidad.

Se reconoce que la información constituye precisamente la materia prima para generar conocimiento, por lo que es la punta de lanza del desarrollo económico de las naciones, por ello, se habla sin exagerar de la Sociedad de la Información y de la Revolución de la Información, cuya intensidad y alcance se equiparan a las de las otras dos grandes revoluciones que han marcado de manera singular la historia de la Humanidad: la Neolítica y la Industrial.

¿Cuáles son las principales características de la información?

En general la información tiene una estructura interna y puede ser calificada según las siguientes características:

- *Significado (semántica):* Del significado extraído de la información, cada individuo o sistema experto evalúa las posibles consecuencias y adecua sus actitudes y acciones conforme a las circunstancias. Las expectativas que tiene el ente se dan de manera literal al significado de la información.
- *Importancia (relativa al receptor):* La importancia de la información para un receptor se refiere a qué grado cambia la actitud o la conducta de los individuos. En las modernas sociedades, los individuos obtienen de los medios de comunicación masiva gran cantidad de información, una gran parte de la misma es poco importante para ellos, porque altera de manera muy poco significativa su conducta. Algunas veces, se cuenta con la seguridad de que un hecho hace menos probables algunas cosas y más otras.
- *Vigencia (en la dimensión espacio-tiempo):* Se refiere a si está actualizada o desfasada. En la práctica la vigencia de una información es difícil de evaluar, ya que en general acceder a una información no permite conocer de inmediato si dicha información tiene o no vigencia.
- *Validez (relativa al emisor):* Se evalúa si el emisor es fiable o puede proporcionar información falsa.
- *Valor (activo intangible volátil):* La utilidad que tiene dicha información para el emisor y para el destinatario. Dentro del gran ambiente de negocios de hoy, la información se convierte en uno de los activos más valiosos para todo tipo de organizaciones e individuos, y dependiendo de su naturaleza puede alcanzar altos valores monetarios.

2 https://es.wikipedia.org visitada el 11 de mayo de 2021.

¿Qué tipos de información existen?

Existen diversos y variados tipos de información, tales como:

- *Información de carácter restringido o privilegiado:* Se trata de información de naturaleza sensible que no se comparte públicamente, es decir, está restringida a determinadas personas, grupos u organizaciones. Normalmente, este tipo de información se comparte en reuniones de corte gerencial, políticas o de gobierno. Ejemplos de este tipo de información son los secretos comerciales relacionados con el diseño de nuevos productos y patentes, o bien, los secretos de estado.
- *Información de carácter público:* Se caracteriza por ser una información accesible a todos los interesados en conocer su contenido. Se publica en cualquier tipo de medio, y en principio, cualquiera puede contar con fácil acceso a ella. Ejemplos de este tipo de información son las noticias de un periódico, un anuncio en televisión, o charla gratuita.
- *Información de carácter privado:* Este tipo de información está relacionada con la privacidad de los individuos, por ejemplo: las contraseñas bancarias o los documentos propiedad de una empresa. Normalmente, incluso los colaboradores suelen firmar un convenio de confidencialidad con sus patronos para no desvelar ciertos datos de las marcas cuando empiezan a trabajar para ellas.
- *Información de carácter externo:* Es la información que llega del exterior a determinadas empresas para gestionar algunos temas en concreto. Se utiliza también para valorar a la competencia. Por ejemplo, es el caso en el que llegan datos, o informaciones de competidores presentes en el sector o mercado que provienen de fuentes externas.
- *Información de carácter interno:* Se trata de aquella que tan solo conoce un grupo de personas. Por ejemplo, la información sobre un proyecto determinado que está trabajando una marca y que un departamento ha de conocer para desarrollar su labor.

A partir de lo mencionado anteriormente, puede notarse que existen muchos tipos de información, no necesariamente se circunscribe al ámbito digital. Un documento impreso propiedad de una empresa pública o privada, grupo o personal, constituye información que podría contar con un valor económico dependiendo de su naturaleza. De igual forma, los secretos industriales, una fotografía, una conversación telefónica, un trozo de papel con datos escritos a mano acerca de un individuo, un audio o video, entre muchos otros, también constituyen información.

¿Cuáles son los usos de la información?

Se considera que la generación u obtención de información persigue principalmente los siguientes objetivos:

- Aumentar y mejorar la calidad del conocimiento del usuario, o dicho de otra manera reducir la incertidumbre existente sobre un conjunto de alternativas lógicamente posibles.
- Proporcionar a los tomadores de decisiones la materia prima fundamental para el desarrollo de soluciones más efectivas y la elección de mejores alternativas.
- Proporcionar una serie de reglas de evaluación y criterios de decisión para fines de control.

- Genera poder en muchos contextos y sentidos, tales como el poder político, religioso, económico y militar, entre muchos otros.

La Seguridad de la Información

¿Qué es la Seguridad de la Información?

Por definición, la Seguridad de la Información involucra tres conceptos claves[3], a saber:

- *Confidencialidad:* El concepto de confidencialidad se refiere a que la información debe ser accedida únicamente por los autorizados, y de manera restringida a la información que verdaderamente estos requieran. Se busca prevenir la divulgación no autorizada de información crítica y sensible. Dentro de los aspectos a considerar dentro de la confidencialidad de la información de los individuos, está: su origen racial o étnico, sus convicciones religiosas y espirituales, su estado socioeconómico, información relativa a su salud o vida sexual, antecedentes delictivos, entre otros.
- *Integridad:* El concepto de integridad de la información, se relaciona con la protección de la exactitud que debe dársele a la información, tanto en su procesamiento como en su almacenamiento. Toda modificación de datos o información deben realizarla por los que se encuentran debidamente autorizados, y de manera controlada. Se busca evitar la modificación de información confidencial. La violación de la integridad de la información se presenta cuando un individuo, programa o proceso, ya sea por accidente o con mala fe, modifica, corrompe o borra parte o la totalidad de cierta información.
- *Disponibilidad:* La información debe estar disponible para quienes tienen cuentan con autorización para accederla, en el momento preciso, en el lugar y de acuerdo con el formato de presentación en que se requiera. Se busca garantizar la continuidad de los servicios sustentada en reglas claras de accesibilidad para los interesados.

La Ciberseguridad

¿Qué es la Ciberseguridad?

La Ciberseguridad es parte de la Seguridad de la Información, comprende la práctica de defender los activos digitales o informáticos en cualquiera de sus configuraciones[4] en contra de la materialización de eventos no deseados. Puede dividirse, de acuerdo con la empresa Kaspersky[5], en algunas categorías comunes:

- *Seguridad de la Red*. Constituye la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o por software malicioso (también conocido como malware).

3 https://www.pmg-ssi.com visitada el 11 de mayo de 2021.
4 Computadoras, servidores, dispositivos móviles, los sistemas electrónicos, redes, Bases de Datos, entre muchos otros.
5 https://latam.kaspersky.com visitada el 3 de Mayo de 2021.

- *Seguridad de las Aplicaciones.* Se enfoca en mantener el software y los dispositivos electrónicos y digitales libres de potenciales amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

- *Seguridad de los Datos.* Se centra en proteger la integridad y la privacidad de los datos, tanto en el almacenamiento como en su trasmisión de manera segura.

- *Seguridad Operativa.* Incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

- *La recuperación ante desastres y la continuidad de las Tecnologías de Información (TI).* Definen la forma en que una organización responde a un incidente de ciberseguridad, o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos confidenciales o restringidos.

  Las políticas de recuperación ante desastres, dictan la forma en que la organización restaura sus operaciones e información, para volver a la misma capacidad operativa que existía antes del evento. Esto debe realizarse en el menor tiempo posible y de forma planificada. La continuidad de TI constituye el plan al que recurre la organización, cuando intenta operar sin los recursos que fueron afectados.

- *La capacitación del usuario final.* Aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.

¿Cuáles son las amenazas a las que se enfrenta la Ciberseguridad?

Las amenazas a las que se enfrenta la ciberseguridad son básicamente tres:

- *El delito cibernético.* Incluye agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones.

- *Los ciberataques.* A menudo involucran la recopilación de información con fines políticos.

- *El ciberterrorismo.* Tiene como objetivo vulnerar los sistemas electrónicos para causar pánico o temor.

¿Cómo consiguen los delincuentes vulnerar las medidas de Ciberseguridad?

A continuación, se describen algunos de los métodos más comunes utilizados por los delincuentes para vulnerar la Ciberseguridad:

- *Malware*. Se refiere al software malicioso que un criminal ha creado para interrumpir o dañar el equipo de un usuario legítimo.

Con frecuencia propagado a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima, el malware puede ser utilizado por los delincuentes para ganar dinero o para realizar ataques con fines políticos.

Existen diferentes tipos de malware, tales como:

- *Virus*. Es un programa capaz de autorreplicarse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
- *Troyanos*. Es un tipo de malware que se disfraza como software legítimo. Los criminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan de manera ilegítima datos confidenciales y sensibles.
- *Spyware*. Es un programa que recopila, sin que el usuario lo sepa, información confidencial para los delincuentes. Por ejemplo, los detalles de las tarjetas de crédito, y cuentas bancarias entre muchos otros datos sensibles.
- *Ransomware*. Este malware bloquea el acceso a los archivos y datos de una organización o usuario, con la amenaza de borrarlos, a menos que se pague un rescate.
- *Adware*. Es software de publicidad que puede utilizarse para difundir malware.
- *Botnets*. Comprende redes de computadoras con infección de malware que los criminales utilizan para realizar tareas en línea, sin el permiso del usuario u organización.
- *Inyección de código SQL*[6]. Una inyección de código SQL es un tipo de ciberataque utilizado para acceder, robar o modificar datos de una Base de Datos propiedad de una determinada organización. Los criminales aprovechan las vulnerabilidades de las aplicaciones para insertar código SQL, y así lograr su cometido.
- *Phishing*. Consiste en que los criminales atacan a sus víctimas con correos electrónicos que parecen ser de una fuente legítima, quien de forma sutil les solicita información confidencial. Los ataques de phishing se utilizan a menudo para inducir a que las personas entreguen datos de naturaleza sensible, tales como sus números de tarjetas de crédito y contraseñas, así como otro tipo de información confidencial que debe ser protegida.
- *Ataque de tipo "Man-in-the-middle"*. Comprende un tipo de ciberamenaza en la que un criminal intercepta la comunicación digital entre dos individuos para robar sus datos. Por ejemplo, en una red Wi-Fi no segura, un atacante podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.
- *Ataque de denegación de servicio*. Consiste que los criminales impiden que un sistema informático satisfaga solicitudes legítimas sobrecargando las redes y los servidores con tráfico. Esto hace que el sistema se torne excesivamente lento en sus respuestas, colapse o impide que una organización realice funciones vitales.

6 Siglas en inglés de Structured Query Language. En español lenguaje de consulta estructurada. Es un lenguaje de dominio específico utilizado en programación, diseñado para administrar, y recuperar información de sistemas de gestión de Bases de Datos relacionales.

¿Cuáles son las más recientes ciberamenazas presentes en el entorno?

A continuación, se comenta una de las ciberamenazas más recientes comunicadas por los gobiernos de Estados Unidos, Australia y el Reino Unido:

- *Malware Dridex.* En diciembre del 2019, el Departamento de Justicia de los Estados Unidos (DoJ) imputó al líder de un grupo de criminales organizados por su participación en un ataque global del malware Dridex. Esta campaña malintencionada afectó al público, al gobierno, a la infraestructura y a las empresas de todo el mundo.

  Dridex es un troyano financiero que posee diferentes funcionalidades. Desde el 2014, afecta a las víctimas e infecta a las computadoras a través de correos electrónicos de phishing o malware existente. Es capaz de robar contraseñas, datos bancarios y datos personales que pueden utilizarse en transacciones fraudulentas, y ha causado pérdidas financieras masivas que suman cientos de millones de dólares.

  En respuesta a los ataques de Dridex, el Centro Nacional de Seguridad Cibernética del Reino Unido aconseja a las personas que "*se aseguren de que los dispositivos estén actualizados y los antivirus estén activados y actualizados, y de que realicen copias de seguridad de sus archivos*".

- *Malware Emotet.* A finales de 2019, el Centro Australiano de Seguridad Cibernética advirtió a las organizaciones nacionales sobre la ciberamenaza mundial generada por el malware Emotet. Este sofisticado malware no solo es capaz de robar todo tipo de datos, tales como contraseñas de acceso poco seguras, sino que también puede facilitar el contagio y propagación de otros tipos de malware.

¿Cómo defenderse de las ciberamenazas?

A continuación, se presentan algunos consejos de ciberseguridad:

- *Actualizar el software y el sistema operativo:* esto significa que se aprovecharán las últimas medidas de seguridad disponibles para contrarrestar las amenazas detectadas.

- *Utilizar software antivirus:* las soluciones de seguridad detectarán y eliminarán las amenazas, por esta razón, mantener el software antivirus debidamente actualizado proporcionará un mayor nivel de protección.

- *Utilizar contraseñas seguras:* deben utilizarse contraseñas que no sean fáciles de adivinar.

- *No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos:* los archivos adjuntos podrían estar infectados con malware.

- *No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos:* esta acción constituye una forma común de propagación de malware.

- *Evitar el uso de redes Wi-Fi no seguras en lugares públicos:* el uso de redes no seguras expone a los usuarios a ataques del tipo *"Man-in-the-middle".*

Conclusiones

Lamentablemente, los riesgos que acechan la Seguridad de la Información siguen creciendo aceleradamente a nivel mundial tanto en agresividad como en sofisticación, afectando cada vez a un mayor número de individuos, grupos, organizaciones públicas y privadas.

Por su parte Costa Rica, ha respondido en contra de los delincuentes fortaleciendo su entorno estratégico y su marco jurídico para fortalecer su ambiente de Seguridad de la Información. Al respecto, destacan las siguientes leyes y estrategias:

- Ley N.° 6683 Derechos de Autor y Derechos Conexos[7]

  La protección adecuada de la Propiedad Intelectual resulta primordial dentro del entorno globalizado y el uso de las Tecnologías de Información (TI), en donde prevalece la circulación veloz de la información en todos sus formatos y en la que el conocimiento generado en las áreas académica, empresarial, artística, tecnológica o de índole social es cada vez más accesible para un número mayor de individuos, grupos, entidades públicas y privadas.

  El Registro Nacional de Derechos de Autor y Derechos Conexos se ha convertido en una oficina especializada en la materia, con funciones diversas y variadas que van mucho más allá de la registración. De acuerdo con lo estipulado en la Ley N.° 6683, las siguientes son funciones del Registro:

  - La registración de las obras artísticas y literarias, así como los actos o documentos relativos a negocios jurídicos de derechos de autor y derechos conexos (contratos, actos de enajenación, etc.)
  - Garantizar la seguridad jurídica de los derechos inscritos con respecto a terceros y dar correcta publicidad de ellos.
  - Fomentar la difusión y el conocimiento sobre los derechos de autor y derechos conexos.
  - Servir de órgano de información y cooperación con los organismos nacionales e internacionales.
  - Orientar y vigilar la utilización lícita de las obras protegidas.
  - Supervisar a las personas naturales o jurídicas que utilicen las obras, interpretaciones, ejecuciones y producciones protegidas.
- Ley N.º 8968 Protección de la Persona frente al tratamiento de sus datos personales[8]

  El Artículo 1. *Objetivo y fin*, indica lo siguiente:

  > *"Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes."*

7 Decreto Ejecutivo N.º 19117-J-C del 20 de julio de 1989.
8 Diario Oficial La Gaceta, Alcance 287, martes 6 de diciembre del 2016.

Y, el Artículo 2. *Ámbito de aplicación*, aclara lo siguiente:

"Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.

El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando éstas no sean vendidas o de cualquier otra manera comercializadas."

- Ley N.º 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos[9]

  Establece el marco jurídico general para la utilización transparente, confiable y segura en nuestro medio de los documentos electrónicos y la firma digital en las entidades públicas y privadas. Esta ley define la Firma Digital como el conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.

  En su Artículo 1, indica lo siguiente:

  "Que la sociedad de la información y del conocimiento se debe construir sobre la base de la confianza de los ciudadanos y sobre la garantía de la utilización de las tecnologías de la información y las comunicaciones en un doble plano: la protección y confidencialidad de los datos de carácter personal y la seguridad de las transacciones electrónicas."

- Código Penal. Reforma[10] de los Artículos 196, 196 bis, 230, 293 y 295 y adición del Artículo 167 bis

  El Artículo 196 bis. *Violación de datos personales*, indica lo siguiente:

  "Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

  La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:

  a)Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

9 Diario Oficial La Gaceta 77, de fecha 21 de abril de 2006.
10 Presidencia de la República, San José, 24 de abril de 2013.

b) La información vulnerada corresponda a un menor de edad o incapaz.

c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.

Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley."

El Artículo 230. *Suplantación de identidad*, establece lo siguiente:

"Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información."

El Artículo 293. *Revelación de secretos de Estado*, indica lo siguiente:

"Será reprimido con prisión de uno a seis años a quien revele secretos de Estado debidamente decretados relativos a la seguridad interna o externa de la nación, la defensa de la soberanía nacional o las relaciones exteriores de la Republica."

El Artículo 295. *Espionaje*, señala lo siguiente:

"Será reprimido con prisión de uno a seis años a quien procure u obtenga indebidamente secretos de Estado debidamente decretados relativos a la seguridad interna o externa de la nación, la defensa de la soberanía nacional y las relaciones exteriores de Costa Rica.

La pena será de dos a ocho años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación."

- Estrategia Nacional de Ciberseguridad de Costa Rica[11]

  Esta estrategia plantea un esfuerzo conjunto y articulado por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) entre todos los sectores interesados del país, para garantizar que los objetivos en la materia sean equilibrados, eficaces y acordes con la realidad nacional, definiendo los principios generales que marcarán la pauta país en el campo de la Ciberseguridad. El MICITT contó con el apoyo técnico especializado de la Organización de los Estados Americanos (OEA).

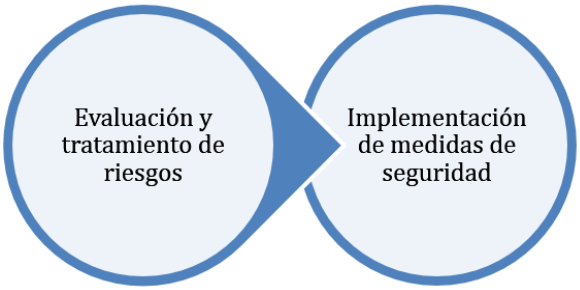
11 Costa Rica. Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Estrategia Nacional de Ciberseguridad Costa Rica 2017. – San José, C. R.: MICITT, 2017. ISBN: 978-9968-732-52-9.

Hacia la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) mediante la implementación de la Norma ISO-27001

El eje central de la Norma ISO-27001 es proteger la confidencialidad, integridad y disponibilidad de la información propiedad de una entidad pública o privada. Esto se realiza investigando cuáles son las potenciales amenazas y eventos no deseados que podrían afectar la información, es decir, a través de la identificación y evaluación de los riesgos, y luego definiendo lo que es necesario implementar para evitar que las amenazas se materialicen, en otras palabras, mediante la mitigación o tratamiento sistemático de los potenciales riesgos[12].

Figura 1

Estructura de la Norma ISO-27001



Las medidas o controles de seguridad a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica. Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, individuos, activos de información, entre otros, dentro de la Norma ISO-27001 se ha detallado cómo amalgamar todos estos elementos dentro de un Sistema de Gestión de Seguridad de la Información (SGSI).

En la siguiente figura se muestra que la Gestión de la Seguridad de la Información no se limita solamente a la Ciberseguridad, sino que también existen diferentes aspectos que se superponen unos con otros, tales como los procesos de Continuidad del Negocio, y la Gestión y Control de las Tecnologías de Información (TI), todos ellos aspectos relevantes de orden gerencial y organizacional.

Figura 2

Gestión de Riesgos Organizacionales

12 Dirección electrónica https://www.advisera.com visitada el 6 de mayo de 2021.

Es importante hacer notar que en la figura anterior también se muestra la relación existente entre Seguridad de la Información y la Gestión de Riesgos Organizacionales.

Para finalizar, es conveniente indicar que todos los temas mencionados en este artículo, deben ser abordados y analizados oportunamente por los dueños y directores a cargo de la organización, dado que el impacto de un evento no deseado en materia de Seguridad de la Información además de pérdidas económicas, conlleva efectos colaterales, tales como el daño a la buena imagen de una marca u organización, y la pérdida de confianza de sus clientes o usuarios.

OCU
BOLETÍN

Los retos de documentar en la administración pública.

LIC. DIEGO ROBERTO PORRAS CORDERO
Auditor

diegoroberto.porras@ucr.ac.cr

Los retos de documentar en la administración pública.

¿Qué es documentar?

Documentar es poner en papel *lo que se debe hacer* y/o *lo que se hace*.

Pero *¿qué es lo que se debe hacer?* Lo que se debe hacer es lo que está legalizado, normado o reglamentado y lo que se designa como parte de los objetivos o funciones de una institución, de un departamento o individualmente a una persona funcionaria.

¿Y qué es *lo que se hace*? Lo que se hace es lo que se ejecuta en la práctica.

Retomando la expresión *poner en papel*, esta hace referencia a poner por escrito. La práctica más común es la de hacer procedimientos o hacer formularios.

Un procedimiento es una descripción de la forma específica para llevar a cabo un proceso, mientras que un formulario es un medio para capturar información necesaria para la ejecución de un proceso.

Por ejemplo, en la atención de un paciente en un servicio médico, el proceso inicia con la presentación del paciente en la recepción. La persona que le atiende le solicita que complete una hoja con información personal e información médica básica y el paciente toma asiento, completa la información, la entrega en la recepción y espera a ser llamado para su valoración médica.

El proceso ya fue descrito, al menos, la primera parte. Se puede suponer que, por su simpleza, esa parte del proceso puede ejecutarse de forma satisfactoria consistentemente exista, o no, un documento escrito (procedimiento), sin embargo, otras partes del proceso puede que sean más complicadas, como la verificación del seguro, el procesamiento del pago o el traslado del expediente del paciente a otra dependencia o algún otro aspecto del proceso y, lo anterior, se hace aún más complejo cuando 100 o más personas realizan el mismo trabajo en 20 o más locaciones diferentes. Si se quiere que todas las personas que trabajan como recepcionistas procedan de la misma forma, uno de los medios para lograrlo es la documentación del proceso por medio de un procedimiento.

Por otra parte, no es realista pensar que la persona en la recepción pueda recordar todos los datos que debe solicitar al paciente

ni que pueda recordar y transmitir fielmente al doctor tratante toda la información personal y médica del paciente y que este, a su vez, recuerde todos los detalles al atender al paciente. Un medio para simplificar este proceso es utilizar un formulario.

Existen otras formas de documentar un proceso, más visuales que los procedimientos tradicionales en blanco y negro, como los son afiches, panfletos o videos, pero implican complicaciones adicionales que no forman parte del alcance de este artículo.

¿Qué documentar?

Se tiene claro entonces, que para facilitar la ejecución uniforme de un proceso, se puede elaborar un procedimiento, y para facilitar el registro de información se puede elaborar un formulario.

La gran pregunta es **qué documentar**. Se había adelantado que *lo que se debe hacer* y/o l*o que se hace* son los principales focos de atención.

Se debe entender que leyes, normas, reglamentos que rigen sobre un determinado proceso de la administración pública indican el ***qué*** *se debe hacer* y, para su correcta implementación, se debe establecer el ***cómo*** *se debe hacer* a lo interno de la institución, departamento y/o puesto de trabajo. Por tanto, no es práctico ni recomendable expresar que determinada ley, norma o reglamento se aplica íntegramente pues su función es la de establecer lineamientos, y el deber de cada institución es definir la forma en la que cumple con dichos lineamientos.

Por ejemplo, las Normas Generales para Auditoría del Sector Público (R-DC-64-2014), en adelante, NGASP, en su apartado 107.01 establecen que:

> *"El personal de auditoría debe mantener y perfeccionar sus capacidades y competencias profesionales mediante la participación en programas de educación y capacitación profesional continua"*

El apartado de la norma supra es claro en establecer el lineamiento, de que el personal de auditoría debe mantener y perfeccionar sus capacidades y competencias profesionales y que, para ello, debe participar en programas de educación y capacitación continua; sin embargo, la forma en la que se implementa el lineamiento en cada una de las instituciones del sector público costarricense, puede ser diferente por sus condiciones particulares, como:

- Una institución provee un monto determinado de presupuesto anualmente específico, para la capacitación del personal de la auditoría interna, con uso discrecional por parte de ésta.
- Una institución provee un monto determinado de presupuesto anualmente, para la capacitación del personal de toda la institución, y la persona que ostenta el puesto de Auditor(a) Interno(a) debe solicitar y justificar, la financiación de capacitaciones específicas para el personal a su cargo.
- Una institución no establece o no le asignan presupuesto para capacitación del personal.

Si la auditoría interna cuenta con presupuesto propio para capacitación, puede establecer sus propias condicionantes, por ejemplo: que solo se financien capacitaciones grupales (dirigidas a todo el personal de auditoría) o, por el contrario, que solo se financien capacitaciones individuales (dirigidas a una persona específica), que solo se financien capacitaciones de aprovechamiento y no de participación, que se financien capacitaciones específicas sobre habilidades duras (profesionales, académicas) pero no sobre habilidades blandas, etc.

Por otra parte, si la auditoría interna cuenta con presupuesto para capacitación, pero no propio, podría establecer sus propias condicionantes, pero posiblemente, el control del presupuesto y las condiciones sean establecidas por la misma institución.

Finalmente, si la auditoría interna no cuenta con presupuesto para capacitación, podría establecerse, por ejemplo: que las actividades de capacitación serán gestionadas por medio de convenios de cooperación con otras auditorías internas, o se disponga que el personal de auditoría debe gestionar y financiar sus propias capacitaciones.

Aunado a lo anterior y en relación con la capacitación del personal de auditoría, se debe tener en cuenta lo siguiente, entre otros aspectos:

- Quién, cómo y cuándo procede con las inscripciones.
- Quién, cómo y cuándo se procede con el pago de las inscripciones.
- Quién, cómo y cuándo se evalúa la eficacia de la capacitación.
- Quién, cómo y cuándo registra las capacitaciones a las que asiste el personal.
- Qué hacer si la persona inscrita no pudo asistir a la capacitación, que se le financió por una incapacidad u otra situación.
- Qué hacer si la persona no aprobó la capacitación (cuando es de aprovechamiento).
- Qué hacer si la capacitación contratada no fue satisfactoria (evaluación de proveedores de capacitación).

A partir de lo anterior, se observa que de un lineamiento, simple, sencillo y concreto como el señalado en el apartado 107.01 de las NGASP, se puede extraer un sinnúmero de particularidades que incrementan la complejidad de un proceso y que hacen necesaria su documentación. Si aunado a lo anterior, se considera que en la administración pública no es suficiente decir que algo se hace o se hizo, si no se puede demostrar fehacientemente, se palpa la necesidad de establecer un procedimiento y de uno o más formularios para el control del proceso y de la información que genera.

En el último listado se incluyen elementos que no están indicados expresamente en la norma, sin embargo, se había indicado al inicio de este artículo que se debe documentar *lo que se debe hacer* y/o *lo que se hace*. En este ejemplo específico, *lo que se debe hacer es* lo que indica la norma (mantener personal capacitado) y *lo que se hace* (o se debería hacer) es el proceso de inscripción

y pago, la evaluación de la eficacia de capacitación, el control de capacitaciones llevadas por cada persona funcionaria, etc.

En términos generales, una organización, departamento o persona funcionaria debe establecer aquello que debe implementar y le es requerido por leyes, normativas o reglamentos y, a su vez, establecer aquello que es complementario y necesario para asegurar que el proceso sea ejecutado adecuadamente. Además, se deben documentar aquellos procesos que, aunque no sean requerimientos legales o reglamentarios, son necesarios para alcanzar los objetivos de la organización, departamento o puesto de trabajo.

¿Cómo documentar?

Hasta el momento, se ha mencionado al procedimiento y al formulario como herramientas para documentar un proceso.

Respecto al nombre de estos instrumentos, se puede decir que no son los únicos que se pueden emplear. Como sinónimo de *procedimiento*, resulta común encontrar protocolo, instructivo, instrucción y, como sinónimo de formulario, resulta común encontrar formato, machote, plantilla, entre otros. Lo importante no es como se les denomine sino como se gestionan.

Para la gestión documental, es recomendable establecer un procedimiento... sí, un procedimiento para gestionar documentos.

Nótese que se hace referencia a *documentos* como concepto que incluye procedimientos, formularios y otros tipos de documentos que se puedan emitir internamente en una institución o departamento.

En dicho procedimiento se pueden establecer las responsabilidades y *lo que se debe hacer* para:

- Elaboración: quién o quiénes pueden elaborar documentos o actualizarlos.
- Revisión: quién o quiénes deben revisar un documento antes de su aprobación final.
- Aprobación: quién o quiénes aprueban un documento para su emisión.
- Distribución: quién se encarga de ponerlo a disposición de las personas usuarias luego de su aprobación.
- Resguardo: quién se encarga de resguardarlos (evitar extravíos, daños, etc.)
- Actualización: quién se encarga de asegurarse de que se mantienen vigentes.

Además, se pueden incluir otros aspectos como el establecimiento de la jerarquía documental, el formato y contenido mínimo de acuerdo con el tipo de documento, entre otros.

La jerarquía documental, en términos generales, establece los nombres que serán usados y su orden de importancia relativa, lo que permite, a su vez, afinar detalles sobre lo indicado en el listado anterior.

Por ejemplo, a lo interno de una auditoría interna del sector público costarricense,

podría establecerse una jerarquía documental como la siguiente:

Tipo	Documento
Externo	Ley General de Control Interno.
	• Normas para el ejercicio de la auditoría interna en el sector público. • Normas generales de auditoría para el sector público. • Lineamientos generales para el análisis de presuntos hechos irregulares.
	Reglamento Organizativo.
Interno	Procedimientos.
	Formularios.

Nota: No se debe considerar como una lista exhaustiva sino como un ejemplo ilustrativo.

Un procedimiento debe incluir el propósito u objetivo, su aplicación o alcance, la descripción del proceso, un listado de la documentación interna y externa que se menciona como referencia. Estas podrían considerarse secciones o apartados.

Por otra parte, debería incluir información básica como nombre del procedimiento, código, versión, fecha de entrada en vigor, personal involucrado (quien elabora, quien revisa y quien aprueba), la cantidad de páginas que conforman al documento, entre otros. Éstos elementos podrían incorporarse en un encabezado o en una portada.

Es usual encontrarse con procedimientos que incluyen, como sección o apartado, las responsabilidades. Es recomendable, por el contrario, que las responsabilidades no sean listadas en una sección aparte, sino que sean plasmadas explícitamente en los pasos de la descripción del proceso.

De hecho, un procedimiento debe describir, por medio de pasos, sencillos y concretos, las acciones (en secuencia lógica) que se deben realizar, quién debe realizarlas (las responsabilidades) y, cómo realizarlas.

Dependiendo de la complejidad de la acción concreta que se está documentando en el procedimiento, se podría considerar detallarla, pero en otro documento, un documento que sea complementario al procedimiento y derivado de éste, pero ubicado en un peldaño inferior de la jerarquía documental.

Por ejemplo, las NGASP establece en su apartado 205 Comunicación de resultados, numeral 01 lo siguiente:

> *"La organización de auditoría debe establecer e implementar políticas y procedimientos sobre las formas de comunicación y el trámite de documentos que origine el proceso de auditoría"*

En ese sentido, una auditoría interna del sector público debe establecer un procedimiento para la comunicación de resultados de auditoría.

En dicho procedimiento se debe indicar, como uno de los pasos, la **realización del informe de auditoría**, pero los detalles específicos de cómo elaborar un informe (su estructura de apartados y el contenido mínimo de cada uno, las fuentes, márgenes,

interlineado de párrafos a utilizar, cómo presentar los cuadros, gráficos y figuras, el estilo de redacción, etc.) desvían la atención de lo medular en el procedimiento que es la realización del informe, por lo que es recomendable que éstos detalles se incluyan en otro documento. Se puede crear entonces una guía o instructivo (la nomenclatura se debe incorporar en la jerarquía documental) para desarrollar los detalles de la realización del informe de auditoría.

¿En qué extensión documentar?

A partir de lo anterior, es válido cuestionarse ¿en qué extensión se debe documentar un proceso? Y ¿cuáles procesos se deben documentar? No hay una respuesta definitoria, pues la normativa aplicable y el conocimiento técnico y experiencia con los que se cuente a lo interno de la institución o del departamento en materia de gestión de procesos y elaboración de procedimientos, así como la madurez en su uso, puede determinar la respuesta a ambas preguntas.

Es importante reconocer que, al documentar, son aplicables los adagios populares "todo extremo es malo" y "ni tanto que queme al santo ni tan poco que no lo alumbre" ya que la documentación no es un fin en sí mismo, por lo que debe prevalecer el sentido común para determinar lo que se debe documentar y su extensión.

En ocasión de una auditoría de calidad, una persona comentaba que recién habían derogado el procedimiento para el uso del servicio sanitario... ¡acción que se nos enseña desde la infancia!... parece broma, pero es una historia real. Lamentablemente, en tiempos de pandemia, se ha tenido que recurrir a afiches informativos para documentar la forma correcta de lavado de manos para evitar infecciones... ¡acción que se nos enseña desde la infancia!... parece broma, pero es una historia real.

Una planificación sistemática del proceso de documentación, puede permitir determinar los procesos que se ejecutan en la institución, departamento o puesto de trabajo, así como su interrelación y, de esa forma, poder establecer con criterio técnico los procedimientos y documentación relacionada que se requieran para ejecutar satisfactoriamente los procesos, y que no se llegue a caer en absurdos (aparentes) como en el caso del procedimiento para el uso del servicio sanitario, que no tiene relación con la misión (o propósito) de una institución, o de un departamento o de un puesto de trabajo.

Se debe tener en cuenta lo indicado anteriormente, respecto a que la documentación no es un fin en sí misma, la documentación de procesos se debe acompañar de sesiones de capacitación para asegurar que se comprende, no sólo el contenido de un procedimiento específico sino del esfuerzo que se realiza por documentar.

Retos: consideraciones finales.

Como personas funcionarias públicas tenemos el deber de ejecutar nuestro trabajo eficaz y eficientemente y así coadyuvar con el cumplimiento de los objetivos de la institución para la que laboramos.

Si existe una iniciativa de documentación, sea incipiente o madura, nuestro deber es apoyarla y enriquecerla con nuestro conocimiento y con nuestra experiencia, pero sobre todo, con una actitud de apertura al cambio y mejoramiento continuo.

Si no existe tal iniciativa... ¿qué esperas para dar el primer paso y liderar con el ejemplo?

OCU BOLETÍN

El Valor del Control y el Control del Valor

LICDA. MARIELA PÉREZ IBARRA
Subcontralora

mariela.perez@ucr.ac.cr

El Valor del Control y el Control del Valor

Las personas nos referimos al concepto de control en muchos ámbitos y de formas distintas. Es así como el mencionar la palabra control puede interpretarse de varias maneras. En este sentido, y con el fin de aclarar el término adecuadamente, a continuación se presenta como la Real Academia Española (RAE) define la palabra control:

1. *m. Comprobación, inspección, fiscalización, intervención.*
2. *m. Dominio, mando, preponderancia.*
3. *m. Oficina, despacho, dependencia, etc., donde se controla.*
4. *m. puesto de control.*
5. *m. Regulación, manual o automática, sobre un sistema.*
6. *m. testigo (muestra).*
7. *m. Mando o dispositivo de regulación.*
8. *m. Tablero o panel donde se encuentran los mandos. U. m. en pl.*
9. *m. Examen parcial para comprobar la marcha de los alumnos.*[1]

Entonces, es necesario que el emisor aclare al receptor el concepto de control que utiliza en el mensaje que transmite, ya sea de forma verbal o escrita. Esta conceptualización permite darle un sentido claro del tema a tratar.

Ahora bien, en el ámbito de la Administración, tanto del sector público como de organizaciones privadas, la determinación del control es clave si se considera el marco COSO, el cual es base para la formulación de la Ley General de Control Interno (LGCI) vigente en Costa Rica desde el año 2002. Vale la pena aclarar que el COSO es el acrónimo del Committee of Sponsoring Organizations of the Tradeway Commission, que corresponde a una organismo integrado por varias organizaciones que busca brindar una referencia estandarizada en temas de control interno, fraude, gestión administrativa, entre otros. Es referente de buenas prácticas administrativas para el sector privado, pero varios elementos de este documento fueron considerados en la LGCI, por lo que son de acatamiento obligatorio en el sector público.

Lo importante es que COSO determina el valor del control, en un Sistema de Control Interno, ejecutado por la administración activa en procura del logro de los objetivos propuestos; buscando la eficiencia y eficacia

1 Tomado de la dirección electrónica https://dle.rae.es/control, el 2/5/2021.

en las actividades y procedimientos ejecutados, la confiabilidad en la información financiera y el cumplir con la normativa aplicable vigente.

Así que todas las actividades relacionadas con las definiciones de control por la RAE, pueden ser parte de un sistema de control interno que busca el éxito de la planificación establecida en las instituciones y organizaciones, pero su valor sólo puede medirse si su ejecución realmente es efectiva, de lo contrario podría ser más bien un acto burocrático de cumplimiento obligatorio pero que más bien interfiere con el logro de los objetivos propuestos.

En consecuencia, es importante que:

1. Realizar evaluaciones periódicas a los sistemas de control interno establecidos por quienes pueden modificarlos, con el fin de realizar los cambios que se requieran oportunamente y brindar herramientas para que se ejecutan las labores asignadas adecuadamente.

2. Asegurarse que las personas que ejecutan las labores entiendan claramente los elementos del control y los procedimientos dispuestos para ello, al comprenderlos serán conscientes del valor de esos controles en sus funciones diarias y como contribuyen al bienestar social o financiera de la entidad en la cual son colaboradores. Es fundamental el mantener canales de comunicación abiertos y procesos de capacitación periódicos, para contar con colaboradores debidamente preparados para la adecuada ejecución de las funciones que realiza.

Ahora bien, otro elemento relacionado con el control es el poder determinar el valor de lo que se quiere controlar, para lo cual traigo a colación la definición de la palabra valor según la RAE:

1. *m. Grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar o deleite.*

2. *m. Cualidad de las cosas, en virtud de la cual se da por poseerlas cierta suma de dinero o equivalente.*

3. *m. Alcance de la significación o importancia de una cosa, acción, palabra o frase.*

4. *m. Subsistencia y firmeza de algún acto.*

5. *m. Fuerza, actividad, eficacia o virtud de las cosas para producir sus efectos.*

6. *m. Rédito, fruto o producto de una hacienda, estado o empleo.*

7. *m. Equivalencia de una cosa a otra, especialmente hablando de las monedas.*

8. *m. Cualidad del ánimo, que mueve a acometer resueltamente grandes empresas y a arrostrar los peligros. U. t. en sent. peyor.,- denotando osadía, y hasta desvergüenza.* ¿Cómo tienes valor para eso? Tuvo el valor de negarlo.

9. *m. Persona que posee o a la que se le atribuyen cualidades positivas para desarrollar una determinada actividad. Es un joven valor de la guitarra.*

10. *m. Fil. Cualidad que poseen algunas realidades, consideradas bienes, por lo cual son estimables.*

11. *m. Mús. Duración del sonido que corresponde a cada nota, según la figura con que esta se representa.*

12. *m. Pint. En una pintura o un dibujo, grado de claridad, media tinta o sombra que tiene cada tono o cada pormenor en relación con los demás.*

13. *m. pl. Econ. Títulos representativos o anotaciones en cuenta de participación en sociedades, de cantidades prestadas, de mercaderías, de depósitos y de fondos monetarios, futuros, opciones, etc., que son objeto de operaciones mercantiles. Los valores están en alza, en baja, en calma.*

Es así como al hablar del control del valor, me refiero a las actividades ejecutadas para proteger, custodiar, promover o cualquier otro acto establecido, con el fin de preservar aquello que se estima valioso. Lo relevante de esta apreciación del valor es que permite determinar otro principio fundamental del control, el cual radica en que las actividades de controlar no deben ser más costosa que el valor de lo controlado.

Un control que requiera mantenerse sin que se mida el costo que se incurre, podría más bien limitar el fin por el cual se implantó, lo que produciría rendimientos negativos a la organización que se reflejaría en su información financiera y que no presenta un elemento positivo en el logro de los objetivos planteados.

En ese sentido, para que un sistema de control interno sea valorado adecuadamente y logre cumplir con su razón de ser, debe realmente coadyuvar con el cumplimiento de los objetivos planteados para lo cual fueron establecidos; de lo contrario podría más bien incidir negativamente en los procesos ejecutados. Así mismo, el conocer el valor del control y de lo controlado es también una tarea necesaria con el fin de contribuir al uso eficiente de los recursos disponibles.

En conclusión, es fundamental que las personas que tiene la potestad del establecimiento, mantenimiento, perfeccionamiento y evaluación del sistema de control interno, lo analicen de forma periódica, para así conocer el aporte de los controles establecidos considerando lo siguiente: el valor que aporta a la organización en el logro de los objetivos establecidos y que los mismos contribuyan de forma positiva en la economía de la entidad en la que laboran. Sólo con esta práctica se logra que el cumplimiento del modelo COSO y de la LGCI, para las instituciones del sector público costarricense, sea un aporte positivo para quienes ejecutan sus labores y quienes reciben el bien o servicio requerido; de lo contrario se podría estar en presencia de procesos burocráticos que perjudican la relación con el usuario de los servicios prestados o del costo del bien ofrecido.

Control Interno

BOLETÍN TÉCNICO **2022**

Nota: Los artículos en este Boletín Técnico son aportes de funcionarios de la Oficina de Contraloría Universitaria, sin embargo, no corresponden a pronunciamientos oficiales de ésta.

Lo invitamos a visitar nuestro sitio web http://www.ocu.ucr.ac.cr en la que podrá obtener información sobre la función de auditoría, temas de interés para la administración universitaria; incluso puede remitirnos sus observaciones y sugerencias.

Comuníquese con nosotros si desea que se considere un artículo para publicar en este boletín.

Publicación periódica de la Oficina de Contraloría Universitaria

Teléfonos: 2511-1433 **Fax:** 2224-3670
Correo electrónico: contraloria.universitaria@ucr.ac.cr
Sitio web: http://www.ocu.ucr.ac.cr

Contraloría Universitaria
UCR